

12/26/01  
1131 U.S. PTO

**PATENT APPLICATION TRANSMITTAL LETTER**  
(Large Entity)

Docket No.  
00001-0417

TO THE ASSISTANT COMMISSIONER FOR PATENTS

Transmitted herewith for filing under 35 U.S.C. 111 and 37 C.F.R. 1.53 is the patent application of:

Scott A. Vanstone et al.

For: **METHOD OF PUBLIC KEY GENERATION**

11073 U.S. PTO  
10/025924  
12/26/01

Enclosed are:

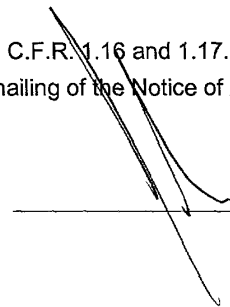
- ☐ Certificate of Mailing with Express Mail Mailing Label No.
- ☒ seven sheets of drawings.
- ☐ A certified copy of a application.
- ☒ Declaration ☐ Signed. ☒ Unsigned.
- ☒ Power of Attorney
- ☐ Information Disclosure Statement
- ☐ Preliminary Amendment
- ☐ Other:

**CLAIMS AS FILED**

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	14	- 20 =	0	x \$18.00	\$0.00
Indep. Claims	2	- 3 =	0	x \$84.00	\$0.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>					\$0.00
BASIC FEE					\$740.00
TOTAL FILING FEE					\$740.00

- ☒ A check in the amount of \$740.00 to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. as described below. A duplicate copy of this sheet is enclosed.
  - ☐ Charge the amount of as filing fee.
  - ☐ Credit any overpayment.
  - ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
  - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Dated: December 21, 2001

  
\_\_\_\_\_  
Signature

cc:

P01LARGE/REV06

FEE TRANSMITTAL for FY 2002		Complete if Known	
		Application Number	Not Yet Assigned
Patent fees are subject to annual revision.		Filing Date	Not Yet Assigned
		First Named Inventor	Scott A. Vanstone
		Examiner Name	Not Yet Assigned
		Group Art Unit	Not Yet Assigned
TOTAL AMOUNT OF PAYMENT		\$740.00	Attorney Docket No. 00001-0417

METHOD OF PAYMENT		FEE CALCULATION (continued)	
<b>1.</b> <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to: Deposit Account Number <b>Orange &amp; Chari</b> Deposit Account Name <b>150633</b> <input checked="" type="checkbox"/> Charge Any Additional Fee Required Under 37 CFR §§ 1.16 and 1.17 <input type="checkbox"/> Applicant claims small entity status See 37 CFR § 1.27		<b>3. ADDITIONAL FEES</b> Large Entity Small Entity Fee Code (\$) Fee Code (\$) Fee Description Fee Paid	
<b>2.</b> <input checked="" type="checkbox"/> Payment Enclosed: <input checked="" type="checkbox"/> Check <input type="checkbox"/> Credit card <input type="checkbox"/> Money Order <input type="checkbox"/> Other		105 130 205 65 Surcharge - late filing fee or oath	
<b>FEE CALCULATION</b>		127 50 227 25 Surcharge - late provisional filing fee or cover sheet	
<b>1. BASIC FILING FEE</b> Large Entity Small Entity Fee Code (\$) Fee Code (\$) Fee Description Fee Paid		139 130 139 130 Non - English specification	
101 740 201 370 Utility filing fee 740.00		147 2,520 147 2,520 For filing a request for ex parte reexamination	
106 330 206 165 Design filing fee		112 920* 112 920* Requesting publication of SIR prior to Examiner action	
107 510 207 255 Plant filing fee		113 1,840* 113 1,840* Requesting publication of SIR after Examiner action	
108 740 208 370 Reissue filing fee		115 110 215 55 Extension for reply within first month	
114 160 214 80 Provisional filing fee		116 400 216 200 Extension for reply within second month	
SUBTOTAL (1) 740.00		117 920 217 460 Extension for reply within third month	
<b>2. EXTRA CLAIM FEES</b>		118 1,440 218 720 Extension for reply within fourth month	
Total Claims -20** = 0 X Fee from below = 0.00		128 1,960 228 980 Extension for reply within fifth month	
Independent Claims -3** = 0 X Fee from below = 0.00		119 320 219 160 Notice of Appeal	
Multiple Dependent		120 320 220 160 Filing a brief in support of an appeal	
Large Entity Small Entity Fee Code (\$) Fee Code (\$) Fee Description Fee Paid		121 280 221 140 Request for oral hearing	
103 18 203 9 Claims in excess of 20		138 1,510 138 1,510 Petition to institute a public use proceeding	
102 84 202 42 Independent claims in excess of 3		140 110 240 55 Petition to revive - unavoidable	
104 280 204 140 Multiple dependent claim, if not paid		141 1,280 241 640 Petition to revive - unintentional	
109 84 209 42 ** Reissue independent claims over original patent		142 1,280 242 640 Utility issue fee (or reissue)	
110 18 210 9 ** Reissue claims in excess of 20 and over original patent		143 460 243 230 Design issue fee	
SUBTOTAL (2) 0.00		144 620 244 310 Plant issue fee	
**or number previously paid, if greater; For Reissues, see above		122 130 122 130 Petitions to the Commissioner	
		123 50 123 50 Processing fee under 37 CFR § 1.17(q)	
		126 180 126 180 Submission of Information Disclosure Statement	
		581 40 581 40 Recording each patent assignment per property (times number of properties)	
		146 740 246 370 Filing a submission after final rejection (37 CFR § 1.129(a))	
		149 740 249 370 For each additional invention to be examined (37 CFR § 1.129(b))	
		179 740 279 370 Request for Continued Examination (RCE)	
		169 900 169 900 Request for expedited examination of a design application	
		Other fee (specify)	
		SUBTOTAL (3)	

SUBMITTED BY		Complete (if applicable)	
Name (Print/Type) John R.S. Orange	Registration No. (Attorney/Agent) 29,725	Telephone (416)601-8440	
Signature		Date December 21, 2001	

**WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

12/26/01  
1131 U.S. PTO

**PATENT APPLICATION TRANSMITTAL LETTER**  
(Large Entity)

Docket No.  
00001-0417

TO THE ASSISTANT COMMISSIONER FOR PATENTS

Transmitted herewith for filing under 35 U.S.C. 111 and 37 C.F.R. 1.53 is the patent application of:

Scott A. Vanstone et al.

For: **METHOD OF PUBLIC KEY GENERATION**

11073 U.S. PTO  
10/025924  
12/26/01

Enclosed are:

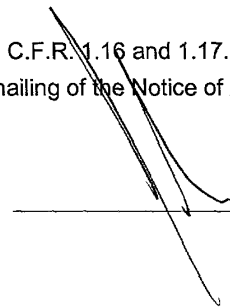
- ☐ Certificate of Mailing with Express Mail Mailing Label No.
- ☒ seven sheets of drawings.
- ☐ A certified copy of a application.
- ☒ Declaration ☐ Signed. ☒ Unsigned.
- ☒ Power of Attorney
- ☐ Information Disclosure Statement
- ☐ Preliminary Amendment
- ☐ Other:

**CLAIMS AS FILED**

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	14	- 20 =	0	x \$18.00	\$0.00
Indep. Claims	2	- 3 =	0	x \$84.00	\$0.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>					\$0.00
BASIC FEE					\$740.00
TOTAL FILING FEE					\$740.00

- ☒ A check in the amount of \$740.00 to cover the filing fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge and credit Deposit Account No. as described below. A duplicate copy of this sheet is enclosed.
  - ☐ Charge the amount of as filing fee.
  - ☐ Credit any overpayment.
  - ☒ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
  - ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

Dated: December 21, 2001

  
\_\_\_\_\_  
Signature

cc:

P01LARGE/REV06

FEE TRANSMITTAL for FY 2002		Complete if Known	
		Application Number	Not Yet Assigned
Patent fees are subject to annual revision.		Filing Date	Not Yet Assigned
		First Named Inventor	Scott A. Vanstone
		Examiner Name	Not Yet Assigned
		Group Art Unit	Not Yet Assigned
TOTAL AMOUNT OF PAYMENT		\$740.00	Attorney Docket No. 00001-0417

METHOD OF PAYMENT		FEE CALCULATION (continued)	
<b>1.</b> <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to: Deposit Account Number <b>Orange &amp; Chari</b> Deposit Account Name <b>150633</b> <input checked="" type="checkbox"/> Charge Any Additional Fee Required Under 37 CFR §§ 1.16 and 1.17 <input type="checkbox"/> Applicant claims small entity status See 37 CFR § 1.27		<b>3. ADDITIONAL FEES</b> Large Entity Small Entity Fee Code (\$) Fee Code (\$) Fee Description Fee Paid	
<b>2.</b> <input checked="" type="checkbox"/> Payment Enclosed: <input checked="" type="checkbox"/> Check <input type="checkbox"/> Credit card <input type="checkbox"/> Money Order <input type="checkbox"/> Other		105 130 205 65 Surcharge - late filing fee or oath	
<b>FEE CALCULATION</b>		127 50 227 25 Surcharge - late provisional filing fee or cover sheet	
<b>1. BASIC FILING FEE</b> Large Entity Small Entity Fee Code (\$) Fee Code (\$) Fee Description Fee Paid		139 130 139 130 Non - English specification	
101 740 201 370 Utility filing fee 740.00		147 2,520 147 2,520 For filing a request for ex parte reexamination	
106 330 206 165 Design filing fee		112 920* 112 920* Requesting publication of SIR prior to Examiner action	
107 510 207 255 Plant filing fee		113 1,840* 113 1,840* Requesting publication of SIR after Examiner action	
108 740 208 370 Reissue filing fee		115 110 215 55 Extension for reply within first month	
114 160 214 80 Provisional filing fee		116 400 216 200 Extension for reply within second month	
SUBTOTAL (1) 740.00		117 920 217 460 Extension for reply within third month	
<b>2. EXTRA CLAIM FEES</b>		118 1,440 218 720 Extension for reply within fourth month	
Total Claims -20** = 0 X Fee from below = 0.00		128 1,960 228 980 Extension for reply within fifth month	
Independent Claims -3** = 0 X Fee from below = 0.00		119 320 219 160 Notice of Appeal	
Multiple Dependent		120 320 220 160 Filing a brief in support of an appeal	
Large Entity Small Entity Fee Code (\$) Fee Code (\$) Fee Description Fee Paid		121 280 221 140 Request for oral hearing	
103 18 203 9 Claims in excess of 20		138 1,510 138 1,510 Petition to institute a public use proceeding	
102 84 202 42 Independent claims in excess of 3		140 110 240 55 Petition to revive - unavoidable	
104 280 204 140 Multiple dependent claim, if not paid		141 1,280 241 640 Petition to revive - unintentional	
109 84 209 42 ** Reissue independent claims over original patent		142 1,280 242 640 Utility issue fee (or reissue)	
110 18 210 9 ** Reissue claims in excess of 20 and over original patent		143 460 243 230 Design issue fee	
SUBTOTAL (2) 0.00		144 620 244 310 Plant issue fee	
**or number previously paid, if greater; For Reissues, see above		122 130 122 130 Petitions to the Commissioner	
		123 50 123 50 Processing fee under 37 CFR § 1.17(q)	
		126 180 126 180 Submission of Information Disclosure Statement	
		581 40 581 40 Recording each patent assignment per property (times number of properties)	
		146 740 246 370 Filing a submission after final rejection (37 CFR § 1.129(a))	
		149 740 249 370 For each additional invention to be examined (37 CFR § 1.129(b))	
		179 740 279 370 Request for Continued Examination (RCE)	
		169 900 169 900 Request for expedited examination of a design application	
		Other fee (specify)	
		SUBTOTAL (3)	

SUBMITTED BY		Complete (if applicable)	
Name (Print/Type) John R.S. Orange	Registration No. (Attorney/Agent) 29,725	Telephone (416)601-8440	
Signature		Date December 21, 2001	

**WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.



## METHOD OF PUBLIC KEY GENERATION

### FIELD OF THE INVENTION

- 5 The present invention relates to public key cryptosystems and more particularly to key generation within such systems.

### BACKGROUND OF THE INVENTION

- 10 The basic structure of a public key cryptosystem is well known and has become ubiquitous with security in data communication systems. Such systems use a private key  $k$  and a corresponding public key  $\alpha^k$  where  $\alpha$  is a generator of the group. Thus one party may encrypt a message  $m$  with the intended recipients public key and the recipient may apply his private key to decrypt it.

- 15 Similarly, the cryptosystems may be used for key agreement protocols where each party exponentiates the other party's public key with their own private key. Thus party A will take B's public key  $\alpha^b$  and exponentiate it with A's private key  $a$  to obtain a session key  $\alpha^{ab}$ . Similarly, B will take A's public key  $\alpha^a$  and exponentiate it with B's private key  $b$  to obtain the same session key  $\alpha^{ab}$ . Thereafter data may be transferred using a symmetric key protocol utilizing the common  
20 session key.

- Public key cryptosystems may also be used to sign messages to authenticate the author and/or the contents. In this case the sender will sign a message using his private key and a recipient can verify the message by applying the public key of the sender. If the received  
25 message and the recovered message correspond then the authenticity is verified.

- The public key cryptosystems rely on the intractability of the discrete log problem in finite field arithmetic, that is even when the generator  $\alpha$  and public key is known, it is computationally infeasible to obtain the corresponding private key. The security of such systems  
30 does therefore depend on the private key remaining secret. To mitigate the opportunity of disclosing the private key, protocols have been developed that use a pair of private keys and

corresponding public keys, referred to as long term and short term or ephemeral key pairs respectively. The ephemeral private key is generated at the start of each session between a pair of correspondents, usually by a random number generator. The corresponding ephemeral public key is generated and the resultant key pair used in one of the possible operations described above.

- 5 The long-term public key is utilized to authenticate the correspondent through an appropriate protocol. Once the session is terminated, the ephemeral key is securely discarded and a new ephemeral key generated for a new session.

10 Some of the more popular protocols for signature are the ElGamal family of signature schemes such as the Digital Signature Algorithm or DSA. The DSA algorithm utilizes both long term and ephemeral keys to generate a signature of the message. The DSA domain parameters are preselected. They consist of a prime number  $p$  of a predetermined length, by way of example 1024 bits; a prime number  $q$  of a predetermined bit length, by way of example 160 bits, where  $q$  divides  $p-1$ ; a generator  $\alpha$  lying between 2 and  $p-1$  and which satisfies the condition  
15  $(\alpha^q \bmod p) = 1$ , and; a cryptographic hash function  $H$ , such as SHA-1.

20 The DSA requires the signatory to select an ephemeral key  $k$  lying between 1 and  $q-1$ . A first signature component  $r$  is generated from the generator  $\alpha$  such that  $r = (\alpha^k \bmod p) \bmod q$ . A second signature component  $s$  is generated such that  $s = k^{-1}(H(m) + dr) \bmod q$ , and  $d$  is the long term private key of the signatory. The signature on the message  $m$  is  $(r,s)$ . The signature may be verified by computing

$H(m)$ ,

$$u_1 = s^{-1}H(m) \bmod q$$

$$u_2 = s^{-1}r \bmod q$$

- 25  $v = \alpha^{u_1} \beta^{u_2} \bmod p$ , where  $\beta = \alpha^d \bmod p$  is the long term public key of the signatory and finally verifying that  $r = v \bmod q$ . The use of both the ephemeral and long-term keys in the signature binds the identity of the signatory to the ephemeral key but does not render the long-term key vulnerable.

- 30 A similar signature protocol known as ECDSA may be used for elliptic curve cryptosystems. In this protocol  $k$  is selected in the interval 1 to  $n-1$  where  $n$  is an  $l$  bit prime. The signature component  $r$  is generated by converting the  $x$  coordinate of the public key  $kP$ , where  $P$

is the seed point on the curve, to an integer mod  $n$ , i.e.  $r = x_{kp} \bmod n$ . The component  $s = k^{-1}(H(m) + dr) \bmod n$  and the signature on the message  $m$  is  $(r, s)$ .

It will be apparent in ElGamal signature schemes such as the DSA and ECDSA, that if an ephemeral key  $k$  and the associated message  $m$  and signature  $(r, s)$  is obtained it may be used to yield the long term private key  $d$  and thereafter each of the ephemeral keys  $k$  can be obtained. Neither the DSA nor the ECDSA inherently disclose any information about the public key  $k$ . They both require the selection of  $k$  to be performed by a random number generator and it will therefore have a uniform distribution throughout the defined interval. However the implementation of the DSA may be done in such a way as to inadvertently introduce a bias in to the selection of  $k$ . This small bias may be exploited to extract a value of the private key  $d$  and thereafter render the security of the system vulnerable. One such implementation is the DSS mandated by the National Institute of Standards and Technology (NIST) FIPS 186-2 Standard. The DSS stipulates the manner in which an integer is to be selected for use as a private key. A seed value,  $SV$ , is generated from a random number generator which is then hashed by a SHA-1 hash function to yield a bit string of predetermined length, typically 160 bits. The bit string represents an integer between 0 and  $2^{160} - 1$ . However this integer could be greater than the prime  $q$  and so the DSS requires the reduction of the integer mod  $q$ , i.e.  $k = \text{SHA-1}(\text{seed}) \bmod q$ .

Accordingly the algorithm for selecting  $k$  may be expressed as :-

if  $\text{SHA-1}(\text{seed}) \geq q$  then  $k \leftarrow \text{SHA-1}(\text{seed}) - q$   
else  $k \leftarrow \text{SHA-1}(\text{seed})$ .

With this algorithm it is to be expected that more values will lie in the first interval than the second and therefore there is a potential bias in the selection of  $k$ .

Recent work by Daniel Bleichenbacher suggests that the modular reduction to obtain  $k$  introduces sufficient bias in to the selection of  $k$  that an examination of  $2^{22}$  signatures could yield the private key  $d$  in  $2^{64}$  steps using  $2^{40}$  memory units. This suggests that there is a need for the careful selection of the ephemeral key  $k$ .

## SUMMARY OF THE INVENTION

It is therefore an object of the present invention to obviate or mitigate the above disadvantages in the generation of a private key.

5

In general terms the present invention provides a key generation technique in which any bias is eliminated during the selection of the key.

## BRIEF DESCRIPTION OF THE DRAWINGS

10

Embodiments of the invention will now be described by way of example only with reference to the accompanying drawings in which:-

10055924 122601

Figure 1 is a schematic representation of a data communication system;

15

Figure 2 is a flow chart showing a first embodiment of key generation;

Figure 3 is a flow chart showing a second embodiment;

20

Figure 4 is a flow chart showing a third embodiment;

Figure 5 is a flow chart showing a fourth embodiment;

Figure 6 is a flow chart showing a fifth embodiment; and

25

Figure 7 is a flow chart showing a sixth embodiment.

## DESCRIPTION OF THE PREFERRED EMBODIMENTS

30

Referring, therefore to figure 1, a data communication system 10 includes a pair of correspondents 12, 14 connected by a communication link 16. The link 16 may be a dedicated link, a multipurpose link such as a telephone connection or a wireless link depending on the particular applications. Similarly, the correspondents 12, 14 may be computer terminals, point-of-sale devices, automated teller machines, constrained devices such as PDA's, cellphones, pagers or any other device enabled for communication over a link 16.

35

Each of the correspondents 12, 14 includes a secure cryptographic function 20 including a secure memory 22, an arithmetic processor 24 for performing finite field operations, a random number generator 26 and a cryptographic hash function 28 for performing a secure cryptographic hash such as SHA-1. The output of the function 28 will be a bit string of predetermined length, typically 160 bits although other lengths such as 256, 384 or 512 are being used more frequently. It will be appreciated that each of these functions is controlled by a processor executing instructions to provide functionality and inter-operability as is well known in the art.

The secure memory 22 includes a register 30 for storing a long-term private key,  $d$ , and a register 32 for storing an ephemeral private key  $k$ . The contents of the registers 30, 32 may be retrieved for use by the processor 24 for performing signatures, key exchange and key transport functions in accordance with the particular protocols to be executed under control of the processor.

The long term private key,  $d$ , is generated and embedded at the time of manufacture or initialization of the cryptographic function and has a corresponding long-term public key  $\alpha^d$ . The long-term public key  $\alpha^d$  is stored in the memory 22 and is generally made available to other correspondents of the system 10.

The ephemeral key,  $k$ , is generated at each signature or other cryptographic exchange by one of the routines disclosed below with reference to figures 2 to 9. Once the key,  $k$ , and corresponding public key  $\alpha^k$  is generated, it is stored in the register 32 for use in the cryptographic protocol, such as the DSA or ECDSA described above.

Referring, therefore, to figure 2, a first method of generating a key,  $k$ , originates by obtaining a seed value (SV) from the random number generator 26. For the purposes of an example, it will be assumed that the cryptographic function is performed over a group of order  $q$ , where  $q$  is a prime represented as a bit string of predetermined length  $l$ . By way of example only it will be assumed that the length  $l$  is 160 bits, although, of course, other orders of the field may be used.

To provide a value of k of the appropriate order, the hash function 28 has an l bit output, e.g. a 160 bit output. The bit string generated by the random number generator 26 is greater than l bits and is therefore hashed by the function 28 to produce an output H(seed) of l bits.

5

The resultant output H(seed) is tested against the value of q and a decision made based on the relative values. If  $H(\text{seed}) < q$  then it is accepted for use as k. If not, the value is rejected and the random number generator is conditioned to generate a new value which is again hashed by the function 28 and tested. This loop continues until a satisfactory value is obtained.

10

A further embodiment is shown in figure 3. In this embodiment, the output of the random number generator 26 is hashed by hash function 28 as before and tested against the value of q. If the H(seed) value is not accepted, the output of the random number generator 26 is incremented by a deterministic function and rehashed by function 28.

15

The resultant value H(seed) is again tested and the procedure repeated until a satisfactory value of k is obtained.

The output may be incremented by adding a particular value to the seed value at each iteration, or may be incremented by applying a non-linear deterministic function to the seed value. For example, the output may be incremented by applying the function  $f(\text{seed}) = a.\text{seed}^2 + b \bmod 2^{160}$ , where a and b are integer constants.

20

25

A further embodiment is shown in figure 4 which has particular applicability to an elliptic curve cryptosystem. By way of example it will be assumed that a 163 bit string is required and that the output of the hash function 28 is 160 bits.

30

The random number generator 26 generates a seed value SV which is processed by the hash function 28 to obtain a first output H(seed).

The seed value SV is incremented by a selected function to provide a seed value SV+ which is further processed by the hash function 28 to provide a second output H(seed+).

5 The two outputs are then combined, typically by cocatenation, to produce a 320 bit string H(seed)//H(seed+). The excess bits, in this case 157 are rejected and the resultant value tested against the value of q. If the resultant value is less than q, it is accepted as the key k, if not the value is rejected.

10 Upon rejection, the random number generator may generate a new value as disclosed in figure 2 or may increment the seed value as disclosed in figure 3.

15 A further embodiment is shown in figure 5 which is similar to that of figure 4. In the embodiment of figure 5, the selection of the required l bit string is obtained by applying a l-bit wide masking window to the combined bit string.

20 This is tested against the value of q and if acceptable is used as the value of k. If it is not acceptable it is rejected and the l bit window incremented along the combined bit string to obtain a new value.

25 The values are tested and the window incremented until a satisfactory value is obtained.

A similar procedure may be used directly on an extended output of the hash function 28 as shown in figure 6 by applying a window to obtain the required l bit string. The bit string is tested against q and the window incremented until a satisfactory value of k is obtained.

25

30 As shown in figure 7, the value of k may be generated by utilizing a low Hamming weight integer obtained by combing the output of the random number generator 26 to facilitate computation of an intermediate public key  $\alpha^k$ . The integer is masked by combination with predetermined precomputed value k' to obtain the requisite Hamming weight for security. Such a procedure is disclosed in copending Canadian application 2,217,925. This procedure is modified to generate the low Hamming weight integer k as a bit string greater than l, for

example, a 180 bit string. The masking value  $k'$  is distributed throughout the 180 bit string and the resultant value reduced mod  $q$  to obtain a 163 bit value  $k''$ . Note that the value  $\alpha^{k''}$  can be efficiently computed by combining the precomputed value  $\alpha^{k'}$  with the efficiently computable value  $\alpha^k$ .

5

A similar technique may be used by relying on multiplicative masking. In this embodiment the value of  $k$  is combined with a value  $\beta$  where  $\beta = \alpha^u$ . The value of  $u$  is a secret value that is used to mask the low Hamming weight of  $k$ . Again, the values of  $u$  and the low Hamming weight

10 resultant value is  $k'' = u^k \text{ mod } q$ . It will be appreciated that  $\alpha^{k''}$  can be efficiently computed since  $\beta = \alpha^u$  is precomputed, and since  $k$  has low Hamming weight.

Although the invention has been described with reference to certain specific  
embodiments, various modifications thereof will be apparent to those skilled in the art without  
15 departing from the spirit and scope of the invention as outlined in the claims appended hereto.



**THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE  
PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:**

1. A method of generating a key over a group of order  $q$ , said method including the steps of:
  - generating a seed value from a random number generator;
  - performing a hash function on said seed number to provide an output;
  - determining whether said output is less than said prime number  $q$ ;
  - accepting said output for use as a key if the value thereof is less than said prime number  $q$ ; and
  - rejecting said output as a key if said value is not less than said order  $q$ .
2. The method of claim 1 wherein another seed value is generated by said random number generator if said output is rejected.
3. The method of claim 1 wherein the step of accepting said output as a key includes a further step of storing said key.
4. The method of claim 1 wherein said key is used for generation of a public key.
5. The method of claim 1 wherein said order  $q$  is prime number represented by a bit string of predetermined length  $l$ .
6. The method of claim 5 wherein said output from said hash function is a bit string of predetermined length  $l$ .
7. The method of claim 1 wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.
8. The method of claim 7, wherein said step of incrementing includes a further step of adding a particular value to said seed value.
9. A method of generating a key over a group of order  $q$ , said method including the steps of:
  - generating a seed value from a random number generator;
  - performing a hash function on said seed number to provide a first output;

incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output;

combining said first output and second output to produce a new output;

determining whether said new output has a value less than said order q;

accepting said new output as a key k if said new output has a value less than order q; and rejecting said new output as a key if said new output has a value less than order q

10. The method of claim 9 wherein upon rejection of said new output a new seed value is generated by said random number generator.
11. The method of claim 9 wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained.
12. The method of claim 9 wherein a bit string greater than a predetermined length l is obtained and an l bit string selected therefrom for comparison with said order q.
13. The method of claim 12 wherein upon rejection of said bit string of predetermined length l, a further l bit string is selected.
14. The method of claim 9 wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length l.



MOBILEIRON, INC. - EXHIBIT 1003  
Page 016

1002594, 123601

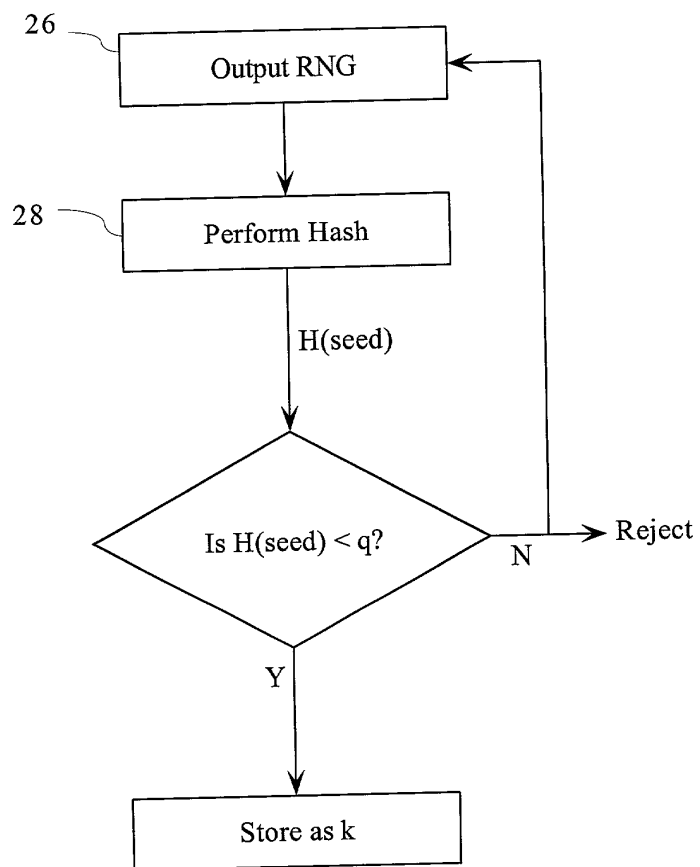


Fig. 2

1003924 12301  
T0327 425207

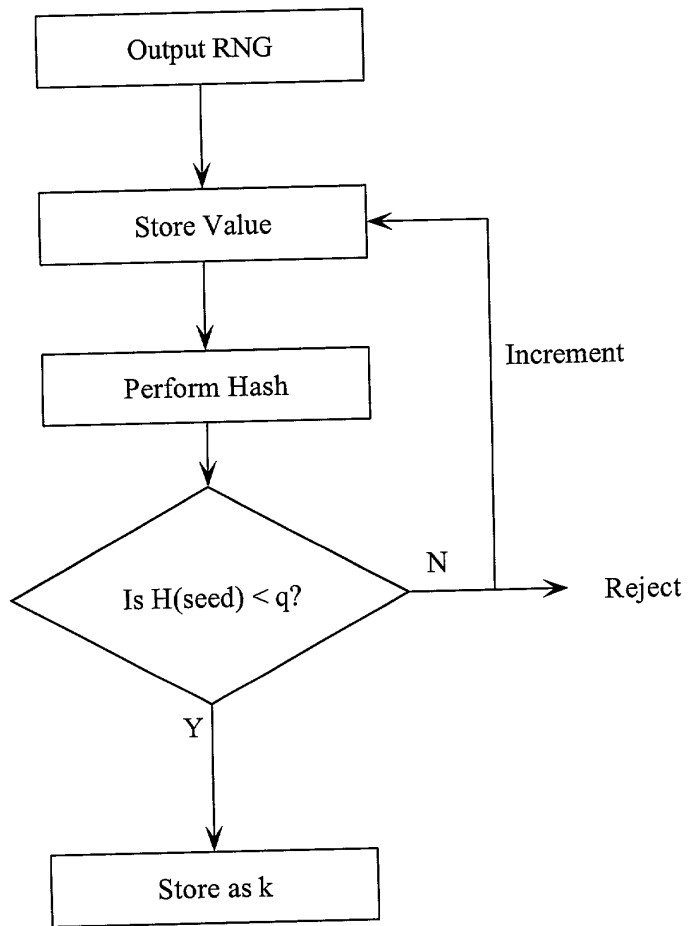


Fig. 3

10025934-13601

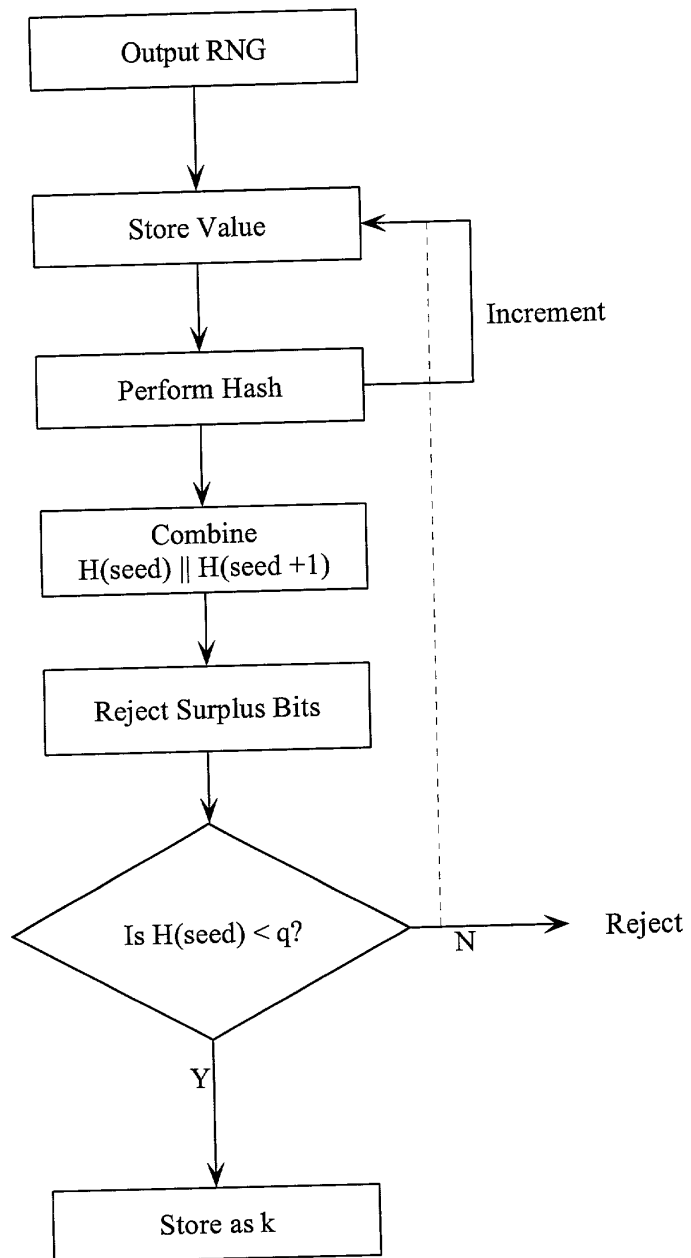


Fig. 4

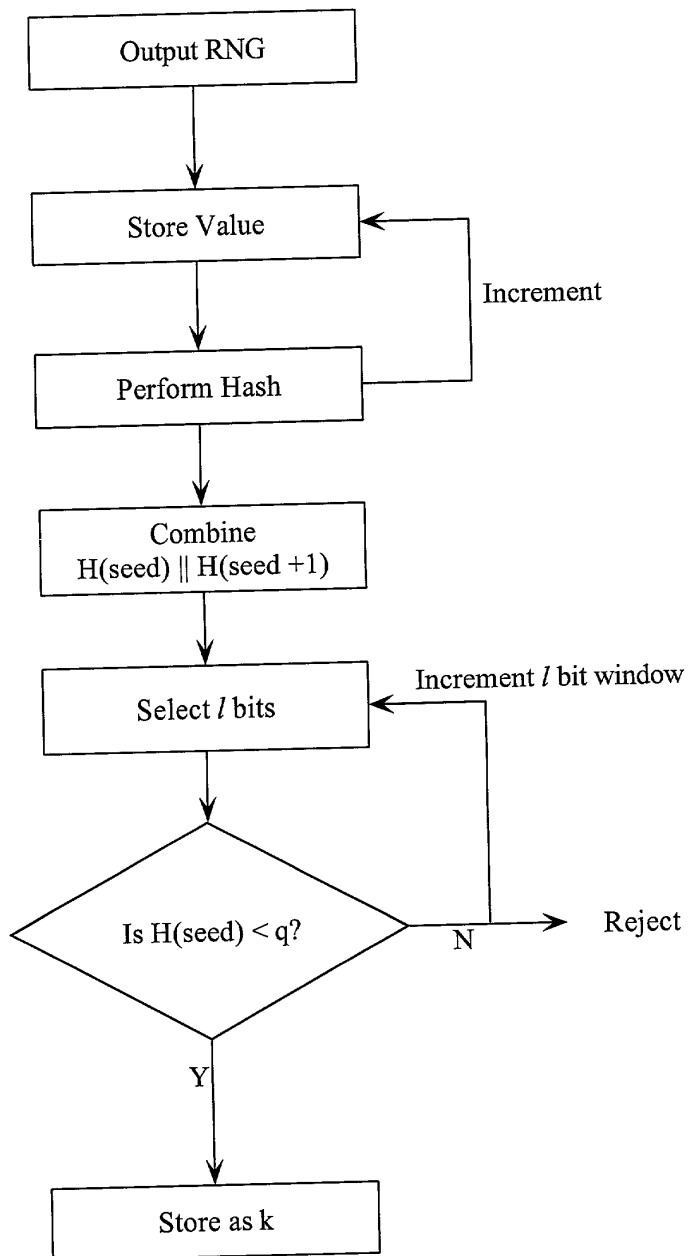


Fig. 5



1003924 426207

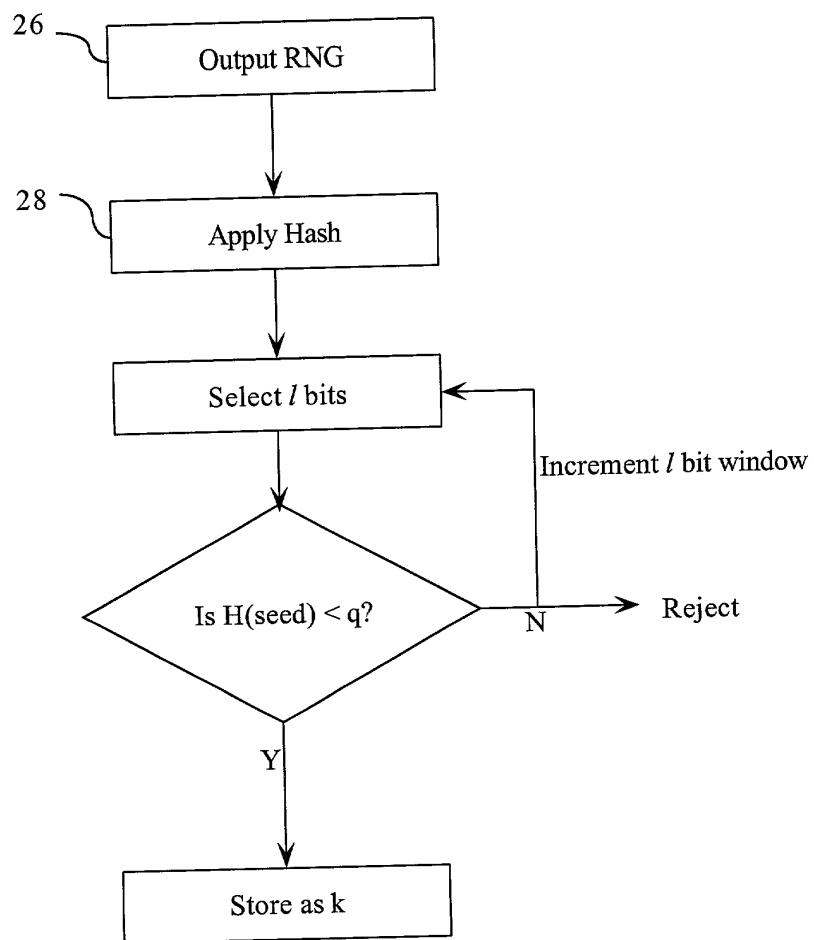


Fig. 6

10025941.12601

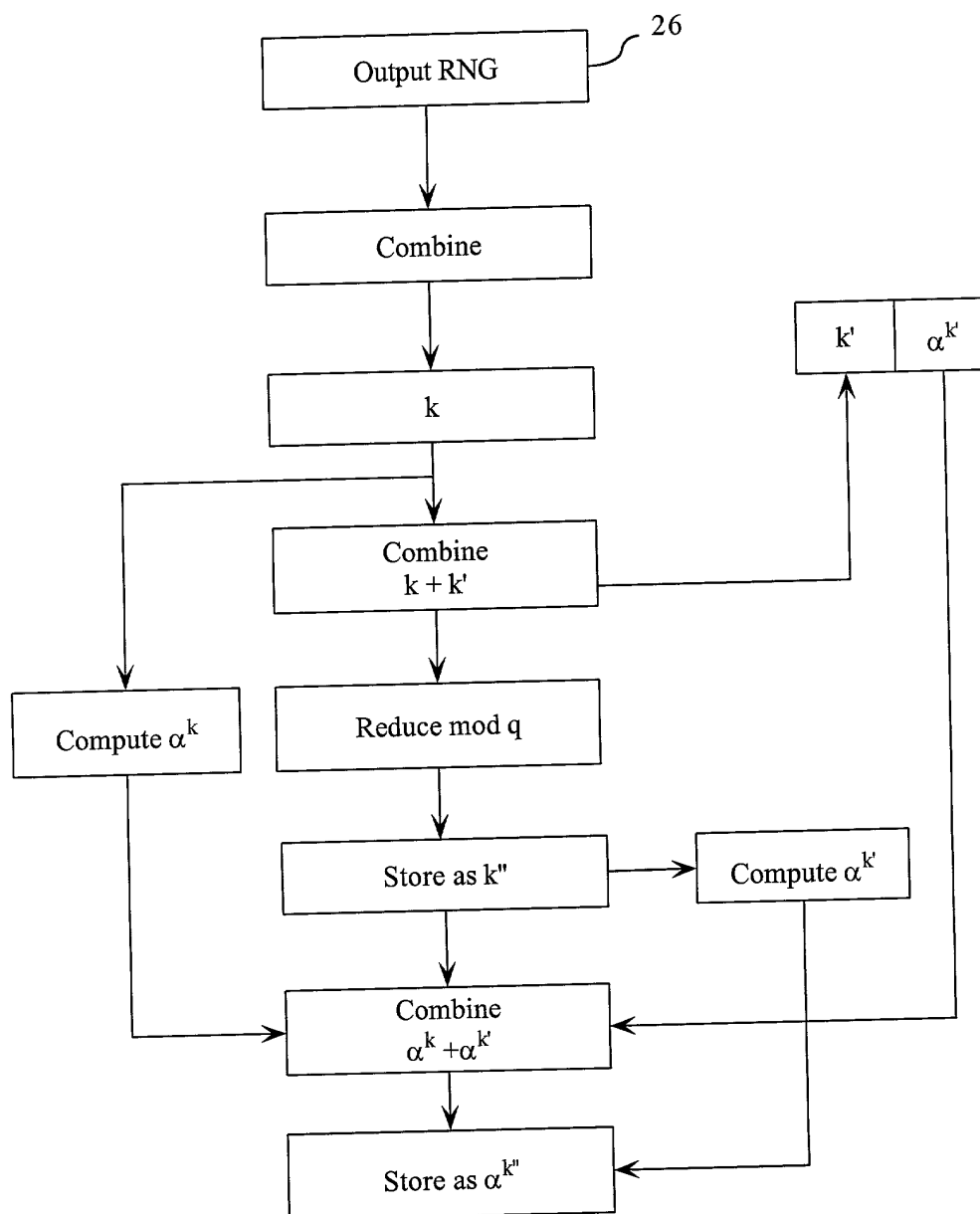


Fig. 7

Docket No.  
00001-0417

## Declaration and Power of Attorney For Patent Application

### English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

#### METHOD OF PUBLIC KEY GENERATION

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on \_\_\_\_\_ as United States Application No. or PCT International Application Number \_\_\_\_\_ and was amended on \_\_\_\_\_ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)	Priority	Not Claimed
<div style="display: flex; justify-content: space-between;"> <div> <u>2,329,590</u> (Number) </div> <div> <u>Canada</u> (Country) </div> <div> <u>27/12/2000</u> (Day/Month/Year Filed) </div> </div>	<input type="checkbox"/>	<input type="checkbox"/>
<div style="display: flex; justify-content: space-between;"> <div>_____ (Number)</div> <div>_____ (Country)</div> <div>_____ (Day/Month/Year Filed)</div> </div>	<input type="checkbox"/>	<input type="checkbox"/>
<div style="display: flex; justify-content: space-between;"> <div>_____ (Number)</div> <div>_____ (Country)</div> <div>_____ (Day/Month/Year Filed)</div> </div>	<input type="checkbox"/>	<input type="checkbox"/>

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

_____	_____
(Application Serial No.)	(Filing Date)
_____	_____
(Application Serial No.)	(Filing Date)
_____	_____
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

_____	_____	_____
(Application Serial No.)	(Filing Date)	(Status)
		(patented, pending, abandoned)
_____	_____	_____
(Application Serial No.)	(Filing Date)	(Status)
		(patented, pending, abandoned)
_____	_____	_____
(Application Serial No.)	(Filing Date)	(Status)
		(patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

**POWER OF ATTORNEY:** As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

<b>John R.S. Orange</b>	<b>29,725</b>
<b>Santosh K. Chari</b>	<b>41,477</b>
<b>Jeffrey Wong</b>	<b>46,414</b>

Send Correspondence to: **Orange & Chari**  
**Suite 4900, P.O. Box 190**  
**66 Wellington Street West**  
**Toronto, Ontario M5K 1H6 Canada**

Direct Telephone Calls to: *(name and telephone number)*  
**John R.S. Orange (416)601-8440**

Full name of sole or first inventor <b>Scott A. Vanstone</b>	
Sole or first inventor's signature	Date
Residence <b>10140 Pineview Trail, P.O. Box 490, Campbellville, Ontario L0P 1B0 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of second inventor, if any <b>Ashok Vadekar</b>	
Second inventor's signature	Date
Residence <b>250 Harris Street, R.R. 4, Rockwood, Ontario N0B 2K0 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of third inventor, if any <b>Robert J. Lambert</b>	
Third inventor's signature	Date
Residence <b>630 Holm Street, Cambridge, Ontario L5M 5N1 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of fourth inventor, if any <b>Robert P. Gallant</b>	
Fourth inventor's signature	Date
Residence <b>4788 Rosebush Road, Mississauga, Ontario L5M 5N1 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of fifth inventor, if any <b>Daniel R. Brown</b>	
Fifth inventor's signature	Date
Residence <b>106 Banstock Drive, Toronto, Ontario M2K 2H6 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of sixth inventor, if any <b>Alfred Menezes</b>	
Sixth inventor's signature	Date
Residence <b>1302-2267 Lakeshore Blvd. West Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	



## UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
www.uspto.gov



Bib Data Sheet

CONFIRMATION NO. 7632

<b>SERIAL NUMBER</b> 10/025,924	<b>FILING DATE</b> 12/26/2001 <b>RULE</b>	<b>CLASS</b> 380	<b>GROUP ART UNIT</b> 2131	<b>ATTORNEY DOCKET NO.</b> 00001-0417
<b>APPLICANTS</b> Scott A. Vanstone, Campbellville, CANADA; Ashok Vadekar, Rockwood, CA; Robert J. Lambert, Cambridge, CANADA; Robert P. Gallant, Mississauga, CANADA; Daniel R. Brown, Toronto, CANADA; Alfred Menezes, West Canada, CANADA;				
<b>** CONTINUING DATA *****</b>				
<b>** FOREIGN APPLICATIONS *****</b> CANADA 2,329,590 12/27/2000				
<b>IF REQUIRED, FOREIGN FILING LICENSE GRANTED</b> <b>** 02/25/2002</b>				
Foreign Priority claimed <input type="checkbox"/> yes <input type="checkbox"/> no 35 USC 119 (a-d) conditions <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Met after met Allowance Verified and Acknowledged _____ Examiner's Signature Initials		<b>STATE OR COUNTRY</b> CANADA	<b>SHEETS DRAWING</b> 7	<b>TOTAL CLAIMS</b> 14
				<b>INDEPENDENT CLAIMS</b> 2
<b>ADDRESS</b> AIR MAIL Orange & Chari 66 Wellington Street West, Suite 4900 P.O. Box 190 Toronto , ON M5K 1H6 CANADA				
<b>TITLE</b> Method of public key generation				
<b>FILING FEE RECEIVED</b> 870	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees ( Filing ) <input type="checkbox"/> 1.17 Fees ( Processing Ext. of time ) <input type="checkbox"/> 1.18 Fees ( Issue ) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit	

PATENT APPLICATION SERIAL NO. \_\_\_\_\_

U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICE  
FEE RECORD SHEET

12/28/2001 GGEBREA1 00000009 10025924

01 FC:101

740.00 OP

PTO-1556  
(5/87)

\*U.S. GPO: 2000-468-987/39595



# PATENT APPLICATION FEE DETERMINATION RECORD

Effective October 1, 2001

Application or Docket Number

## CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	14	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	14 minus 20 = *	
INDEPENDENT CLAIMS	2 minus 3 = *	
MULTIPLE DEPENDENT CLAIM PRESENT <input type="checkbox"/>		

\* If the difference in column 1 is less than zero, enter "0" in column 2

## CLAIMS AS AMENDED - PART II

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total *	Minus **	=
	Independent *	Minus ***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>		

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total *	Minus **	=
	Independent *	Minus ***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>		

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total *	Minus **	=
	Independent *	Minus ***	=
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>		

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."

\*\*\*If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

SMALL ENTITY TYPE ☐

OR

OTHER THAN SMALL ENTITY

RATE	FEE
BASIC FEE	370.00
X\$ 9=	
X42=	
+140=	
TOTAL	

RATE	FEE
BASIC FEE	740.00
X\$18=	
X84=	
+280=	
TOTAL	

SMALL ENTITY

OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE
X\$ 9=	
X42=	
+140=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$18=	
X84=	
+280=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$ 9=	
X42=	
+140=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$18=	
X84=	
+280=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$ 9=	
X42=	
+140=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$18=	
X84=	
+280=	
TOTAL ADDIT. FEE	

<b>CLAIMS ONLY</b>							SERIAL NO.	FILING DATE
							APPLICANT(S)	
CLAIMS								
	AS FILED		AFTER 1st AMENDMENT		AFTER 2nd AMENDMENT			
	IND.	DEP.	IND.	DEP.	IND.	DEP.	*	*
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								
25								
26								
27								
28								
29								
30								
31								
32								
33								
34								
35								
36								
37								
38								
39								
40								
41								
42								
43								
44								
45								
46								
47								
48								
49								
50								
TOTAL IND.	2	↓		↓		↓		
TOTAL DEP.	12	←		←		←		
TOTAL CLAIMS	14							
51								
52								
53								
54								
55								
56								
57								
58								
59								
60								
61								
62								
63								
64								
65								
66								
67								
68								
69								
70								
71								
72								
73								
74								
75								
76								
77								
78								
79								
80								
81								
82								
83								
84								
85								
86								
87								
88								
89								
90								
91								
92								
93								
94								
95								
96								
97								
98								
99								
100								
TOTAL IND.		↓		↓		↓		
TOTAL DEP.		←		←		←		
TOTAL CLAIMS								

\* MAY BE USED FOR ADDITIONAL CLAIMS OR ADMENDMENTS

FORM PTO-2022 (1-98)
U.S. DEPARTMENT OF COMMERCE  
Patent and Trademark Office



## UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
www.uspto.gov

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417

CONFIRMATION NO. 7632

## FORMALITIES LETTER



\*OC000000007542113\*

Orange & Chari  
66 Wellington Street West, Suite 4900  
P.O. Box 190  
Toronto, ON M5K 1H6  
CANADA

Date Mailed: 02/27/2002

## NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

*Filing Date Granted*

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(l) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.
- **The balance due by applicant is \$ 130.**

*A copy of this notice MUST be returned with the reply.*

Customer Service Center  
Initial Patent Examination Division (703) 308-1202

PART 3 - OFFICE COPY



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
www.uspto.gov

APPLICATION NUMBER	FILING/RECEIPT DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417

CONFIRMATION NO. 7632

FORMALITIES LETTER



\*OC000000007542113\*

Orange & Chari  
66 Wellington Street West, Suite 4900  
P.O. Box 190  
Toronto, ON M5K 1H6  
CANADA

Date Mailed: 02/27/2002

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

*Filing Date Granted*

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(l) of \$130 for a non-small entity, must be submitted with the missing items identified in this letter.
- The balance due by applicant is \$ 130.

*A copy of this notice MUST be returned with the reply.*

Customer Service Center  
Initial Patent Examination Division (703) 308-1202

PART 2 - COPY TO BE RETURNED WITH RESPONSE

03/28/2002 MBERHE 00000049 10025924

01 FC:105

130.00 0P

13 TP \$

<b>Response To Notice To File Missing Parts Of Application</b> <b>Filing Date Granted (PTO-1533)(Large Entity)</b>		Docket No. 00001-0417	
In Re Application Of: VANSTONE, Scott A. et al.			
Serial No. 10/025,924	Filing Date December 26, 2001	Examiner Not Yet Assigned	Group Art Unit 2131
Invention: <b>METHOD OF PUBLIC KEY GENERATION</b>			
<u>TO THE ASSISTANT COMMISSIONER FOR PATENTS:</u> <u>Box Missing Parts</u> <p>This is a response to the Notice to File Missing Parts of Application - Filing Date Granted (PTO-1533) mailed on <u>February 27, 2002</u>.</p> <p style="text-align: center;"><small>Date</small></p> <p>Enclosed herewith for filing are the following:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> A copy of the Notice to File Missing Parts of Application - Filing Date Granted (PTO-1533). <b>(REQUIRED)</b></li> <li><input checked="" type="checkbox"/> An oath or declaration in compliance with 37 CFR 1.63, including residence information and identifying the application by the above Application Number and Filing Date.</li> <li><input type="checkbox"/> A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date.</li> <li><input type="checkbox"/> An oath or declaration in compliance with 37 CFR 1.63 listing the names of all inventors and signed by the omitted inventor(s), identifying this application by the above Application Number and Filing Date.</li> <li><input type="checkbox"/> A verified English translation of the non-English language application papers as originally filed. It is requested that this translation be used as the copy for examination purposes in the United States Patent and Trademark Office.</li> <li><input type="checkbox"/> Other (list):</li> </ul> <div style="border: 1px solid black; height: 200px; width: 100%; margin-top: 10px;"></div>			

<b>Response To Notice To File Missing Parts Of Application</b> <b>Filing Date Granted (PTO-1533)(Large Entity)</b>			Docket No. 00001-0417
In Re Application Of: VANSTONE, Scott A. et al.			
Serial No. 10/025,924	Filing Date December 26, 2001	Examiner Not Yet Assigned	Group Art Unit 2131
Invention: <b>METHOD OF PUBLIC KEY GENERATION</b>			
<u>TO THE ASSISTANT COMMISSIONER FOR PATENTS:</u> <u>Box Missing Parts</u>			
<input checked="" type="checkbox"/> Completion of application fees as calculated below:			
<input type="checkbox"/> Utility application filing fee			
<input type="checkbox"/> Design application filing fee			
<input type="checkbox"/> Total number of independent claims = _____			
<input type="checkbox"/> Total number of claims = _____			
<input type="checkbox"/> Multiple dependent claims			
<input checked="" type="checkbox"/> Surcharge for late payment of filing fee and/or late filing of original declaration or oath			\$130.00
<input type="checkbox"/> Petition and fee for filing by other than all the inventors or a person not the inventor			
<input type="checkbox"/> Fee for processing an application filed with a non-English language specification			
<input type="checkbox"/> Fee for processing and retention of application			
Total completion of application fees			\$130.00
<p>This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a response to the above-identified Notice to File Missing Parts of Application. The requested extension is as follows (check time period desired). If an additional time extension is required, please consider this a petition therefor.</p> <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 45%;"> <input type="checkbox"/> One month    <input type="checkbox"/> Two months    <input type="checkbox"/> Three months    <input type="checkbox"/> Four months    <input type="checkbox"/> Five months </div> <div style="width: 50%;"> from: _____ until: _____  <div style="text-align: center; font-size: small;">Date Date</div> </div> </div> <div style="text-align: right; margin-top: 10px;"> Total time extension fees _____  Total fees due <b>\$130.00</b> </div>			

**Response To Notice To File Missing Parts Of Application  
Filing Date Granted (PTO-1533) (Large Entity)**

Docket No.  
00001-0417

In Re Application Of:

VANSTONE, Scott A. et al.

Serial No.  
10/025,924

Filing Date  
December 26, 2001

Examiner  
Not Yet Assigned

Group Art Unit  
2131

Invention:

**METHOD OF PUBLIC KEY GENERATION**

TO THE ASSISTANT COMMISSIONER FOR PATENTS:

Box Missing Parts

The fee of \$130.00 is to be paid as follows:

- ☒ A check in the amount of the fee is enclosed.
- ☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. 150633  
A duplicate copy of this sheet is enclosed.
- ☐ If an additional extension of time is required, please consider this a petition therefor and charge any additional fees which may be required to Deposit Account No.  
A duplicate copy of this sheet is enclosed.



Signature

Dated: March 25, 2002

Jeffrey Wong 46,414  
Orange & Chari  
Suite 4900, P.O. Box 190  
66 Wellington St. W.,  
Toronto, Ontario M5K 1H6  
CANADA

Tel.: (416) 601-8440 Fax: (416) 601-8454

CC:

I certify that this document and fee is being deposited on \_\_\_\_\_ with the U.S. Postal Service as first class mail under 37 C.F.R. 1.8 and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence


Docket No.  
00001-0417

113

# Declaration and Power of Attorney For Patent Application

## English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

### METHOD OF PUBLIC KEY GENERATION

the specification of which

(check one)

☐ is attached hereto.

☒ was filed on December 26, 2001 as United States Application No. or PCT International Application Number 10/025,924 and was amended on \_\_\_\_\_

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)			Priority Not Claimed
<u>2,329,590</u>	<u>Canada</u>	<u>27/12/2000</u>	<input type="checkbox"/>
(Number)	(Country)	(Day/Month/Year Filed)	
<u>                    </u>	<u>                    </u>	<u>                    </u>	<input type="checkbox"/>
(Number)	(Country)	(Day/Month/Year Filed)	
<u>                    </u>	<u>                    </u>	<u>                    </u>	<input type="checkbox"/>
(Number)	(Country)	(Day/Month/Year Filed)	



I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

_____	_____
(Application Serial No.)	(Filing Date)
_____	_____
(Application Serial No.)	(Filing Date)
_____	_____
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

_____	_____	_____
(Application Serial No.)	(Filing Date)	(Status)
		(patented, pending, abandoned)
_____	_____	_____
(Application Serial No.)	(Filing Date)	(Status)
		(patented, pending, abandoned)
_____	_____	_____
(Application Serial No.)	(Filing Date)	(Status)
		(patented, pending, abandoned)

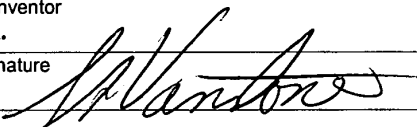
I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

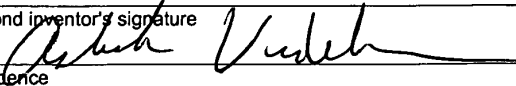
**POWER OF ATTORNEY:** As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*


**Orange & Chari (Customer No. 27,155)**

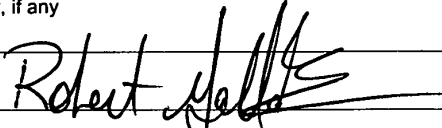
Send Correspondence to: **Orange & Chari**  
**Suite 4900, P.O. Box 190**  
**66 Wellington Street West**  
**Toronto, Ontario M5K 1H6 Canada**

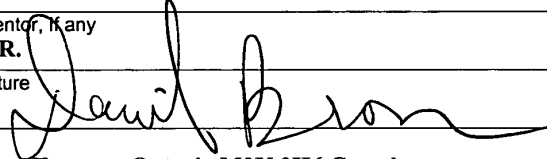
Direct Telephone Calls to: *(name and telephone number)*  
**John R.S. Orange (416)601-8440**

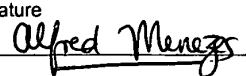
Full name of sole or first inventor <b>VANSTONE, Scott A.</b>	
Sole or first inventor's signature 	Date <b>Jan 25/2002</b>
Residence <b>10140 Pineview Trail, P.O. Box 490, Campbellville, Ontario L0P 1B0 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of second inventor, if any <b>VADEKAR, Ashok</b>	
Second inventor's signature 	Date <b>Jan 25/2002</b>
Residence <b>250 Harris Street, R.R. 4, Rockwood, Ontario N0B 2K0 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of third inventor, if any <b>LAMBERT, Robert J.</b>	
Third inventor's signature 	Date <b>Jan 25, 2002</b>
Residence <b>630 Holm Street, Cambridge, Ontario L5M 5N1 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of fourth inventor, if any <b>GALLANT, Robert P.</b>	
Fourth inventor's signature 	Date <b>Jan 30, 2002</b>
Residence <b>4788 Rosebush Road, Mississauga, Ontario L5M 5N1 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of fifth inventor, if any <b>BROWN, Daniel R.</b>	
Fifth inventor's signature 	Date <b>Jan 25/2002</b>
Residence <b>106 Banstock Drive, Toronto, Ontario M2K 2H6 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of sixth inventor, if any <b>MENEZES, Alfred</b>	Date <b>Jan 26/2002</b>
Sixth inventor's signature 	Date
Residence <b>1302-2267 Lakeshore Blvd. West Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

ATTORNEY DOCKET NO.: 00001-0417

**IN THE UNITED STATES PATENT & TRADEMARK OFFICE**

#4

The patent application of:

VANSTONE, Scott A. et al.

Serial No.: 10/025,924

Group Art Unit: 2131

Filed: December 26, 2001

Examiner: Unassigned

Title: METHOD OF PUBLIC KEY GENERATION

Assistant Commissioner for Patents  
Washington, D.C. 20231

RECEIVED

MAR 27 2002


Technology Center 2100

**PRIORITY CLAIM UNDER RULE 55**

Dear Sir:

The benefit of the filing date in Canada of a patent application corresponding to the above-identified application, is hereby claimed under 37 C.F.R. 1.55 and 35 U.S.C. § 119 in accordance with the Paris Convention for the Protection of Industrial Property. A certified copy of the corresponding Canadian Patent Application bearing Serial no. 2,329,590, filed December 27, 2000, is submitted herewith.

Respectfully submitted,

March 26/02  
Date  
\_\_\_\_\_  
Attorney for Applicant  
Registration No. 46414



Office de la propriété  
intellectuelle  
du Canada

Un organisme  
d'Industrie Canada

Canadian  
Intellectual Property  
Office

An Agency of  
Industry Canada



*Bureau canadien  
des brevets  
Certification*

*Canadian Patent  
Office  
Certification*

La présente atteste que les documents  
ci-joints, dont la liste figure ci-dessous,  
sont des copies authentiques des docu-  
ments déposés au Bureau des brevets.

This is to certify that the documents  
attached hereto and identified below are  
true copies of the documents on file in  
the Patent Office.

Specification and Drawings as originally filed with Application for Patent Serial No:  
2,329,590, on December 27, 2000, by CERTICOM CORP., assignee of Scott A.  
Vanstone, Ashok V. Vadekar, Robert J. Lambert, Robert P. Gallant, Daniel R. Brown and  
Alfred Menezes, for "Method of Public Key Generation".

RECEIVED

MAR 27 2002

Technology Center 2100

**CERTIFIED COPY OF  
PRIORITY DOCUMENT**

**FIED COPY OF  
ITY DOCUMENT**

Agent certificateur/Certifying Officer

March 22, 2002

Date

Canada

OPIC CIPO

MOBILEIRON, INC. - EXHIBIT 1003

Page 041

# **ABSTRACT**

A potential bias in the generation of a private key is avoided by selecting the key and comparing it against the system parameters. If a predetermined condition is attained it is accepted. If not it is rejected and a new key is generated.

## METHOD OF PUBLIC KEY GENERATION

### FIELD OF THE INVENTION

- 5 The present invention relates to public key cryptosystems and more particularly to key generation within such systems.

### BACKGROUND OF THE INVENTION

- 10 The basic structure of a public key cryptosystem is well known and has become ubiquitous with security in data communication systems. Such systems use a private key  $k$  and a corresponding public key  $\alpha^k$  where  $\alpha$  is a generator of the group. Thus one party may encrypt a message  $m$  with the intended recipients public key and the recipient may apply his private key to decrypt it.
- 15 Similarly, the cryptosystems may be used for key agreement protocols where each party exponentiates the other party's public key with their own private key. Thus party A will take B's public key  $\alpha^b$  and exponentiate it with A's private key  $a$  to obtain a session key  $\alpha^{ab}$ . Similarly, B will take A's public key  $\alpha^a$  and exponentiate it with B's private key  $b$  to obtain the same session key  $\alpha^{ab}$ . Thereafter data may be transferred using a symmetric key protocol utilizing the common
- 20 session key.

- Public key cryptosystems may also be used to sign messages to authenticate the author and/or the contents. In this case the sender will sign a message using his private key and a recipient can verify the message by applying the public key of the sender. If the received
- 25 message and the recovered message correspond then the authenticity is verified.

- The public key cryptosystems rely on the intractability of the discrete log problem in finite field arithmetic, that is even when the generator  $\alpha$  and public key is known, it is computationally infeasible to obtain the corresponding private key. The security of such systems
- 30 does therefore depend on the private key remaining secret. To mitigate the opportunity of disclosing the private key, protocols have been developed that use a pair of private keys and

corresponding public keys, referred to as long term and short term or ephemeral key pairs respectively. The ephemeral private key is generated at the start of each session between a pair of correspondents, usually by a random number generator. The corresponding ephemeral public key is generated and the resultant key pair used in one of the possible operations described above.

- 5 The long-term public key is utilized to authenticate the correspondent through an appropriate protocol. Once the session is terminated, the ephemeral key is securely discarded and a new ephemeral key generated for a new session.

- 10 Some of the more popular protocols for signature are the ElGamal family of signature schemes such as the Digital Signature Algorithm or DSA. The DSA algorithm utilizes both long term and ephemeral keys to generate a signature of the message. The DSA domain parameters are preselected. They consist of a prime number  $p$  of a predetermined length, by way of example 1024 bits; a prime number  $q$  of a predetermined bit length, by way of example 160 bits, where  $q$  divides  $p-1$ ; a generator  $\alpha$  lying between 2 and  $p-1$  and which satisfies the condition
  - 15  $(\alpha^q \bmod p) = 1$ , and; a cryptographic hash function  $H$ , such as SHA-1.

- 20 The DSA requires the signatory to select an ephemeral key  $k$  lying between 1 and  $q-1$ . A first signature component  $r$  is generated from the generator  $\alpha$  such that  $r = (\alpha^k \bmod p) \bmod q$ . A second signature component  $s$  is generated such that  $s = k^{-1}(H(m) + dr) \bmod q$ , and  $d$  is the long term private key of the signatory. The signature on the message  $m$  is  $(r,s)$ . The signature may be

- 25 verified by computing
 
$$H(m),$$

$$u_1 = s^{-1}H(m) \bmod q$$

$$u_2 = s^{-1}r \bmod q$$

$$v = \alpha^{u_1} \beta^{u_2} \bmod p, \text{ where } \beta = \alpha^d \bmod p \text{ is the long term public key of the signatory and}$$
- 30 finally verifying that  $r = v \bmod q$ . The use of both the ephemeral and long-term keys in the signature binds the identity of the signatory to the ephemeral key but does not render the long-term key vulnerable.

- 30 A similar signature protocol known as ECDSA may be used for elliptic curve cryptosystems. In this protocol  $k$  is selected in the interval 1 to  $n-1$  where  $n$  is an  $l$  bit prime. The signature component  $r$  is generated by converting the  $x$  coordinate of the public key  $kP$ , where  $P$



is the seed point on the curve, to an integer mod  $n$ , i.e.  $r = x_{kP} \bmod n$ . The component  $s = k^{-1}(H(m) + dr) \bmod n$  and the signature on the message  $m$  is  $(r, s)$ .

It will be apparent in ElGamal signature schemes such as the DSA and ECDSA, that if an  
 5 ephemeral key  $k$  and the associated message  $m$  and signature  $(r, s)$  is obtained it may be used to  
 yield the long term private key  $d$  and thereafter each of the ephemeral keys  $k$  can be obtained.  
 Neither the DSA nor the ECDSA inherently disclose any information about the public key  $k$ .  
 They both require the selection of  $k$  to be performed by a random number generator and it will  
 therefore have a uniform distribution throughout the defined interval. However the  
 10 implementation of the DSA may be done in such a way as to inadvertently introduce a bias in to  
 the selection of  $k$ . This small bias may be exploited to extract a value of the private key  $d$  and  
 thereafter render the security of the system vulnerable. One such implementation is the DSS  
 mandated by the National Institute of Standards and Technology (NIST) FIPS 186-2 Standard.  
 The DSS stipulates the manner in which an integer is to be selected for use as a private key. A  
 15 seed value,  $SV$ , is generated from a random number generator which is then hashed by a SHA-1  
 hash function to yield a bit string of predetermined length, typically 160 bits. The bit string  
 represents an integer between 0 and  $2^{160} - 1$ . However this integer could be greater than the prime  
 $q$  and so the DSS requires the reduction of the integer mod  $q$ , i.e.  $k = \text{SHA-1}(\text{seed}) \bmod q$ .

20 Accordingly the algorithm for selecting  $k$  may be expressed as :-

if  $\text{SHA-1}(\text{seed}) \geq q$  then  $k \leftarrow \text{SHA-1}(\text{seed}) - q$   
 else  $k \leftarrow \text{SHA-1}(\text{seed})$ .

With this algorithm it is to be expected that more values will lie in the first interval than the  
 second and therefore there is a potential bias in the selection of  $k$ .

25 Recent work by Daniel Bleichenbacher suggests that the modular reduction to obtain  $k$   
 introduces sufficient bias in to the selection of  $k$  that an examination of  $2^{22}$  signatures could yield  
 the private key  $d$  in  $2^{64}$  steps using  $2^{40}$  memory units. This suggests that there is a need for the  
 careful selection of the ephemeral key  $k$ .

30

## SUMMARY OF THE INVENTION

It is therefore an object of the present invention to obviate or mitigate the above disadvantages in the generation of a private key.

5

In general terms the present invention provides a key generation technique in which any bias is eliminated during the selection of the key.

## BRIEF DESCRIPTION OF THE DRAWINGS

10

Embodiments of the invention will now be described by way of example only with reference to the accompanying drawings in which:-

Figure 1 is a schematic representation of a data communication system;

15

Figure 2 is a flow chart showing a first embodiment of key generation;

Figure 3 is a flow chart showing a second embodiment;

20

Figure 4 is a flow chart showing a third embodiment;

Figure 5 is a flow chart showing a fourth embodiment;

Figure 6 is a flow chart showing a fifth embodiment; and

25

Figure 7 is a flow chart showing a sixth embodiment.

## DESCRIPTION OF THE PREFERRED EMBODIMENTS

30

Referring, therefore to figure 1, a data communication system 10 includes a pair of correspondents 12, 14 connected by a communication link 16. The link 16 may be a dedicated link, a multipurpose link such as a telephone connection or a wireless link depending on the particular applications. Similarly, the correspondents 12, 14 may be computer terminals, point-of-sale devices, automated teller machines, constrained devices such as PDA's, cellphones, pagers or any other device enabled for communication over a link 16.

35

Each of the correspondents 12, 14 includes a secure cryptographic function 20 including a secure memory 22, an arithmetic processor 24 for performing finite field operations, a random number generator 26 and a cryptographic hash function 28 for performing a secure cryptographic hash such as SHA-1. The output of the function 28 will be a bit string of predetermined length, typically 160 bits although other lengths such as 256, 384 or 512 are being used more frequently. It will be appreciated that each of these functions is controlled by a processor executing instructions to provide functionality and inter-operability as is well known in the art.

The secure memory 22 includes a register 30 for storing a long-term private key,  $d$ , and a register 32 for storing an ephemeral private key  $k$ . The contents of the registers 30, 32 may be retrieved for use by the processor 24 for performing signatures, key exchange and key transport functions in accordance with the particular protocols to be executed under control of the processor.

The long term private key,  $d$ , is generated and embedded at the time of manufacture or initialization of the cryptographic function and has a corresponding long-term public key  $\alpha^d$ . The long-term public key  $\alpha^d$  is stored in the memory 22 and is generally made available to other correspondents of the system 10.

The ephemeral key,  $k$ , is generated at each signature or other cryptographic exchange by one of the routines disclosed below with reference to figures 2 to 9. Once the key,  $k$ , and corresponding public key  $\alpha^k$  is generated, it is stored in the register 32 for use in the cryptographic protocol, such as the DSA or ECDSA described above.

Referring, therefore, to figure 2, a first method of generating a key,  $k$ , originates by obtaining a seed value (SV) from the random number generator 26. For the purposes of an example, it will be assumed that the cryptographic function is performed over a group of order  $q$ , where  $q$  is a prime represented as a bit string of predetermined length  $l$ . By way of example only it will be assumed that the length  $l$  is 160 bits, although, of course, other orders of the field may be used.

To provide a value of  $k$  of the appropriate order, the hash function 28 has an  $l$  bit output, e.g. a 160 bit output. The bit string generated by the random number generator 26 is greater than  $l$  bits and is therefore hashed by the function 28 to produce an output  $H(\text{seed})$  of  $l$  bits.

5

The resultant output  $H(\text{seed})$  is tested against the value of  $q$  and a decision made based on the relative values. If  $H(\text{seed}) < q$  then it is accepted for use as  $k$ . If not, the value is rejected and the random number generator is conditioned to generate a new value which is again hashed by the function 28 and tested. This loop continues until a satisfactory value is obtained.

10

A further embodiment is shown in figure 3. In this embodiment, the output of the random number generator 26 is hashed by hash function 28 as before and tested against the value of  $q$ . If the  $H(\text{seed})$  value is not accepted, the output of the random number generator 26 is incremented by a deterministic function and rehashed by function 28.

15

The resultant value  $H(\text{seed})$  is again tested and the procedure repeated until a satisfactory value of  $k$  is obtained.

The output may be incremented by adding a particular value to the seed value at each iteration, or may be incremented by applying a non-linear deterministic function to the seed value. For example, the output may be incremented by applying the function  $f(\text{seed}) = a.\text{seed}^2 + b \bmod 2^{160}$ , where  $a$  and  $b$  are integer constants.

20

A further embodiment is shown in figure 4 which has particular applicability to an elliptic curve cryptosystem. By way of example it will be assumed that a 163 bit string is required and that the output of the hash function 28 is 160 bits.

25

The random number generator 26 generates a seed value  $SV$  which is processed by the hash function 28 to obtain a first output  $H(\text{seed})$ .

30

The seed value SV is incremented by a selected function to provide a seed value SV+ which is further processed by the hash function 28 to provide a second output H(seed+).

5 The two outputs are then combined, typically by cocatenation, to produce a 320 bit string H(seed)/H(seed+). The excess bits, in this case 157 are rejected and the resultant value tested against the value of q. If the resultant value is less than q, it is accepted as the key k, if not the value is rejected.

10 Upon rejection, the random number generator may generate a new value as disclosed in figure 2 or may increment the seed value as disclosed in figure 3.

A further embodiment is shown in figure 5 which is similar to that of figure 4. In the embodiment of figure 5, the selection of the required l bit string is obtained by applying a l-bit wide masking window to the combined bit string.

15 This is tested against the value of q and if acceptable is used as the value of k. If it is not acceptable it is rejected and the l bit window incremented along the combined bit string to obtain a new value.

20 The values are tested and the window incremented until a satisfactory value is obtained.

A similar procedure may be used directly on an extended output of the hash function 28 as shown in figure 6 by applying a window to obtain the required l bit string. The bit string is tested against q and the window incremented until a satisfactory value of k is obtained.

25 As shown in figure 7, the value of k may be generated by utilizing a low Hamming weight integer obtained by combing the output of the random number generator 26 to facilitate computation of an intermediate public key  $\alpha^k$ . The integer is masked by combination with predetermined precomputed value k' to obtain the requisite Hamming weight for security. Such  
30 a procedure is disclosed in copending Canadian application 2,217,925. This procedure is modified to generate the low Hamming weight integer k as a bit string greater than l, for

example, a 180 bit string. The masking value  $k'$  is distributed throughout the 180 bit string and the resultant value reduced mod  $q$  to obtain a 163 bit value  $k''$ . Note that the value  $\alpha^{k''}$  can be efficiently computed by combining the precomputed value  $\alpha^{k'}$  with the efficiently computable value  $\alpha^k$ .

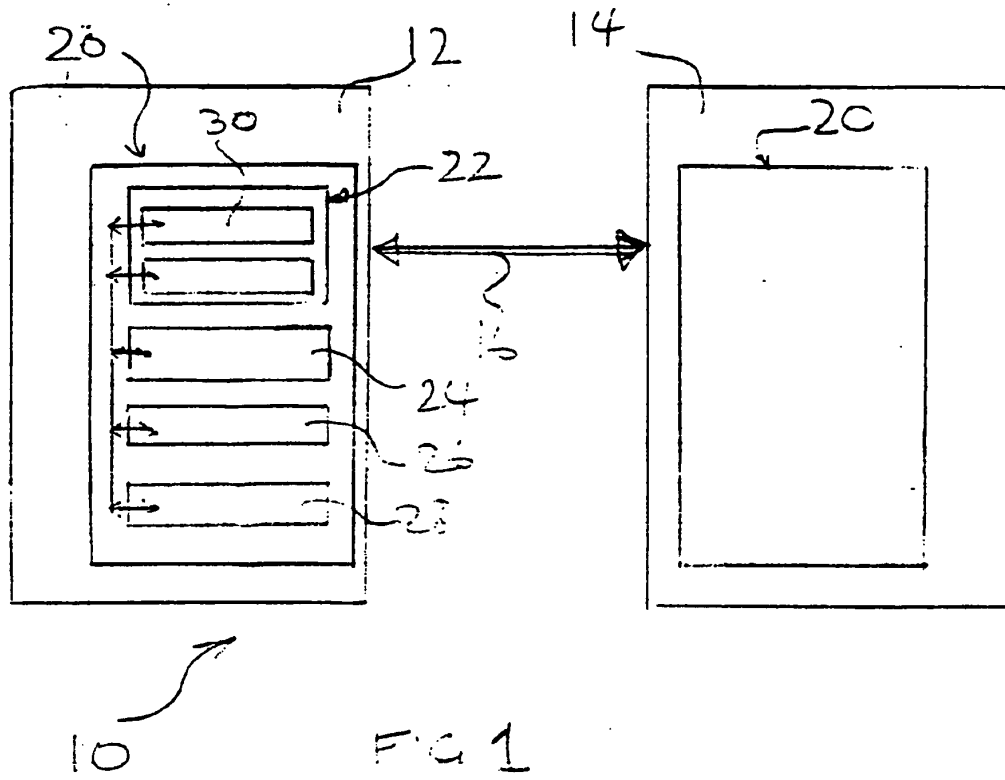
5

A similar technique may be used by relying on multiplicative masking. In this embodiment the value of  $k$  is combined with a value  $\beta$  where  $\beta = \alpha^u$ . The value of  $u$  is a secret value that is used to mask the low Hamming weight of  $k$ . Again, the values of  $u$  and the low Hamming weight number  $k$  can be chosen to have bit lengths greater than  $l$ , for example, bit lengths of 180. The resultant value is  $k'' = u^k \bmod q$ . It will be appreciated that  $\alpha^{k''}$  can be efficiently computed since  $\beta = \alpha^u$  is precomputed, and since  $k$  has low Hamming weight.

10

Although the invention has been described with reference to certain specific embodiments, various modifications thereof will be apparent to those skilled in the art without departing from the spirit and scope of the invention as outlined in the claims appended hereto.

15



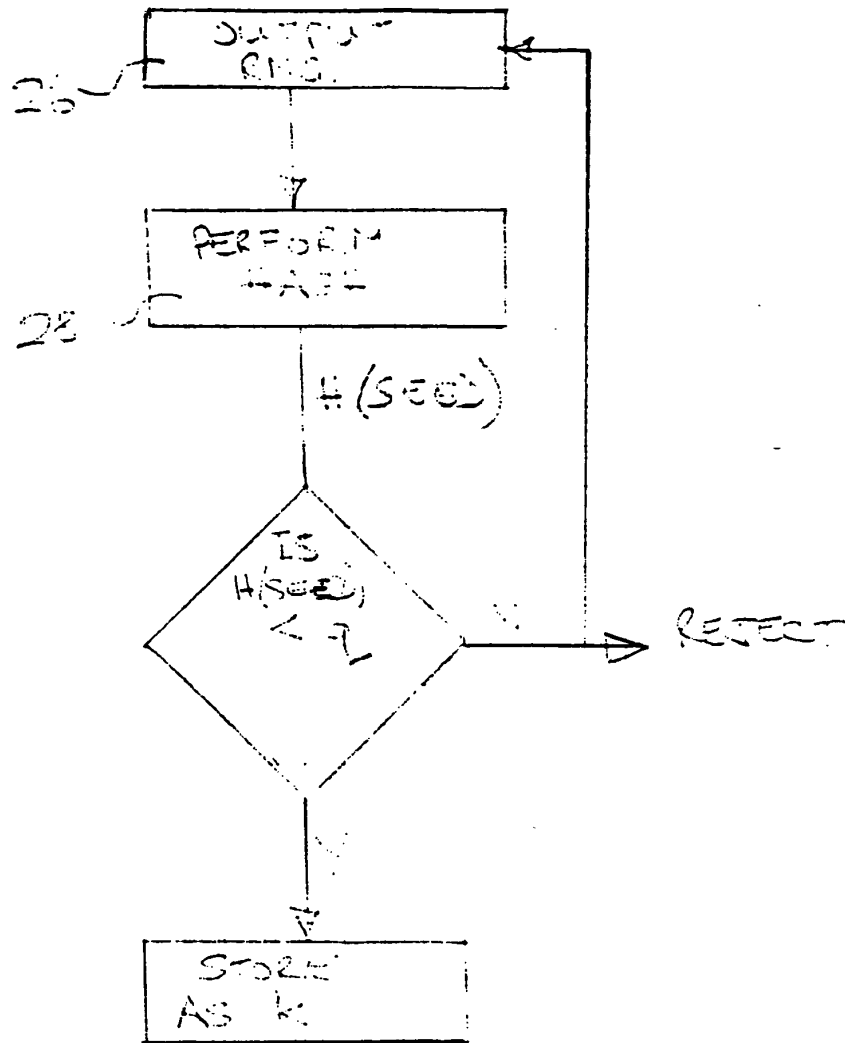
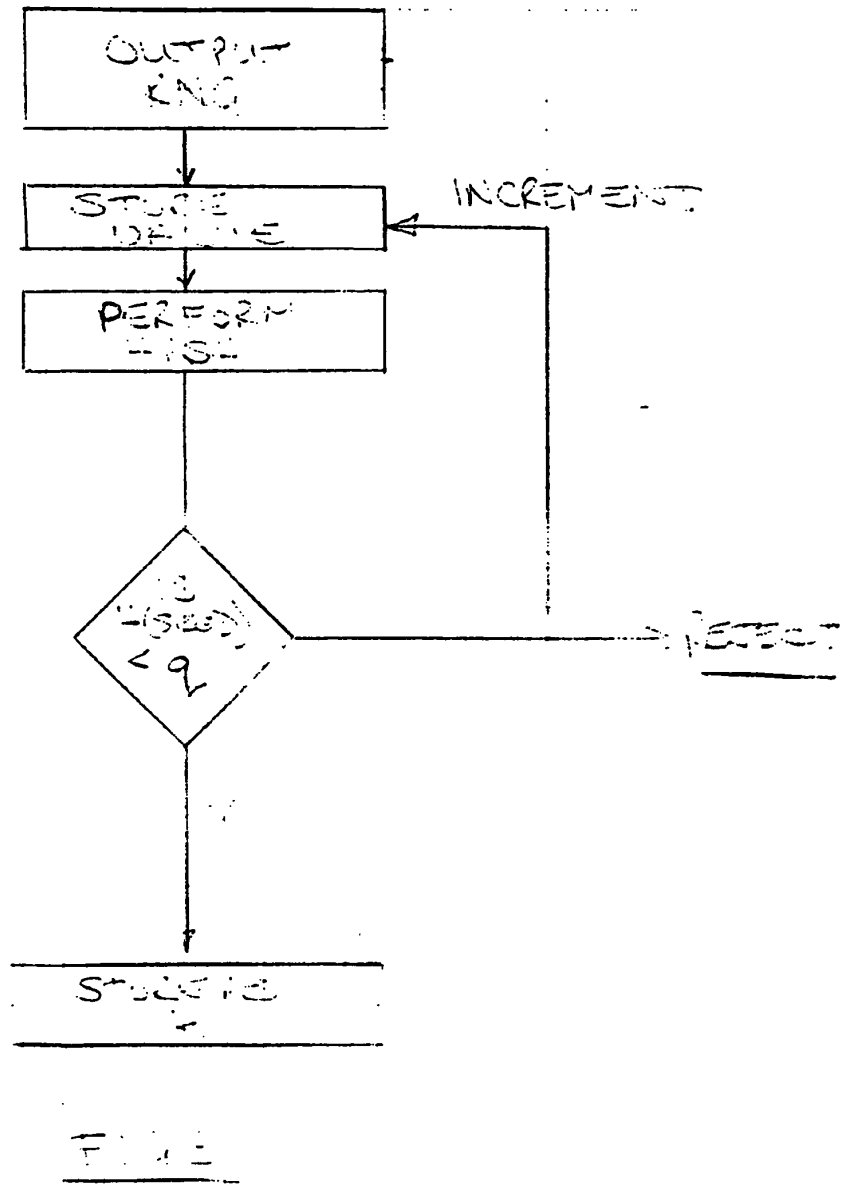


Fig 1





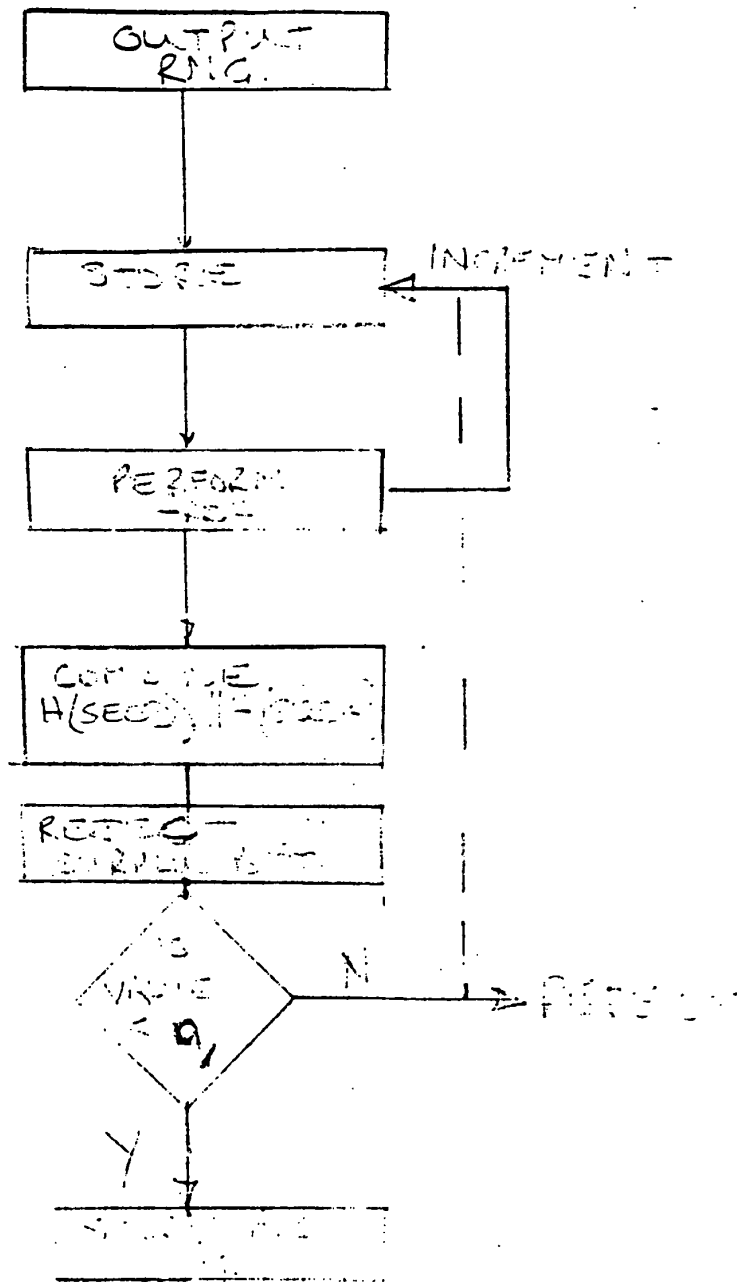


FIG 4

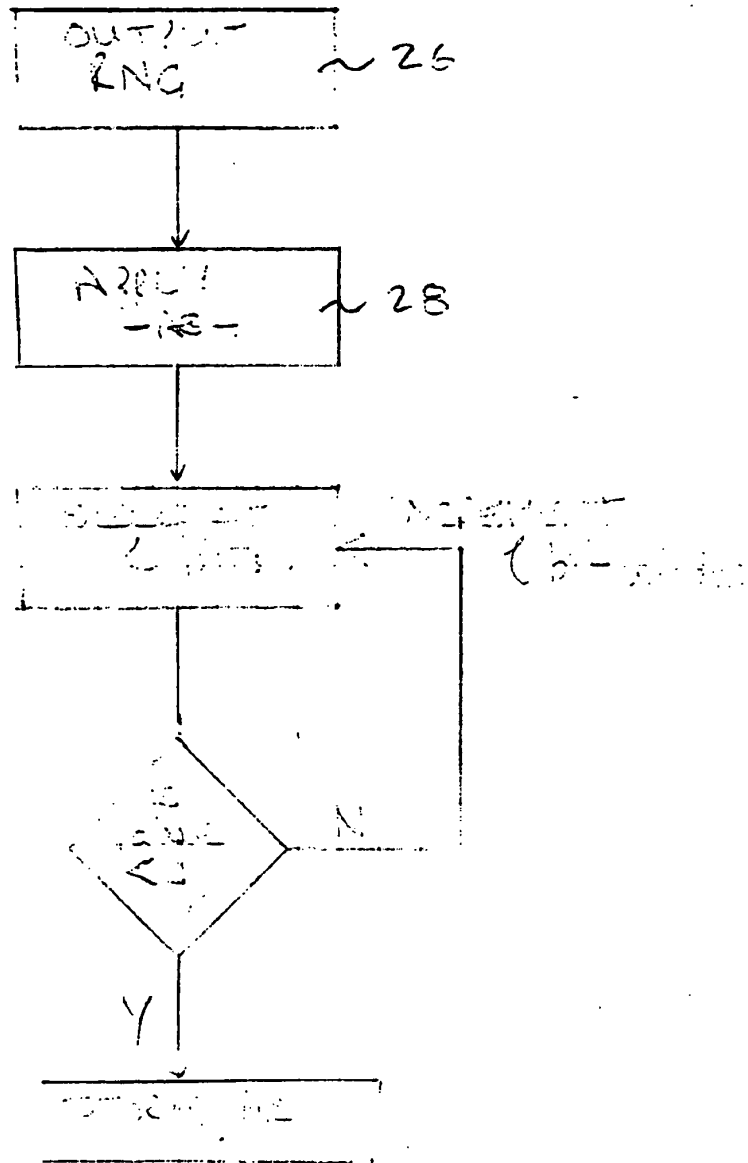
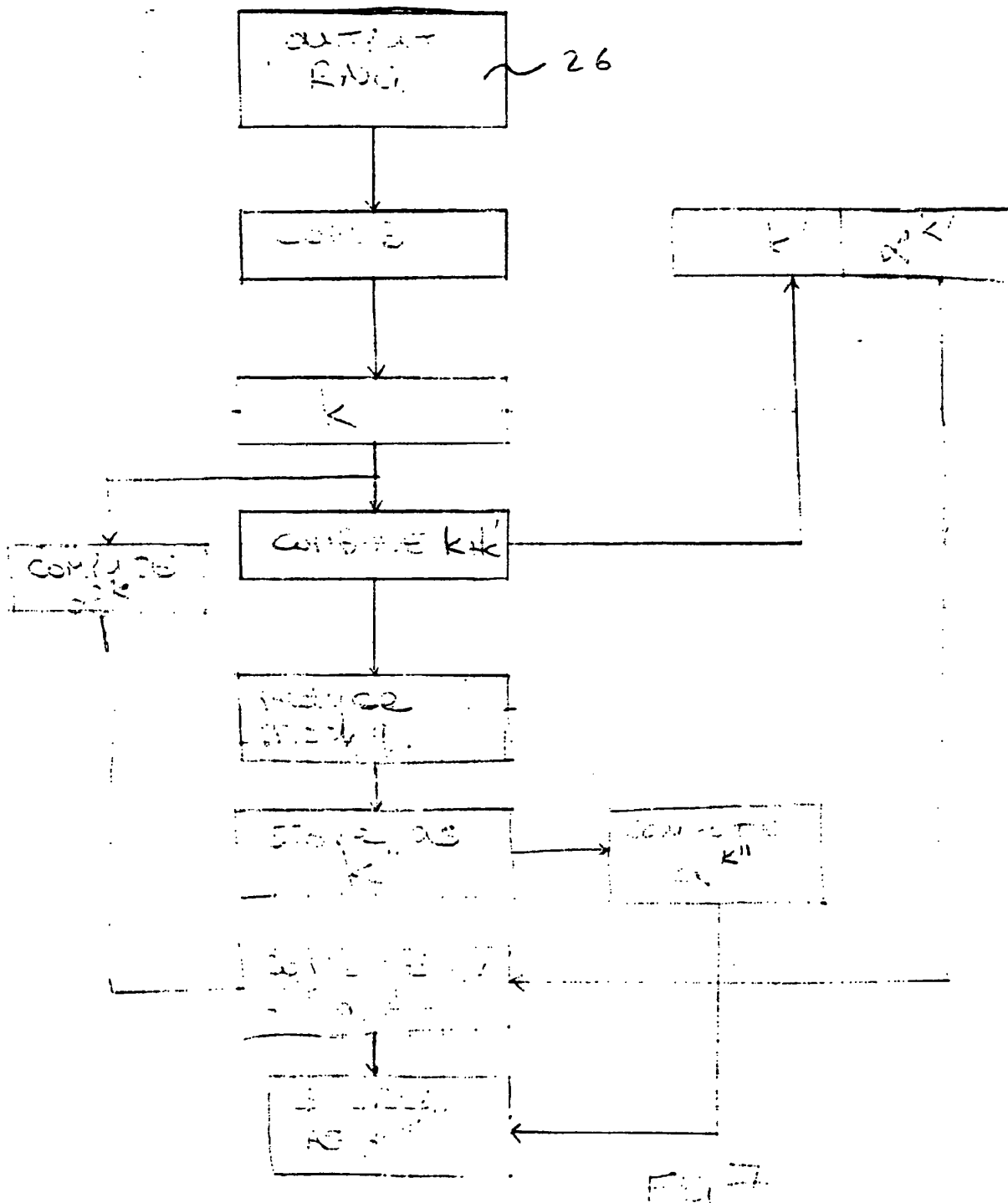


FIG. 5.



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

### **IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

PLUS Search Results for S/N 10025924, Searched March 03, 2005

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present. PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

6079018  
5910989  
6067621  
5953420  
5537475  
4995082  
6078909  
6307938  
6341349  
6345098  
6405923  
6151395  
5907618  
6058188  
6483921  
6108783  
5724279  
6240436  
6209016  
6212279  
6212279  
6282290  
6289454  
6473508  
6081598  
5867578  
5600725  
5955717  
6202933  
6131162  
6195433  
6275587  
5577123  
5963649  
4807287  
6490352  
5933503  
6213391  
6213391  
5606609  
6397329  
4935962  
6567832  
6745220  
6298153  
6173402  
6754820  
6279110  
5432852  
6212281

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	372	380/44.ccls. and @ad<"20001201"	US-PGPUB; USPAT	OR	ON	2005/03/01 10:12
S3	1	S1 and ((ephemeral adj2 key))	US-PGPUB; USPAT	OR	ON	2005/02/28 15:01
S4	410	380/277.ccls. and @ad<"20001201"	US-PGPUB; USPAT	OR	ON	2005/02/28 15:03
S5	280	331/78.ccls. and @ad<"20001201"	US-PGPUB; USPAT	OR	ON	2005/02/28 15:03
S6	274	708/250.ccls. and @ad<"20001201"	US-PGPUB; USPAT	OR	ON	2005/02/28 15:04
S8	6	"2217925"	US-PGPUB; USPAT	OR	ON	2005/02/28 15:42
S9	287	380/44.ccls. and @ad<"20001201" and (key with generat\$4)	US-PGPUB; USPAT	OR	ON	2005/02/28 16:30
S11	13	380/44.ccls. and @ad<"20001201" and (key with generat\$4) with (generat\$4 with (seed near3 (value or number)))	US-PGPUB; USPAT	OR	ON	2005/02/28 16:48
S12	1	("5963646").PN.	US-PGPUB; USPAT	OR	OFF	2005/02/28 16:34
S13	1	380/44.ccls. and @ad<"20001201" and (key with generat\$4) with (generat\$4 with (seed near3 (value or number))) with (hash\$4 or sha-1 or sha)	US-PGPUB; USPAT	OR	ON	2005/02/28 17:24
S14	14	380/44.ccls. and @ad<"20001201" and ((elgamal near3 signature) or dsa or ecdsa)	US-PGPUB; USPAT	OR	ON	2005/02/28 17:25
S16	287	380/44.ccls. and @ad<"20001201" and (generat\$4 with key)	US-PGPUB; USPAT	OR	ON	2005/02/28 17:28
S18	94	380/44.ccls. and @ad<"20001201" and (generat\$4 with key) with (random adj2 number)	US-PGPUB; USPAT	OR	ON	2005/02/28 17:28
S21	8	380/44.ccls. and @ad<"20001201" and (generat\$4 with key) with (random adj2 number) same (hash or md5 or sha-1 or sha)	US-PGPUB; USPAT	OR	ON	2005/02/28 17:45
S23	2	"380"/\$.ccls. and @ad<"20001201" and (generat\$4 with key) with (random adj2 number) same (hash or md5 or sha-1 or sha) with (prime adj2 (number or no))	US-PGPUB; USPAT	OR	ON	2005/02/28 17:45
S24	3	"380"/\$.ccls. and @ad<"20001201" and (generat\$4 with key) with (random adj2 number) same (hash or md5 or sha-1 or sha) same (prime adj2 (number or no))	US-PGPUB; USPAT	OR	ON	2005/02/28 17:45

Search History 3/4/05 12:48:56 PM Page 1  
C:\APPS\EAST\Workspaces\10025924.wsp

S25	9	"380"/\$.ccls. and (generat\$4 with key) with (random adj2 number) same (hash or md5 or sha-1 or sha) same (prime adj2 (number or no))	US-PGPUB; USPAT	OR	ON	2005/02/28 17:31
S26	2	380/44.ccls. and @ad<"20001201" and (ephemeral with key)	US-PGPUB; USPAT	OR	ON	2005/03/01 08:18
S27	24	"380"/\$.ccls. and @ad<"20001201" and (ephemeral with key)	US-PGPUB; USPAT	OR	ON	2005/03/01 10:36
S29	2	"380"/44.ccls. and @ad<"20001201" and (ecdsa)	US-PGPUB; USPAT	OR	ON	2005/03/01 08:22
S31	1	"380"/\$.ccls. and @ad<"20001201" and (generat\$4 near3 key) with (hash or digest or sha or sha-1) with (seed) with (random adj2 (number or no))	US-PGPUB; USPAT	OR	ON	2005/03/01 08:25
S32	1	(generat\$4 near3 key) with (hash or digest or sha or sha-1) with (seed) with (random adj2 (number or no)) and @ad<"20001201"	US-PGPUB; USPAT	OR	ON	2005/03/01 08:25
S33	5	(generat\$4 near3 key) with (hash or digest or sha or sha-1) same (random adj2 (number or no)) and @ad<"20001201" and 380/44.ccls.	US-PGPUB; USPAT	OR	ON	2005/03/01 08:32
S34	36	(generat\$4 near3 key) with (hash or digest or sha or sha-1) same (random adj2 (number or no)) and @ad<"20001201" and "380"/\$.ccls.	US-PGPUB; USPAT	OR	ON	2005/03/01 08:39
S35	2	(generat\$4 near3 key) with (hash or digest or sha or sha-1) same (random adj2 (number or no)) same prime and @ad<"20001201" and "380"/\$.ccls.	US-PGPUB; USPAT	OR	ON	2005/03/01 08:44
S36	2	(generat\$4 near3 key) with (hash or digest or sha or sha-1) same (random adj2 (number or no)) same prime and @ad<"20001201"	US-PGPUB; USPAT	OR	ON	2005/03/01 08:44
S37	2	(generat\$4 near3 key) with (hash or digest or sha or sha-1) same (random adj2 (number or no)) same prime and @ad<"20001201"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/01 08:45
S38	4	(generat\$4 near3 key) same (hash or digest or sha or sha-1) same (random adj2 (number or no)) same prime and @ad<"20001201"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/01 08:47



S41	9	(dsa or ecdsa or "elliptic curve digital signature algorithm" or "digital signature algorithm") and 380/44.ccls. and @ad<"20001201"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/01 08:59
S42	2	(dsa or ecdsa or "elliptic curve digital signature algorithm" or "digital signature algorithm") same (generat\$4 near3 key) and 380/44.ccls. and @ad<"20001201"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/01 08:51
S44	235	(generat\$4 with random) and 380/44.ccls. and @ad<"20001201"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/01 09:01
S45	16	(generat\$4 with random) with (hash or sha or sha-1 or digest) and 380/44.ccls. and @ad<"20001201"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/01 09:01
S46	3	(generat\$4 with random) with (hash or sha or sha-1 or digest) same prime and 380/44.ccls. and @ad<"20001201"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/01 09:30
S47	17	elgamal and 380/44.ccls. and @ad<"20001201"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/01 09:30
S48	13	380/44.ccls. and @ad<"20001201" and (dsa or dss or "digital signature algorithm")	US-PGPUB; USPAT	OR	ON	2005/03/01 10:14
S49	14	380/44.ccls. and @ad<"20001201" and (dsa or dss or "digital signature algorithm" or "digital signature standard")	US-PGPUB; USPAT	OR	ON	2005/03/01 10:26
S52	13	"fips-186"	US-PGPUB; USPAT	OR	ON	2005/03/01 10:27
S53	565	"380"/\$.ccls. and @ad<"20001201" and (generat\$4 near3 (public adj2 key))	US-PGPUB; USPAT	OR	ON	2005/03/01 10:36
S54	54	"380"/44.ccls. and @ad<"20001201" and (generat\$4 near3 (public adj2 key))	US-PGPUB; USPAT	OR	ON	2005/03/01 10:36

S55	2	"380"/44.ccls. and @ad<"20001201" and (generat\$4 near3 (public adj2 key)) with seed	US-PGPUB; USPAT	OR	ON	2005/03/01 10:36
S57	1	"380"/44.ccls. and @ad<"20001201" and (generat\$4 near3 (public adj2 key)) same random same hash	US-PGPUB; USPAT	OR	ON	2005/03/01 10:37
S58	21	"380"/44.ccls. and @ad<"20001201" and (generat\$4 near3 (public adj2 key)) same random	US-PGPUB; USPAT	OR	ON	2005/03/01 10:39
S59	1	"380"/44.ccls. and @ad<"20001201" and (generat\$4 near3 (public adj2 key)) same random same hash	US-PGPUB; USPAT	OR	ON	2005/03/01 10:40
S60	16	"380"/\$.ccls. and @ad<"20001201" and (generat\$4 near3 (public adj2 key)) same random same hash	US-PGPUB; USPAT	OR	ON	2005/03/01 11:06
S61	4	((("5214703") or ("6490680") or ("6128737") or ("6195433"))).PN.	US-PGPUB; USPAT	OR	OFF	2005/03/01 11:07
S62	545	"380"/\$.ccls. and (increment\$4 or increas\$4 or add\$4) with ((seed adj2 value) or (random adj2 (no or number)))	US-PGPUB; USPAT	OR	ON	2005/03/04 10:03
S63	44	"380"/44.ccls. and (increment\$4 or increas\$4 or add\$4) with ((seed adj2 value) or (random adj2 (no or number)))	US-PGPUB; USPAT	OR	ON	2005/03/04 10:06
S64	1	"380"/44.ccls. and (increment\$4 or increas\$4 or add\$4) with ((seed adj2 value) or (random adj2 (no or number))) same (perform\$4 near3 (hash or digest or sha or sha-1))	US-PGPUB; USPAT	OR	ON	2005/03/04 10:04
S65	4	"380"/44.ccls. and (increment\$4 or increas\$4 or add\$4) with ((seed adj2 value) or (random adj2 (no or number))) and (perform\$4 near3 (hash or digest or sha or sha-1))	US-PGPUB; USPAT	OR	ON	2005/03/04 10:04
S66	6	"380"/44.ccls. and (increment\$4 or increas\$4 or add\$4) with ((seed adj2 value) or (random adj2 (no or number))) same (combin\$4 or join\$4)	US-PGPUB; USPAT	OR	ON	2005/03/04 10:28
S67	44	"380"/44.ccls. and (increment\$4 or increas\$4 or add\$4) with ((seed adj2 value) or (random adj2 (no or number)))	US-PGPUB; USPAT	OR	ON	2005/03/04 10:29
S68	16	"380"/44.ccls. and (increment\$4 or increas\$4 ) with ((seed adj2 value) or (random adj2 (no or number)))	US-PGPUB; USPAT	OR	ON	2005/03/04 11:30

S69	8	"380"/44.ccls. and (increment\$4) with ((seed adj2 value) or (random adj2 (no or number)))	US-PGPUB; USPAT	OR	ON	2005/03/04 11:32
S70	28	(increment\$4) adj ((seed adj2 value) or (random adj2 (no or number)))	US-PGPUB; USPAT	OR	ON	2005/03/04 11:32



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632
7590	03/24/2005		EXAMINER	
Orange & Chari 66 Wellington Street West, Suite 4900 P.O. Box 190 Toronto, ON M5K 1H6 CANADA			GELAGAY, SHEWAYE	
			ART UNIT	PAPER NUMBER
			2133	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/025,924

Applicant(s)

VANSTONE ET AL.

Examiner

Shewaye Gelagay

Art Unit

2133

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on December 26, 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
  - 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26 December 2001 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.
  - Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
  - Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority-under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☒ All b) ☐ Some \* c) ☐ None of:
    - 1. ☒ Certified copies of the priority documents have been received.
    - 2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    - 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. Claims 1-14 have been examined.

#### ***Oath/Declaration***

2. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because: It is not signed by the inventors.

#### ***Drawings***

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: On Page 4, line 31 and Page 5, line 19, "a system 10". Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner,

the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: On Page 4, line 33, "a communication link 16". Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-2 and 4-5 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier "Applied Cryptography", (Pages 483-490).

As per claim 1:

Schneier teaches a method of generating a key over a group of order  $q$ , said method including the steps of:

generating a seed value from a random number generator; (Page 487, line 11; Page 489, lines 15-16)

performing a hash function on said seed number to provide an output; (Page 487, lines 7-8; Page 489, lines 17-18)

determining whether said output is less than said prime number  $q$ ; (Page 487, line 11; ... $k$  less than  $q$ )

accepting said output for use as a key if the value thereof is less than said prime number  $q$ ; (Page 487, lines 12-15) and

rejecting said output as a key if said value is not less than said order  $q$ . (Page 487, line 11)

As per claim 2:

Schneier teaches all the subject matter as discussed above. In addition, Schneier further discloses a method wherein another seed value is generated by said random number generator if said output is rejected. (Page 487, line 11; Page 489, line 22)

As per claim 4:

Schneier teaches all the subject matter as discussed above. In addition, Schneier further discloses a method wherein said key is used for generation of a public key. (Page 487, lines 8-15; Page 488, line 3-8)

As per claim 5:



Schneier teaches all the subject matter as discussed above. In addition, Schneier further discloses a method wherein said order  $q$  is prime number represented by a bit string of predetermined length  $l$ . (Page 487, line 1 and Page 488, line 5)

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Backal United States Letter Patent Number 6,219,421.

As per claim 7:

Schneier teaches all the subject matter as discussed above. Schneier does not explicitly disclose a method wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

Backal in analogous art, however, disclose a method wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key. (Col. 5, lines 61-67)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method of wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Backal (Col. 1, lines 50-51) in order to provide an exceptional degree of security. This way, the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document.

As per claim 8:

Schenier and Backal teach all the subject matter as discussed above. In addition, Backal further discloses a method wherein said step of incrementing includes a further step of adding a particular value to said seed value. (Col. 5, lines 61-67)

As per claim 9:

Schneier teaches a method of generating a key over a group of order  $q$ , said method including the steps of:

generating a seed value from a random number generator; (Page 487, line 11; Page 489, lines 15-16)

performing a hash function on said seed number to provide a first output; (Page 487, lines 7-8; Page 489, lines 17-18)

accepting said new output as a key  $k$  if said new output has a value less than order  $q$ ; (Page 487, line 11; ... $k$  less than  $q$ ) and

rejecting said new output as a key if said new output has a value less than order  $q$ . (Page 487, line 11)

Schneier does not explicitly disclose a method of incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ .

Backal in analogous art, however, disclose a method of

incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; (Col. 5, lines 61-67) and

combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ ; (Col. 5, lines 54-60)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method of incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Backal (Col. 1, lines 50-51) in order to provide an exceptional degree of security. This way, the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document.

As per claim 10:

Schenier and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein upon rejection of said new output a new seed value is generated by said random number generator. (Page 487, line 11; Page 489, line 22)

As per claim 11:

Schenier and Backal teach all the subject matter as discussed above. In addition, Backal further discloses a method wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained. (Col. 5, lines 61-67)

As per claim 12:

Schenier and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein a bit string greater than a predetermined length  $l$  is obtained and an  $l$  bit string selected therefrom for comparison with said order  $q$ . (Page 487, line 1 and Page 488, line 5)

As per claim 13:

Schenier and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein upon rejection of said bit string of predetermined length  $l$ , a further  $l$  bit string is selected. (Page 487, line 1 and Page 488, line 5)

9. Claims 3 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Nel et al. "Generatiion of Keys for use with the Digital Signature Standard (DSS)" (Pages 6-10).

As per claim 3:

Schneier teaches all the subject matter as discussed above. Both references do not explicitly disclose a method wherein the step of accepting said output as a key includes a further step of storing said key.

Nel et al. in analogous art, however, discloses a method wherein the step of accepting said output as a key includes a further step of storing said key. (Page 10, Col. 1, lines 3-4)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method wherein the step of accepting said output as a key includes a further step of storing said key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to be able to reuse the key and also to perform auditing on the key generation process.

As per claim 6:

Schneier teaches all the subject matter as discussed above. Schneier does not explicitly disclose a method wherein said output from said hash function is a bit string of predetermined length *l*.

Nel et al. in analogous art, however, discloses a method wherein said output from said hash function is a bit string of predetermined length *l*. (Page 8, Col. 2, lines 8-11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method wherein said output from said hash function is a bit string of predetermined length *l*. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Nel

et al. (Page 8, Col. 2, lines 6-7) in order to prevent constructing a message which will yield a known value of message digest.

10. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Backal United States Letter Patent Number 6,219,421 and further in view of Nel et al. "Generatiion of Keys for use with the Digital Signature Standard (DSS)" (Pages 6-10).

As per claim 14:

Schenier and Backal teach all the subject matter as discussed above. Both references do not explicitly disclose method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $l$ .

Nel et al. in analogous art, however, discloses a method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $l$ . (Page 8, Col. 2, lines 8-11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $l$ . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Nel et al. (Page 8, Col. 2, lines 6-7) in order to prevent constructing a message which will yield a known value of message digest.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 571-272-3819. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay  
Examiner  
Art Unit 2133

03/04/05

  
ALBERT DECADY  
SUPERVISORY PATENT EXAMINER  
TECNOLOGY CENTER 2100



<b>Notice of References Cited</b>	Application/Control No. 10/025,924	Applicant(s)/Patent Under Reexamination VANSTONE ET AL.	
	Examiner Shewaye Gelagay	Art Unit 2133	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,219,421	04-2001	Backal, Shaul O.	380/28
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			


**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Schneier, Bruce, "Applied Cryptography", 1996, John Wiley & Sons, Inc., 2nd edition, Pages 483-490.
	V	Nel et al., "Generation of Keys for use with the Digital Signature Standard (DSS)", 1993, IEEE, Pages 6-10
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b>Search Notes</b> 	<b>Application No.</b> 10/025,924 <b>Examiner</b> Shewaye Gelagay	<b>Applicant(s)</b> VANSTONE ET AL. <b>Art Unit</b> 2133
--	--	---


  

SEARCHED			
Class	Subclass	Date	Examiner
380	44	3/4/2005	SG
380	277	3/4/2005	SG
708	250	3/4/2005	SG

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
East Searched	3/4/2005	sg
ACM searched (incrementing seed value)	3/4/2005	SG
IEEE searched (increment and combine seed value)	3/4/2005	SG

<b>Index of Claims</b> 	<b>Application No.</b>		<b>Applicant(s)</b>	
	10/025,924		VANSTONE ET AL.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Shewaye Gelagay		2133	

✓	Rejected
=	Allowed

—	(Through numeral) Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claim		Date											
Final	Original												
	1	✓											
	2	✓											
	3	✓											
	4	✓											
	5	✓											
	6	✓											
	7	✓											
	8	✓											
	9	✓											
	10	✓											
	11	✓											
	12	✓											
	13	✓											
	14	✓											
	15												
	16												
	17												
	18												
	19												
	20												
	21												
	22												
	23												
	24												
	25												
	26												
	27												
	28												
	29												
	30												
	31												
	32												
	33												
	34												
	35												
	36												
	37												
	38												
	39												
	40												
	41												
	42												
	43												
	44												
	45												
	46												
	47												
	48												
	49												
	50												

Claim		Date											
Final	Original												
	51												
	52												
	53												
	54												
	55												
	56												
	57												
	58												
	59												
	60												
	61												
	62												
	63												
	64												
	65												
	66												
	67												
	68												
	69												
	70												
	71												
	72												
	73												
	74												
	75												
	76												
	77												
	78												
	79												
	80												
	81												
	82												
	83												
	84												
	85												
	86												
	87												
	88												
	89												
	90												
	91												
	92												
	93												
	94												
	95												
	96												
	97												
	98												
	99												
	100												

Claim		Date											
Final	Original												
	101												
	102												
	103												
	104												
	105												
	106												
	107												
	108												
	109												
	110												
	111												
	112												
	113												
	114												
	115												
	116												
	117												
	118												
	119												
	120												
	121												
	122												
	123												
	124												
	125												
	126												
	127												
	128												
	129												
	130												
	131												
	132												
	133												
	134												
	135												
	136												
	137												
	138												
	139												
	140												
	141												
	142												
	143												
	144												
	145												
	146												
	147												
	148												
	149												
	150												



## UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
WASHINGTON, D.C. 20231  
www.uspto.gov



Bib Data Sheet

CONFIRMATION NO. 7632

<b>SERIAL NUMBER</b> 10/025,924	<b>FILING DATE</b> 12/26/2001 <b>RULE</b>	<b>CLASS</b> 380	<b>GROUP ART UNIT</b> 2131 2133	<b>ATTORNEY DOCKET NO.</b> 00001-0417
<b>APPLICANTS</b> Scott A. Vanstone, Campbellville, CANADA; Ashok Vadekar, Rockwood, CA; Robert J. Lambert, Cambridge, CANADA; Robert P. Gallant, Mississauga, CANADA; Daniel R. Brown, Toronto, CANADA; Alfred Menezes, West Canada, CANADA;				
<b>** CONTINUING DATA *****</b> SG 3/4/05 <b>** FOREIGN APPLICATIONS *****</b> SG 3/4/05 CANADA 2,329,590 12/27/2000				
<b>IF REQUIRED, FOREIGN FILING LICENSE GRANTED</b> <b>** 02/25/2002</b>				
Foreign Priority claimed <input type="checkbox"/> yes <input checked="" type="checkbox"/> no 35 USC 119 (a-d) conditions <input type="checkbox"/> yes <input checked="" type="checkbox"/> no <input type="checkbox"/> Met after met <input type="checkbox"/> Allowance		<b>STATE OR COUNTRY</b> CANADA	<b>SHEETS DRAWING</b> 7	<b>TOTAL CLAIMS</b> 14
Verified and Acknowledged Examiner's Signature <i>Shawna Gelagay</i> Initials <i>SG</i>		<b>INDEPENDENT CLAIMS</b> 2		
<b>ADDRESS</b> AIR MAIL Orange & Chari 66 Wellington Street West, Suite 4900 P.O. Box 190 Toronto, ON M5K 1H6 CANADA				
<b>TITLE</b> Method of public key generation				
<b>FILING FEE RECEIVED</b> 870	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees ( Filing ) <input type="checkbox"/> 1.17 Fees ( Processing Ext. of time ) <input type="checkbox"/> 1.18 Fees ( Issue ) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit	

Appl. No. 10/025,924  
Reply to Office Action of: March 24, 2005



**IN THE UNITED STATES PATENT & TRADEMARK OFFICE**

Appl. No.: 10/025,924  
Applicant: VANSTONE, Scott et al  
Filed: December 26, 2001  
Title: METHOD OF PUBLIC KEY GENERATION  
Art Unit: 2133  
Examiner: GELAGAY, Shewaye  
Docket No.: 67539/00421

Mail Stop Amendment  
U.S. Patent & Trademark Office  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**RESPONSE**

Sir:

This is further to the Office Action dated March 24, 2005. Applicant advises that a petition for a 3-month extension of time is being filed contemporaneously herewith. Applicant wishes to amend the above-identified application as follows:

**Amendments to the Specification:** begin on page 2 of this paper.

**Amendments to the Claims:** are reflected in the listing of claims which begins on page 5 of this paper.

**Amendments to the Drawings:** begin on page 8 of this paper and include an attached replacement sheet containing an amended Figure 1.

**Remarks:** begin on page 9 of this paper.

**BEST AVAILABLE COPY**

**Amendments to the Specification**

Please replace paragraph [0001] with the following replacement paragraph:

[0001] The present invention relates to public key cryptosystems and more particularly to key generation within such systems.

Please replace paragraph [0033] with the following replacement paragraph:

[0033] Referring, therefore, to FIG. 2, a first method of generating a key,  $k$ , originates by obtaining a seed value (SV) from the random number generator 26. For the purposes of an example, it will be assumed that the cryptographic function is performed over a group of order  $q$ , where  $q$  is a prime represented as a bit string of predetermined length  $L$ . By way of example only it will be assumed that the length  $L$  is 160 bits, although, of course, other orders of the field may be used.

Please replace paragraph [0034] with the following replacement paragraph:

[0034] To provide a value of  $k$  of the appropriate order, the hash function 28 has an  $L$  bit output, e.g. a 160 bit output. The bit string generated by the random number generator 26 is greater than  $L$  bits and is therefore hashed by the function 28 to produce an output  $H(\text{seed})$  of  $L$  bits.

Please replace paragraph [0044] with the following replacement paragraph:

[0044] A further embodiment is shown in FIG. 5 which is similar to that of FIG. 4. In the embodiment of FIG. 5, the selection of the required  $L$  bit string is obtained by applying a  $L$ -bit wide masking window to the combined bit string.

Please replace paragraph [0045] with the following replacement paragraph:

**BEST AVAILABLE COPY**

[0045] This is tested against the value of  $q$  and if acceptable is used as the value of  $k$ . If it is not acceptable it is rejected and the  $[[1]]$   $L$  bit window incremented along the combined bit string to obtain anew value.

Please replace paragraph [0047] with the following replacement paragraph:

[0047] A similar procedure may be used directly on an extended output of the hash function 28 as shown in FIG. 6 by applying a window to obtain the required  $[[1]]$   $L$  bit string. The bit string is tested against  $q$  and the window incremented until a satisfactory value of  $k$  is obtained.

Please replace paragraph [0048] with the following replacement paragraph:

[0048] As shown in FIG. 7, the value of  $k$  may be generated by utilizing a low Hamming weight integer obtained by ~~combine~~ combining the output of the random number generator 26 to facilitate computation of an intermediate public key  $\alpha^k$ . The integer is masked by combination with predetermined precomputed value  $k'$  to obtain the requisite Hamming weight for security. Such a procedure is disclosed in copending Canadian application 2,217,925. This procedure is modified to generate the low Hamming weight integer  $k$  as a bit string greater than  $[[1]]$   $L$ , for example a 180 bit string. The masking value  $k'$  is distributed throughout the 180 bit string and the resultant value reduced mod  $q$  to obtain a 163 bit value  $k''$ . Note that the value  $\alpha^{k''}$  can be efficiently computed by combining the precomputed value  $[[\alpha']]$   $\alpha$  with the efficiently computable value  $\alpha^k$ .

Please replace paragraph [0049] with the following replacement paragraph:

[0049] A similar technique may be used by relying on multiplicative masking. In this embodiment the value of  $k$  is combined with a value  $\beta$  where  $\beta = \alpha^u$ . The value of  $u$  is a secret value that is used to mask the low Hamming weight of  $k$ . Again, the values of  $u$  and the low Hamming weight number  $k$  can be chosen to have bit lengths greater than  $[[1]]$   $L$ , for example, bit lengths of 180. The resultant value is  $k'' = u^k \bmod q$ . It will be appreciated that  $\alpha^{k''}$  can be

BEST AVAILABLE COPY

SEP. 22. 2005 3:08PM

NO. 0354 P. 7

Appl. No. 10/025,924

Page 4

Reply to Office Action of: March 24, 2005

efficiently computed since  $\beta = \alpha^n$  is precomputed, and since  $k$  has low Hamming weight.

BEST AVAILABLE COPY



**Amendments to the Claims**

This listing of claims will replace all prior versions and listings of claims in the application:

**Listing of claims:**

1. (currently amended) A method of generating a key over a group of order  $q$ , said method including the steps of:
  - generating a seed value from a random number generator;
  - performing a hash function on said seed number value to provide an output;
  - determining whether said output is less than said prime number  $q$ ;
  - accepting said output for use as a key if the value thereof is less than said prime number  $q$ ; and
  - rejecting said output as a key if said value is not less than said order  $q$ .
2. (original) The method of claim 1 wherein another seed value is generated by said random number generator if said output is rejected.
3. (original) The method of claim 1 wherein the step of accepting said output as a key includes a further step of storing said key.
4. (original) The method of claim 1 wherein said key is used for generation of a public key.
5. (currently amended) The method of claim 1 wherein said order  $q$  is prime number represented by a bit string of predetermined length  $[[1]] \underline{L}$ .
6. (currently amended) The method of claim 5 wherein said output from said hash function is a bit string of predetermined length  $[[1]] \underline{L}$ .
7. (original) The method of claim 1 wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as

BEST AVAILABLE COPY

a key.

8. (original) The method of claim 7, wherein said step of incrementing includes a further step of adding a particular value to said seed value.

9. (currently amended) A method of generating a key over a group of order  $q$ , said method including the steps of:

- generating a seed value from a random number generator;
- performing a hash function on said seed number to provide a first output;
- incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output;
- combining said first output and second output to produce a new output;
- determining whether said new output has a value less than said order  $q$ ;
- accepting said new output as a key  $k$  if said new output has a value less than order  $q$ ; and
- rejecting said new output as a key if said new output has a value less than order  $q$ .

10. (original) The method of claim 9 wherein upon rejection of said new output a new seed value is generated by said random number generator.

11. (original) The method of claim 9 wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained.

12. (currently amended) The method of claim 9 wherein a bit string greater than a predetermined length  $[[1]] \underline{L}$  is obtained and an  $[[1]] \underline{L}$  bit string selected therefrom for comparison with said order  $q$ .

13. (currently amended) The method of claim 12 wherein upon rejection of said bit string of predetermined length  $[[1]] \underline{L}$ , a further  $[[1]] \underline{L}$  bit string is selected.

14. (currently amended) The method of claim 9 wherein said step of combining said first and

BEST AVAILABLE COPY

SEP. 22. 2005 3:09PM

NO. 0354 P. 10

Appl. No. 10/025,924

Page 7

Reply to Office Action of: March 24, 2005

second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $\lfloor \frac{L}{2} \rfloor$ .

BEST AVAILABLE COPY

SEP. 22. 2005 3:09PM

NO. 0354 P. 11

Appl. No. 10/025,924

Page 8

Reply to Office Action of: March 24, 2005

**Amendments to the Drawings**

Please replace the drawing sheet currently on file containing Figure 1, with the replacement sheet containing an amended Figure 1, submitted herewith.

BEST AVAILABLE COPY

**REMARKS**

Applicant wishes to thank the Examiner for reviewing the present application.

**Amendments to the Specification**

The specification is amended to correct several typographical errors. The specification is also amended replacing the character "I", which represents a bitstring of a predetermined length (introduced at paragraph [0033]), with its uppercase alternative "L" in order to distinguish same from the numeral 1 (one). The character "I" was chosen to represent an arbitrary value for the length of the bitstring. Applicant believes that the uppercase alternative is an appropriate substitute, and in no way adds subject matter to the subject application. Applicant advises that each instance of "I" has been amended accordingly for consistency.

**Amendments to the Claims**

Various typographical errors are amended in the claims, and the character "I" has been replaced by "L" in each instance, consistent with the above amendments to the specification. No new matter is added by way of these amendments.

**Amendments to the Drawings**

Figure 1 is amended to include the reference numerals "10" and "16" as recited in paragraph [0028] of the specification. No new matter is added by way of these amendments.

**Oath/Declaration**

The Examiner believes that the oath or declaration for the present application is defective, particularly that it does not identify this application by application number and filing date (MPEP §602.01 and §602.02), and is not signed by the inventors. Applicant advises that a combined Declaration and Power of Attorney meeting the above requirements was filed on February 12, 2002. However, Applicant respectfully re-submits a copy of said document with this response.

**Objections to the Drawings**

The Examiner rejected the Figures for failing to comply with 37 CFR 1.84(p)(5), specifically for failing to identify reference numerals "10" and "16" mentioned in the

**BEST AVAILABLE COPY**

specification. Accordingly, Figure 1 is amended to include numerals 10 and 16 consistent with paragraph [0028] of the specification. Applicant believes the drawings comply with 37 C.F.R. 1.84(p)(5), and are of acceptable form.

Claim Rejections – 35 U.S.C. §102(b)

Claims 1-2 and 4-5 have been rejected under 35 U.S.C. §102(b) as being anticipated by Schneier "Applied Cryptography", pages 483-490 (hereinafter "Schneier"). Applicant respectfully traverses the rejections as follows.

In paragraphs [0013] to [0017] of the subject application, the implementation of the Digital Signature Algorithm (DSA) is discussed, specifically, a bias that is introduced in the selection of the key  $k$ . This bias may be exploited to extract a value of, e.g., the private key  $d$  and thereafter render the security of the system vulnerable (see paragraph [0013]). Moreover, the work of Daniel Bleichenbacher is discussed in paragraph [0017], which suggests that the modular reduction to obtain  $k$  introduces sufficient bias into the selection of  $k$ , such that an examination of  $2^{22}$  signatures could yield the private key  $d$  in  $2^{64}$  steps, using  $2^{40}$  memory units. Bleichenbacher's work suggests that the key  $k$  need be chosen carefully, or the above vulnerability may be exploited.

The present invention provides a key generation technique that intends to eliminate such a bias during the selection of the key. In particular, claim 1 recites a method of generating a key over a group of order  $q$ , having the following steps:

- (a) generating a seed value from a random number generator;
- (b) performing a hash function on said seed value to provide an output;
- (c) determining whether said output is less than said prime number  $q$ ;
- (d) accepting said output for use as a key if the value thereof is less than said prime number  $q$ ; and
- (e) rejecting said output as a key if said value is not less than said order  $q$ .

*[identifiers added for discussion purposes herein only]*

Applicant respectfully submits that Schneier does not teach all steps of claim 1 recited above, and therefore, cannot anticipate claim 1.

Schneier describes the DSA that was proposed for use in the Digital Signature Standard (DSS) by the National Institute of Standards and Technology (NIST). The Examiner relies on

**BEST AVAILABLE COPY**

the following passages: page 487, lines 7-15; and page 489, lines 15-18. On page 487, Schneier discusses a procedure for signing and then verifying a message. There is defined, among others, a private key  $x$ , a public key  $y$ , a message  $m$ , a random number  $k$ , and a value  $q$ . To sign the message  $m$ , Alice first generates a random number  $k$  that is less than  $q$ . The Examiner believes that this step is equivalent to step (c) above. Applicant respectfully disagrees, and believes that the Examiner has misconstrued what Schneier teaches in this passage.

Step (c) of claim 1 involves determining whether the output is less than  $q$ , where the output is a result of a hash on a seed number that is chosen at random. In Schneier,  $k$  is a random number that is generated by Alice, and is said to be less than  $q$ . This value  $k$  is not an output that is a result of a hash on a seed number chosen at random, it is a random number in itself. In fact,  $k$  is actually an input used in generating a signature, not an output that is compared with a prime number  $q$  for generating a key. Moreover, no comparison is even performed in this step by Schneier. In claim 1, the comparison of the output with  $q$  is done so to exclude keys that have the vulnerability discussed above. Schneier simply does not teach such a step.

Moreover, the Examiner believes that lines 12-15 of the passage of page 487 teaches step (d) above. Applicant believes this is entirely incorrect. At lines 12-15, Schneier describes generating signature components  $r$  and  $s$ . Schneier does not teach accepting an output as a key if its value is less than  $q$ . A key has not even been generated by Schneier in these steps. Signature components are in fact created for signing the message  $m$ .

The passage taken from page 489 includes steps of checking whether or not  $q$  is prime. This in no way teaches the step of determining whether an output is less than a prime  $q$ . In fact, Schneier teaches the determination of the nature of  $q$ , not a comparison with another value.

Applicant believes that the Examiner has misconstrued the teachings of Schneier. Schneier does not teach at least steps (c) and (d) recited above. Accordingly, Schneier cannot anticipate claim 1. Therefore, claim 1 is believed to be patentable over Schneier. Claims 2 and 4-5 are dependent on claim 1, and as such are also believed to be patentable over Schneier.

#### Claim Rejections – 35 U.S.C. §103(a)

##### Claims 7-13

Claims 7-13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over

BEST AVAILABLE COPY

Schneier, in view of US Patent No. 6,219,421 to Backal. Applicant respectfully traverses the rejections as follows.

Firstly, claim 7 is dependent on claim 1, and claim 8 is dependent on claim 7. Applicant has shown above that Schneier does not anticipate claim 1. The Examiner has indicated that Schneier does not teach the subject matter of claims 7 and 8. In order to establish a *prima facie* case of obviousness, one of the criteria that must be met is that the references relied upon must teach all elements of the claim (§2143 MPEP). For the combination relied upon by the Examiner to teach all elements of claims 7 and 8, Backal would not only have to teach the subject matter of claims 7 and 8, but also what is missing from Schneier regarding claim 1. Applicant respectfully submits that Backal does not teach what is missing from claim 1, and for at least that reason, claims 7 and 8 are patentable over the combination of Schneier and Backal.

Backal teaches a virtual key method using a virtual matrix to avoid sending large keys over a communication channel. Backal does not teach the step of determining whether an output is less than a prime number  $q$ , where the output is provided by performing a hash function on a seed value generated at random. Backal also does not teach the step of accepting the output as a key if the value thereof is less than  $q$ . Accordingly, Backal does not teach what is missing from Schneier. Therefore, Applicant believes that claims 7 and 8 are patentable over the combination of Schneier and Backal.

Secondly, claim 9 is an independent claim that, in part, teaches the step of determining whether an output has a value less than  $q$ . As shown above, neither Schneier nor Backal teach such a step. Therefore, for at least that reason, Applicant believes that claim 9 is patentable over the combination of Schneier and Backal. Claims 10-13 are either directly or indirectly dependent on claim 9, and as such, are also believed to be patentable over the combination of Schneier and Backal.

In summary, Applicant respectfully submits that neither Schneier, nor Backal teaches a step of determining whether an output is less than a prime number  $q$ , and therefore, for at least that reason, claims 7-13 are patentable over such a combination.

#### Claims 3 & 6

Claims 3 and 6 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, in view of Nel et al. "Generation of Keys for use with the Digital Signature Standard

BEST AVAILABLE COPY



(DSS)", pages 6-10 (hereinafter "Nel"). Applicant respectfully traverses the rejections as follows.

Claims 3 and 6 are both dependent on claim 1. Applicant has shown above that Schneier does not anticipate claim 1. The Examiner has indicated that Schneier does not teach the subject matter of claims 3 and 6. Therefore, similar to the above, Nel must not only teach the subject matter of claims 3 and 6, but also what is missing from Schneier regarding claim 1. Applicant respectfully submits that Nel does not teach what is missing from claim 1, and for at least that reason, claims 3 and 6 are patentable over the combination of Schneier and Nel.

Nel teaches key generation for the DSS, specifically, a summary of the private-key generation method found in the original draft DSA proposal by NIST. In section 5.B, viz., the critically flawed step of  $k = G(t, XKEY) \bmod q$  is shown. This reduction modulo  $q$  introduces the bias discussed earlier in the value  $k$ . The present invention avoids this bias by rejecting values for a key that are not less than  $q$ , in part, using the step of determining whether an output is less than the prime number  $q$ . Nel does not teach such a step, but in fact teaches the vulnerability that the present invention avoids. Nel in no way teaches the step of determining whether an output (to potentially be used as a key) is less than the prime number  $q$ .

Accordingly, Nel does not teach what is missing from Schneier. Therefore, for at least that reason, Applicant believes that claims 3 and 6 are patentable over the combination of Schneier and Nel.

#### Claim 14

Claim 14 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, in view of Backal, and further in view of Nel. Applicant respectfully traverses the rejection as follows.

Claim 14 is dependent on claim 9. Applicant has shown above that none of Schneier, Backal, nor Nel teach a step of determining whether an output is less than a prime number  $q$ . Accordingly, the combination of Schneier, Backal and Nel does not teach all of the subject matter of claim 1, let alone claim 9, which is dependent on claim 1. Therefore, for at least that reason, Applicant believes that claim 14 is patentable over the combination of prior art cited by the Examiner.

BEST AVAILABLE COPY

SEP. 22. 2005 3:11PM

NO. 0354 P. 17

Appl. No. 10/025,924

Reply to Office Action of: March 24, 2005

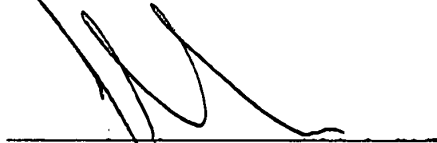
Page 14

Summary

In view of the foregoing, Applicant believes that claims 1-14 clearly and patentably distinguish over the prior art relied upon by the Examiner, and are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R.S. Orange  
Agent for Applicant  
Registration No. 29,725

Date: September 22, 2005

BLAKE, CASSELS & GRAYDON LLP  
Suite 2800, P.O. Box 25  
199 Bay Street, Commerce Court West  
Toronto, Ontario M5L 1A9  
CANADA

Tel: 416.863.3164  
JRO/BSL

BEST AVAILABLE COPY

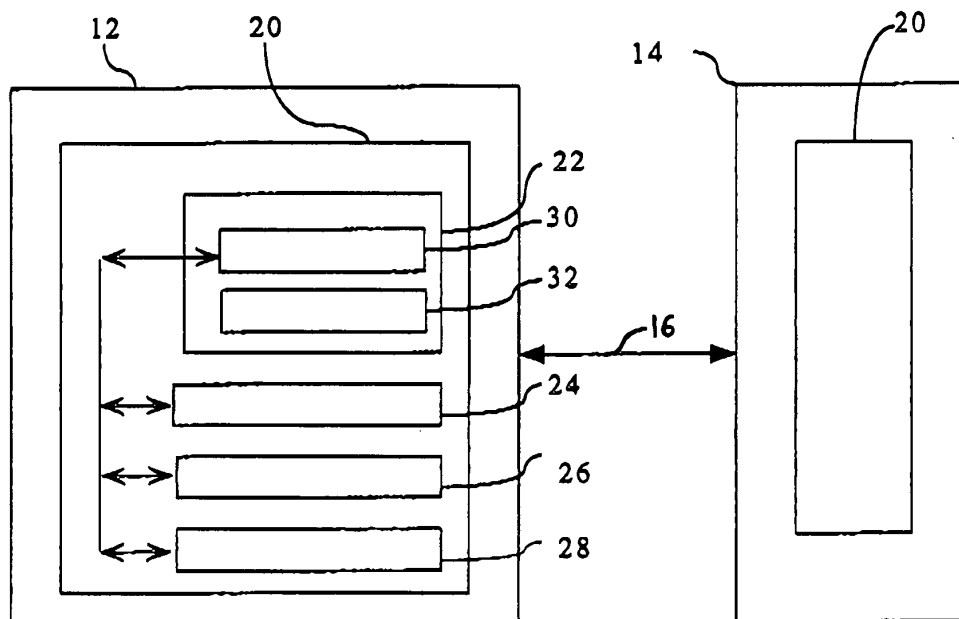
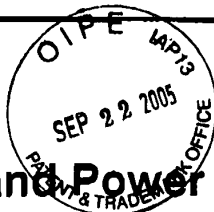


Fig. 1

10 ↗

BEST AVAILABLE



# Declaration and Power of Attorney For Patent Application

## English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

### METHOD OF PUBLIC KEY GENERATION

the specification of which

(check one)

☐ is attached hereto.

☒ was filed on December 26, 2001 as United States Application No. or PCT International Application Number 10/025,924 and was amended on \_\_\_\_\_

(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

### Prior Foreign Application(s)

### Priority Not Claimed

2,329,590

(Number)

Canada

(Country)

27/12/2000

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

_____	_____
(Application Serial No.)	(Filing Date)
_____	_____
(Application Serial No.)	(Filing Date)
_____	_____
(Application Serial No.)	(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

_____	_____	_____
(Application Serial No.)	(Filing Date)	(Status)
		(patented, pending, abandoned)
_____	_____	_____
(Application Serial No.)	(Filing Date)	(Status)
		(patented, pending, abandoned)
_____	_____	_____
(Application Serial No.)	(Filing Date)	(Status)
		(patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

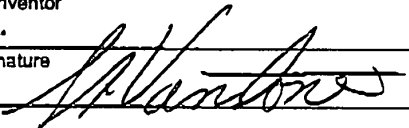
**BEST AVAILABLE COPY**

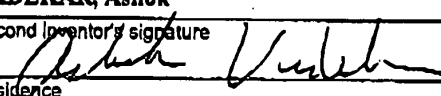
**POWER OF ATTORNEY:** As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

**Orange & Chari (Customer No. 27,155)**

Send Correspondence to: **Orange & Chari**  
Suite 4900, P.O. Box 190  
66 Wellington Street West  
Toronto, Ontario M5K 1H6 Canada

Direct Telephone Calls to: *(name and telephone number)*  
**John R.S. Orange (416)601-8440**

Full name of sole or first inventor <b>VANSTONE, Scott A.</b>	
Sole or first inventor's signature 	Date <b>Jan 25/2002</b>
Residence <b>10140 Pineview Trail, P.O. Box 490, Campbellville, Ontario L0P 1B0 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of second inventor, if any <b>VADEKAR, Ashok</b>	
Second inventor's signature 	Date <b>Jan 25/2002</b>
Residence <b>250 Harris Street, R.R. 4, Rockwood, Ontario N0B 2K0 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

**BEST AVAILABLE COPY**

Full name of third inventor, if any <b>LAMBERT, Robert J.</b>	
Third inventor's signature <i>Robert J. Lambert</i>	Date <i>Jan 25, 2002</i>
Residence <b>630 Holm Street, Cambridge, Ontario L5M 5N1 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of fourth inventor, if any <b>GALLANT, Robert P.</b>	
Fourth inventor's signature <i>Robert Gallant</i>	Date <i>Jan 30, 2002</i>
Residence <b>4788 Rosebush Road, Mississauga, Ontario L5M 5N1 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of fifth inventor, if any <b>BROWN, Daniel R.</b>	
Fifth inventor's signature <i>Daniel Brown</i>	Date <i>Jan 25/2002</i>
Residence <b>106 Banstock Drive, Toronto, Ontario M2K 2H6 Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

Full name of sixth inventor, if any <b>MENEZES, Alfred</b>	
Sixth inventor's signature <i>Alfred Menezes</i>	Date <i>Jan 26/2002</i>
Residence <b>1302-2267 Lakeshore Blvd. West Canada</b>	
Citizenship <b>Canadian</b>	
Post Office Address <b>Same As Above</b>	

BEST AVAILABLE COPY

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b> (Large Entity)				Docket No. 67539/00421	
In Re Application Of: <b>VANSTONE, Scott A; et al</b>					
Application No. 10/025,924	Filing Date 12/26/2001	Examiner <b>GELAGAY, Shewaye</b>	Customer No. 27871	Group Art Unit 2133	Confirmation No. 7632
Invention: <b>METHOD OF PUBLIC KEY GENERATION</b>					
<b>COMMISSIONER FOR PATENTS:</b>					
This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a response to the Office Action of <u>03/24/2005</u> in the above-identified application. <small>Date</small>					
The requested extension is as follows (check time period desired): <input type="checkbox"/> One month <input type="checkbox"/> Two months <input checked="" type="checkbox"/> Three months <input type="checkbox"/> Four months <input type="checkbox"/> Five months from: <u>June 24, 2005</u> until: <u>September 24, 2005</u> <small>Date Date</small>					
The fee for the extension of time is \$1,020 and is to be paid as follows: <input type="checkbox"/> A check in the amount of the fee is enclosed. <input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. 02-2553 <input type="checkbox"/> If an additional extension of time is required, please consider this a petition therefor and charge any additional fees which may be required to Deposit Account No. 02-2553 <input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.					
<b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b>					
Signature <b>John R.S. Orange (Reg. #29,725)</b> <b>Blake, Cassels &amp; Graydon LLP</b> <b>Box 25, Commerce Court West</b> <b>199 Bay Street</b> <b>Toronto, Ontario M5L 1A9</b> <b>CANADA</b> <b>Tel: (416) 863-3164</b> <b>Fax: (416) 863-2653</b>			Dated: Sept. 22, 2005		
09/26/2005 HAL111 00000102 022553 10025924 01 FC:1253 1020.00 DA CC;			I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on _____ (Date) _____ Signature of Person Mailing Correspondence _____ Typed or Printed Name of Person Mailing Correspondence		

P12LARGE/REV09



SEP. 22. 2005 3:12PM

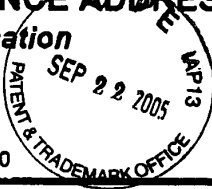
NO. 0354 P. 24

Doc Code:

Approved for use through 07/31/2008. OMB 0651-0035

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**CHANGE OF  
CORRESPONDENCE ADDRESS****Application**Address to:  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Application Number	10/025,924
Filing Date	12/26/2001
First Named Inventor	VANSTONE, Scott A.
Art Unit	2133
Examiner Name	GELAGAY, Shewaye
Attorney Docket Number	67539/00421

Please change the Correspondence Address for the above-identified application to:

☒ The address associated with  
Customer Number:

27871

OR

☐ Firm or  
Individual Name

Address

City

State

ZIP

Country

Telephone

Email

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:

☐ Applicant/Inventor

☐ Assignee of record of the entire interest.  
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☒ Attorney or Agent of record. Registration Number 29,725

☐ Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number

Signature

Typed or Printed

John R.S. Orange (Reg. #29,725)

Date

September 22, 2005

Telephone

(416) 863-3164

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☒ \*Total of 1 forms are submitted.

This collection of information is required by 37 CFR 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending on the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2

Doc Code:

PTO/SB/21 (09-04)

Approved for use through 07/31/2009. OMB 0651-0081

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>TRANSMITTAL FORM</b> OIP SEP 22 2005 PATENT & TRADEMARK OFFICE Do not use for correspondence after initial filing	Application Number	10/025,924
	Filing Date	12/26/2001
	First Named Inventor	VANSTONE, Scott A.
	Art Unit	2133
	Examiner Name	GELAGAY, Shewaye
Total Number of Pages in This Submission	Attorney Docket Number	67539/00421

ENCLOSURES (Check all that apply)		
<input type="checkbox"/> Fee Transmittal Form	<input checked="" type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to TC
<input type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input checked="" type="checkbox"/> Amendment / Reply	<input type="checkbox"/> Petition	<input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declaration(s)	<input checked="" type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address	<input type="checkbox"/> Status Letter
<input checked="" type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Terminal Disclaimer	<input type="checkbox"/> Other Enclosure(s) (please identify below):
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> CD, Number of CD(s) _____	
<input type="checkbox"/> Certified Copy of Priority Document(s)	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Response to Missing Parts/Incomplete Application	Remarks	
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53		
SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT		
Firm Name	Blake, Cassels & Graydon LLP	
Signature		
Printed name	John R. Orange	
Date	September 22, 2005	Reg. No. 29,725

CERTIFICATE OF TRANSMISSION/MAILING		
I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:		
Signature		
Typed or printed name	Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

## \*BIBDATASHEET\*

CONFIRMATION NO. 7632

Bib Data Sheet

<b>SERIAL NUMBER</b> 10/025,924	<b>FILING OR 371(c) DATE</b> 12/26/2001 <b>RULE</b>	<b>CLASS</b> 380	<b>GROUP ART UNIT</b> 2133	<b>ATTORNEY DOCKET NO.</b> 00001-0417
<b>APPLICANTS</b> Scott A. Vanstone, Campbellville, CANADA; Ashok Vadekar, Rockwood, CA; Robert J. Lambert, Cambridge, CANADA; Robert P. Gallant, Mississauga, CANADA; Daniel R. Brown, Toronto, CANADA; Alfred Menezes, West Canada, CANADA;				
<b>** CONTINUING DATA *****</b>  <b>** FOREIGN APPLICATIONS *****</b> CANADA 2,329,590 12/27/2000				
<b>IF REQUIRED, FOREIGN FILING LICENSE GRANTED</b> <b>** 02/25/2002</b>				
Foreign Priority claimed <input type="checkbox"/> yes <input type="checkbox"/> no 35 USC 119 (a-d) conditions <input type="checkbox"/> yes <input type="checkbox"/> no <input type="checkbox"/> Met after met Allowance Verified and Acknowledged <u>Examiner's Signature</u> <u>Initials</u>		<b>STATE OR COUNTRY</b> CANADA	<b>SHEETS DRAWING</b> 7	<b>TOTAL CLAIMS</b> 14
			<b>INDEPENDENT CLAIMS</b> 2	
<b>ADDRESS</b> <div style="text-align: right;">AIR MAIL</div> 27871				
<b>TITLE</b> Method of public key generation				
<b>FILING FEE RECEIVED</b> 870	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:		<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees ( Filing ) <input type="checkbox"/> 1.17 Fees ( Processing Ext. of time ) <input type="checkbox"/> 1.18 Fees ( Issue ) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

## Application or Docket Number

Substitute for Form PTO-875

10/125924

APPLICATION AS FILED - PART I

(Column 1)

(Column 2)

SMALL ENTITY

OR

OTHER THAN  
SMALL ENTITY

FOR	NUMBER FILED	NUMBER EXTRA
BASIC FEE (37 CFR 1.16(e), (b), or (c))		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))		
EXAMINATION FEE (37 CFR 1.16(c), (p), or (q))		
TOTAL CLAIMS (37 CFR 1.16(j))	14 minus 20 =	*
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).	
MULTIPLE DEPENDENT CLAIM PRESENT. (37 CFR 1.16(j))		

\* If the difference in column 1 is less than zero, enter "0" in column 2.

\* If the difference in column 1 is less than zero, enter "0" in column 2.

## APPLICATION AS AMENDED – PART II

9-22-05

(Column 1)

(Column 2)

(Column 3)

## SMALL ENTITY

OR

OTHER THAN  
SMALL ENTITY

AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total (37 CFR 1.16(i))	14	20	=
	Independent (37 CFR 1.16(h))	2	3	=
Application Size Fee (37 CFR 1.16(s))				
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(g))				

SMALL ENTITY	
RATE (\$)	ADDITIONAL FEE (\$)
X =	
X =	
TOTAL ADD'L FEE	

SMALL ENTITY	
RATE (\$)	ADDITIONAL FEE (\$)
X =	
X =	
TOTAL ADD'L FEE	

TOTAL	
ADD'L FEES	

TOTAL	100.00
ADD'L FEE	0.00

{Column 1}

(Column 2)

(Column 3)

ATE (\$)

ADDL

DATE	RATE (\$)
1/1/01	1.00
1/1/02	1.00
1/1/03	1.00
1/1/04	1.00
1/1/05	1.00
1/1/06	1.00
1/1/07	1.00
1/1/08	1.00
1/1/09	1.00
1/1/10	1.00
1/1/11	1.00
1/1/12	1.00
1/1/13	1.00
1/1/14	1.00
1/1/15	1.00
1/1/16	1.00
1/1/17	1.00
1/1/18	1.00
1/1/19	1.00
1/1/20	1.00
1/1/21	1.00
1/1/22	1.00
1/1/23	1.00
1/1/24	1.00
1/1/25	1.00
1/1/26	1.00
1/1/27	1.00
1/1/28	1.00
1/1/29	1.00
1/1/30	1.00
1/1/31	1.00
1/1/32	1.00
1/1/33	1.00
1/1/34	1.00
1/1/35	1.00
1/1/36	1.00
1/1/37	1.00
1/1/38	1.00
1/1/39	1.00
1/1/40	1.00
1/1/41	1.00
1/1/42	1.00
1/1/43	1.00
1/1/44	1.00
1/1/45	1.00
1/1/46	1.00
1/1/47	1.00
1/1/48	1.00
1/1/49	1.00
1/1/50	1.00
1/1/51	1.00
1/1/52	1.00
1/1/53	1.00
1/1/54	1.00
1/1/55	1.00
1/1/56	1.00
1/1/57	1.00
1/1/58	1.00
1/1/59	1.00
1/1/60	1.00
1/1/61	1.00
1/1/62	1.00
1/1/63	1.00
1/1/64	1.00
1/1/65	1.00
1/1/66	1.00
1/1/67	1.00
1/1/68	1.00
1/1/69	1.00
1/1/70	1.00
1/1/71	1.00
1/1/72	1.00
1/1/73	1.00
1/1/74	1.00
1/1/75	1.00
1/1/76	1.00
1/1/77	1.00
1/1/78	1.00
1/1/79	1.00
1/1/80	1.00
1/1/81	1.00
1/1/82	1.00
1/1/83	1.00
1/1/84	1.00
1/1/85	1.00
1/1/86	1.00
1/1/87	1.00
1/1/88	1.00
1/1/89	1.00
1/1/90	1.00
1/1/91	1.00
1/1/92	1.00
1/1/93	1.00
1/1/94	1.00
1/1/95	1.00
1/1/96	1.00
1/1/97	1.00
1/1/98	1.00
1/1/99	1.00
1/1/00	1.00
1/1/01	1.00
1/1/02	1.00
1/1/03	1.00
1/1/04	1.00
1/1/05	1.00
1/1/06	1.00
1/1/07	1.00
1/1/08	1.00
1/1/09	1.00
1/1/10	1.00
1/1/11	1.00
1/1/12	1.00
1/1/13	1.00
1/1/14	1.00
1/1/15	1.00
1/1/16	1.00
1/1/17	1.00
1/1/18	1.00
1/1/19	1.00
1/1/20	1.00
1/1/21	1.00
1/1/22	1.00
1/1/23	1.00
1/1/24	1.00
1/1/25	1.00
1/1/26	1.00
1/1/27	1.00
1/1/28	1.00
1/1/29	1.00
1/1/30	1.00
1/1/31	1.00
1/1/32	1.00
1/1/33	1.00
1/1/34	1.00
1/1/35	1.00
1/1/36	1.00
1/1/37	1.00
1/1/38	1.00
1/1/39	1.00
1/1/40	1.00

ADDI

<b>AMENDMENT B</b>		(Column 1)	<b>CLAIMS REMAINING AFTER AMENDMENT</b>		(Column 2)	<b>HIGHEST NUMBER PREVIOUSLY PAID FOR</b>	(Column 3)	<b>PRESENT EXTRA</b>		<b>RATE (\$)</b>	<b>ADDITIONAL FEE (\$)</b>		<b>RATE (\$)</b>	<b>ADDITIONAL FEE (\$)</b>
	Total (37 CFR 1.16(i))	*	Minus	**	=	X	=	OR	X	=				
	Independent (37 CFR 1.16(j))	*	Minus	***	=	X	=	OR	X	=				
	Application Size Fee (37 CFR 1.16(s))										OR			
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))										OR			
									TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		

TOTAL  
ADD'L FEETOTAL  
ADD'L FEE

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

\*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2*

CLAIMS ONLY							Application Number <b>10/025924</b>		Filing Date		
							Applicant(s)				
							* May be used for additional claims or amendments				
CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT						
	Indep	Depend	Indep	Depend	Indep	Depend	Indep	Depend	Indep	Depend	
1	1										
2		1									
3		1									
4		1									
5		1									
6		1									
7		1									
8		1									
9	1										
10		1									
11		1									
12		1									
13		1									
14		1									
15											
16											
17											
18											
19											
20											
21											
22											
23											
24											
25											
26											
27											
28											
29											
30											
31											
32											
33											
34											
35											
36											
37											
38											
39											
40											
41											
42											
43											
44											
45											
46											
47											
48											
49											
50											
51											
52											
53											
54											
55											
56											
57											
58											
59											
60											
61											
62											
63											
64											
65											
66											
67											
68											
69											
70											
71											
72											
73											
74											
75											
76											
77											
78											
79											
80											
81											
82											
83											
84											
85											
86											
87											
88											
89											
90											
91											
92											
93											
94											
95											
96											
97											
98											
99											
100											
Total Indep	2										
Total Depend	12										
Total Claims	14										

S70	28	(increment\$4) adj ((seed adj2 value) or (random adj2 (no or number)))	US-PGPUB; USPAT	OR	ON	2005/03/04 11:32
S71	1	("6934392").PN.	US-PGPUB; USPAT	OR	OFF	2005/11/15 15:28
S72	1	("6618483").PN.	US-PGPUB; USPAT	OR	OFF	2005/11/15 15:50
S73	1	("6705517").PN.	US-PGPUB; USPAT	OR	OFF	2005/11/15 16:59
S75	1837	(boundary adj2 limit)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/15 17:00
S76	29	(boundary adj2 limit) same key	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/15 17:00
S77	1285	(perform\$4 or generat\$4) same (hash with (seed or random))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/29 18:09
S78	12	(perform\$4 or generat\$4) same (hash with (seed or random)) and ((determin\$4 or verify\$4 or compar\$4 or check\$4) same ((less or lower) with (q or prime)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/29 18:16
S79	15	(perform\$4 or generat\$4) same (hash with (seed or random)) and ((determin\$4 or verify\$4 or compar\$4 or check\$4 or test\$4 ) same ((less or lower) with (q or prime)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/29 18:39
S80	2	(perform\$4 or generat\$4) adj10 (hash with (seed or random)) and ((determin\$4 or verify\$4 or compar\$4 or check\$4 or test\$4 ) adj10 ((less or lower) with (q or prime)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/29 18:40
S81	2	((("6078667") or ("6337909")).PN.	US-PGPUB; USPAT	OR	OFF	2005/11/30 06:49

S82	17	Bleichenbacher	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/30 07:37
S83	3	"security builder"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/30 07:46
S88	5	(generat\$4 with ((hash or digest) same (seed or random))) and ((compar\$4 or test\$4 or verify\$4 or check\$4) with ((less or lower) with (q or prime)))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/11/30 07:49



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632
27871	7590	12/06/2005	EXAMINER	
BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA			GELAGAY, SHEWAYE	
			ART UNIT	PAPER NUMBER
			2137	
DATE MAILED: 12/06/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.



<b>Office Action Summary</b>	Application No.	Applicant(s)	
	10/025,924	VANSTONE ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 22 September 2005.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

## **DETAILED ACTION**

1. This office action is in response to Applicant's amendment filed on September 22, 2005. Claims 1, 5, 6, 9, 12-14 have been amended. Claims 1-14 are pending.

### ***Oath/Declaration***

2. In view of the amendment filed September 22, 2005, the Examiner withdraws the objection to the Oath/Declaration.

### ***Drawings***

In view of the amendment filed September 22, 2005, the Examiner withdraws the objection to the Drawings.

### ***Specification***

3. In view of the amendment filed September 22, 2005, the Examiner withdraws the objection to the Specification.

### ***Response to Arguments***

4. Applicant's arguments, see Remarks, filed September 22, 2005, with respect to the rejection(s) of claim(s) 1-4 under 35 U.S.C. 102(b) and 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made.

### ***Claim Rejections - 35 USC § 112***

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 1 recites the limitation "said prime number q" in lines 5 and 6. There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1-2, 4-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Matyas, Jr. et al. (hereinafter Matyas) United States Letter Patent Number 6,307,938.

As per claim 1:

Schneier teaches a method of generating a key over a group of order q, said method including the steps of:

generating a seed value from a random number generator; (Page 487, line 11; Page 489, lines 15-16)

accepting said output for use as a key if the value thereof is less than said prime number q; (Page 487, lines 12-15) and

rejecting said output as a key if said value is not less than said order  $q$ . (Page 487, line 11)

In addition, Schneier further discloses performing a hash function (Page 487, lines 7-8; Page 489, lines 17-18) and determining whether a random number is less than  $q$ . (Page 487, line 11; ... $k$  less than  $q$ )

Schneier does not explicitly disclose a method of performing a hash function on seed number to provide an output and determining whether said output is less than said prime number  $q$ .

Matyas in analogous art, however, discloses a method of performing a hash of each of seed values with SHA-1 to produce hash values; (Col. 6, lines 7-9) and generating seed involving a test to ensure that it falls within a specified range of allowed values and until it satisfies primality test. (Col. 6, line 65-Col. 8, line 35)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method of performing a hash function on seed number to provide an output and determining whether said output is less than said prime number  $q$ . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Matyas (Col. 7, lines 5-6) in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed.

As per claim 2:

The combination of Schneier and Matyas teach all the subject matter as discussed above. In addition, Schneier further discloses a method wherein another seed value is generated by said random number generator if said output is rejected. (Page 487, line 11; Page 489, line 22)

As per claim 4:

The combination of Schneier and Matyas teach all the subject matter as discussed above. In addition, Schneier discloses a method wherein said key is used for generation of a public key. (Page 487, lines 8-15; Page 488, line 3-8)

As per claim 5:

The combination of Schneier and Matyas teach all the subject matter as discussed above. In addition, Schneier further discloses a method wherein said order  $q$  is prime number represented by a bit string of predetermined length  $l$ . (Page 487, line 1 and Page 488, line 5)

9. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Matyas, Jr. et al. (hereinafter Matyas) United States Letter Patent Number 6,307,938 and further in view of Backal United States Letter Patent Number 6,219,421.

As per claim 7:

The combination of Schneier and Matyas teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein if said output is rejected, said output is incremented by a deterministic function and a hash

function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

Backal in analogous art, however, disclose a method wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key. (Col. 5, lines 61-67)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method of wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Backal (Col. 1, lines 50-51) in order to provide an exceptional degree of security. This way, the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document.

As per claim 8:

The combination of Schneier, Matyas and Backal teach all the subject matter as discussed above. In addition, Backal further discloses a method wherein said step of incrementing includes a further step of adding a particular value to said seed value. (Col. 5, lines 61-67)

As per claim 9:

Schneier teaches a method of generating a key over a group of order  $q$ , said method including the steps of:

generating a seed value from a random number generator; (Page 487, line 11; Page 489, lines 15-16)

accepting said new output as a key  $k$  if said new output has a value less than order  $q$ ; (Page 487, line 11; ... $k$  less than  $q$ ) and

rejecting said new output as a key if said new output has a value less than order  $q$ . (Page 487, line 11)

In addition, Schneier further discloses performing a hash function (Page 487, lines 7-8; Page 489, lines 17-18) and determining whether a random number is less than  $q$ . (Page 487, line 11; ... $k$  less than  $q$ )

Schneier does not explicitly disclose a method of performing a hash function on seed number to provide an output; determining whether said output is less than said prime number  $q$ ; incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ .

Matyas in analogous art, however, discloses a method of performing a hash of each of seed values with SHA-1 to produce hash values; (Col. 6, lines 7-9) and generating seed involving a test to ensure that it falls within a specified range of allowed values and until it satisfies primality test. (Col. 6, line 65-Col. 8, line 35)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method of performing a hash function on seed number to provide an output and determining whether said output is less than said prime number  $q$ . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Matyas (Col. 7, lines 5-6) in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed.

Both references do not explicitly disclose incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ .

Backal in analogous art, however, disclose a method of incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; (Col. 5, lines 61-67) and

combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ ; (Col. 5, lines 54-60)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and



Art Unit: 2137

Matyas to include a method of incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Backal (Col. 1, lines 50-51) in order to provide an exceptional degree of security. This way, the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document.

As per claim 10:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein upon rejection of said new output a new seed value is generated by said random number generator. (Page 487, line 11; Page 489, line 22)

As per claim 11:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Backal further discloses a method wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained. (Col. 5, lines 61-67)

As per claim 12:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein a bit string greater than a predetermined length  $l$  is obtained and an  $l$  bit string selected therefrom for comparison with said order  $q$ . (Page 487, line 1 and Page 488, line 5)

As per claim 13:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein upon rejection of said bit string of predetermined length  $l$ , a further  $l$  bit string is selected. (Page 487, line 1 and Page 488, line 5)

10. Claims 3 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Matyas, Jr. et al. (hereinafter Matyas) United States Letter Patent Number 6,307,938 in view of Nel et al. (hereinafter Nel) "Generation of Keys for use with the Digital Signature Standard (DSS)" (Pages 6-10).

As per claim 3:

The combination of Schneier and Matyas teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein the step of accepting said output as a key includes a further step of storing said key.

Nel in analogous art, however, discloses a method wherein the step of accepting said output as a key includes a further step of storing said key. (Page 10, Col. 1, lines 3-4)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method wherein the step of accepting said output as a key includes a further step of storing said key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to be able to reuse the key and also to perform auditing on the key generation process.

As per claim 6:

The combination of Schneier, Matyas and Nel teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said output from said hash function is a bit string of predetermined length L.

Nel in analogous art, however, discloses a method wherein said output from said hash function is a bit string of predetermined length L. (Page 8, Col. 2, lines 8-11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method wherein said output from said hash function is a bit string of predetermined length L. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Nel et al. (Page 8, Col. 2, lines 6-7) in order to prevent constructing a message which will yield a known value of message digest.

11. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Backal United States Letter Patent

Number 6,219,421 and further in view of Nel et al. (hereinafter Nel) "Generatiion of Keys for use with the Digital Signature Standard (DSS)" (Pages 6-10).

As per claim 14:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. Both references do not explicitly disclose method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $l$ .

Nel in analogous art, however, discloses a method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $l$ . (Page 8, Col. 2, lines 8-11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $l$ . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Nel (Page 8, Col. 2, lines 6-7) in order to prevent constructing a message which will yield a known value of message digest.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shewaye Gelagay  
11/30/05

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER

<b>Notice of References Cited</b>	Application/Control No. 10/025,924	Applicant(s)/Patent Under Reexamination VANSTONE ET AL.	
	Examiner Shewaye Gelagay	Art Unit 2137	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,307,938	10-2001	Matyas et al.	380/44
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			


**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<b>Search Notes</b> 	<b>Application No.</b>		<b>Applicant(s)</b>	
	10/025,924		VANSTONE ET AL.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Shewaye Gelagay		2133	

SEARCHED			
Class	Subclass	Date	Examiner
380	44	3/4/2005	SG
380	277	3/4/2005	SG
708	250	3/4/2005	SG

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
East Searched	3/4/2005	sg
ACM searched (incrementing seed value)	3/4/2005	SG
IEEE searched (increment and combine seed value)	3/4/2005	SG
Updated East search	11/30/2005	SG
STIC (Fast and Focus) search	11/30/2005	sg

MAR. 3. 2006 3:41PM

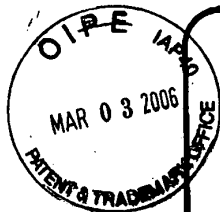
BEST AVAILABLE COPY

NO. 3913 P. 3

Doc Code:

PTO/SB/21 (09-04)  
Approved for use through 07/31/2006. OMB 0851-0031  
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL  
FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	10/025,924
Filing Date	12/26/2001
First Named Inventor	VANSTONE, Scott A
Art Unit	2137
Examiner Name	GELAGAY, Shewaye
Attorney Docket Number	67539/00421

## ENCLOSURES (Check all that apply)

<input type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to TC
<input type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input checked="" type="checkbox"/> Amendment / Reply	<input type="checkbox"/> Petition	<input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declaration(s)	<input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address	<input type="checkbox"/> Status Letter
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Terminal Disclaimer	<input type="checkbox"/> Other Enclosure(s) (please identify below):
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> CD, Number of CD(s) _____	
<input type="checkbox"/> Certified Copy of Priority Document(s)	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Response to Missing Parts/Incomplete Application	Remarks	
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53		

## SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	Blake, Cassels & Graydon LLP		
Signature			
Printed name	Sean X. Zhang		
Date	March 3, 2006	Reg. No.	56,058

## CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	
Typed or printed name	
Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450, DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

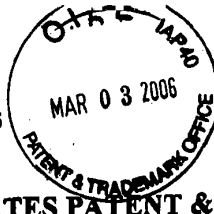


MAR. 3. 2006 3:41PM

NO. 3913 P. 4

Appl. No. 10/025,924

Reply to Office Action of: December 6, 2005



**BEST AVAILABLE COPY**

**IN THE UNITED STATES PATENT & TRADEMARK OFFICE**

Appl. No.: 10/025,924

Applicant: VANSTONE, Scott et al.

Filed: December 26, 2001

Title: METHOD OF PUBLIC KEY GENERATION

Art Unit: 2137

Examiner: GELAGAY, Shewaye

Docket No.: 67539/00421

Mail Stop Amendment  
U.S. Patent & Trademark Office  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**RESPONSE**

Sir:

This is further to the Office Action mailed December 6, 2005. Applicant wishes to amend the above-identified application as follows:

**Amendments to the Claims:** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks:** begin on page 5 of this paper.

Appl. No. 10/025,924  
Reply to Office Action of: December 6, 2005

**BEST AVAILABLE COPY****Amendments to the Claims**

This listing of claims will replace all prior versions and listings of claims in the application:

**Listing of claims:**

1. (currently amended) A method of generating a key over a group of order  $q$ , said method including the steps of:
  - generating a seed value from a random number generator;
  - performing a hash function on said seed value to provide an output;
  - determining whether said output is less than said ~~prime number~~ order  $q$ ;
  - accepting said output for use as a key if the value thereof is less than said ~~prime number~~ order  $q$ ; and
  - rejecting said output as a key if said value is not less than said order  $q$ .
2. (original) The method of claim 1 wherein another seed value is generated by said random number generator if said output is rejected.
3. (original) The method of claim 1 wherein the step of accepting said output as a key includes a further step of storing said key.
4. (original) The method of claim 1 wherein said key is used for generation of a public key.
5. (currently amended) The method of claim 1 wherein said order  $q$  is a prime number represented by a bit string of predetermined length  $L$ .
6. (previously presented) The method of claim 5 wherein said output from said hash function is a bit string of predetermined length  $L$ .
7. (original) The method of claim 1 wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to

Appl. No. 10/025,924  
Reply to Office Action of: December 6, 2005

produce a new output; a determination being made as to whether said new output is acceptable as a key.

8. (original) The method of claim 7, wherein said step of incrementing includes a further step of adding a particular value to said seed value.

9. (currently amended) A method of generating a key over a group of order q, said method including the steps of:

- generating a seed value from a random number generator;
- performing a hash function on said seed number to provide a first output;
- incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output;
- combining said first output and second output to produce a new output;
- determining whether said new output has a value less than said order q;
- accepting said new output as a key k if said new output has a value less than said order q;
- and
- rejecting said new output as a key if said new output has a value less than said order q.

10. (original) The method of claim 9 wherein upon rejection of said new output a new seed value is generated by said random number generator.

11. (original) The method of claim 9 wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained.

12. (previously presented) The method of claim 9 wherein a bit string greater than a predetermined length L is obtained and an L bit string selected therefrom for comparison with said order q.

13. (previously presented) The method of claim 12 wherein upon rejection of said bit string of predetermined length L, a further L bit string is selected.

MAR. 3. 2006 3:42PM

NO. 3913 P. 7

**BEST AVAILABLE COPY**

Appl. No. 10/025,924

Reply to Office Action of: December 6, 2005

14. (previously presented) The method of claim 9 wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L.

**BEST AVAILABLE COPY**

Appl. No. 10/025,924  
Reply to Office Action of: December 6, 2005

**REMARKS**

Applicant wishes to thank the Examiner for reviewing the present application.

**Amendments to the Claims**

Claim 1 is amended replacing the expression "prime number" with "order" on lines 5 and

6.

Claim 5 is amended inserting "a" between "is" and "prime" on line 1.

Claim 9 is amended inserting "said" between "than" and "order" on lines 9 and 10.

**Claim Rejections – 35 U.S.C. § 112**

Claim 1 has been rejected under 35 U.S.C. § 112, second paragraph as being indefinite due to an alleged lack of antecedence for the expression "said prime number q". Applicant amends claim 1 replacing "said prime number q" with "said order q". The expression "order q" is introduced in the preamble of claim 1. Therefore, Applicant believes that claim 1 as amended complies with 35 U.S.C. § 112, second paragraph.

**Claim Rejections – 35 U.S.C. § 103****Regarding Claims 1-2, 4-5:**

Claims 1-2, and 4-5 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier (pages 483-490) in view of US Patent No. 6,307,938 to Matyas Jr. et al. (hereinafter Matyas). Applicant respectfully traverses the rejections as follows.

Schneier teaches the digital signature algorithm (DSA) proposed for use in the Digital Signature Standard (DSS) by the National Institute of Standards and Technology (NIST). The Examiner relies primarily on page 487, line 11, where Alice generates a random number  $k$  which is less than  $q$ . Based on this step, the Examiner believes that Schneier teaches the step of generating a seed value from a random number (i.e.  $k$ ), and the steps of accepting or rejecting the output based on whether or not it is less than a prime  $q$ . Applicant acknowledges that the Examiner admits that Schneier does not teach comparing a hashed version of a seed value with a value  $q$ . The Examiner relies on Matyas as teaching what is missing from Schneier, specifically, the passage from column 6, line 65 to column 8, line 35.

In the above-noted passage, Matyas outlines the ANSI X9.31 method of prime number

Appl. No. 10/025,924  
Reply to Office Action of: December 6, 2005

generation involving hashing SEED values to generate the needed random numbers for generating the primes  $p$  and  $q$ . Assuming one SEED, the method proceeds to choose a SEED, hash the SEED, generate a random number (RN) from the hashed SEED, generate a prime ( $p$ ) from the RN, and perform a primality test on the prime  $p$ . In practice, several SEED values are used to generate the RN and prime  $p$ . The prime  $p$  is chosen from an iterative process that applies the primality test to the value chosen for  $p$  until certain criteria are met.

Applicant respectfully submits that:

- 1) Matyas does not teach performing a hash as asserted by the Examiner, let alone as recited in claim 1; and
- 2) Even if for the sake of argument Matyas did teach performing a hash as the Examiner asserts, there is no motivation to combine Matyas with Schneier.

Regarding 1), as noted above, the ANSI X9.31 procedure generates a prime from random numbers derived from the hash of a SEED value. However, there is no step of comparing an output (let alone an output destined to be a key) with an established value of order  $q$  to determine if that output is less than the prime, as the Examiner asserts. It is the Applicant's recognition that by choosing the key as recited in claim 1, the bias in the selection of  $k$  (identified by the work of Daniel Bleichenbacher) can be minimized.

The ANSI X9.31 method taught by Matyas does not recognize this bias nor provide any steps to avoid the bias, let alone hash a seed value and use this hashed value as an output to determine if the output is less than a predetermined value of a certain order as claimed. In fact, the ANSI method taught by Matyas teaches generating a random number from a hashed SEED, whereas claim 1 recites generating a seed from a random number and then hashing the seed value to produce an output. Therefore the teachings of Matyas relied upon by the Examiner are quite contrary to what is recited in claim 1.

According to MPEP 2143, one of the criteria for establishing a *prima facie* case of obviousness is that the relied upon references teach every element in the claim. Clearly, neither Schneier nor Matyas teach performing a hash function on a seed value that is chosen from a random number generator as recited in claim 1. In fact, the teachings of Matyas that are relied upon by the Examiner teach performing a hash on a seed first and then generating a random number from the hash value, which is quite contrary to what is claimed.

Regarding 2), Schneier teaches in the realm of digital signatures, wherein a number  $q$  is

Appl. No. 10/025,924  
Reply to Office Action of: December 6, 2005

used in generating signature components  $r$  and  $s$ , whereas Matyas teaches in the realm of generating prime numbers from a series of seed values. Clearly there is no direction in the teachings of Schneier to look to the teachings of Matyas since they teach entirely different schemes for achieving entirely different results. In fact, there is nothing in either Schneier or Matyas that would encourage a person skilled in the art to combine the teachings. The Examiner relies on column 7, lines 5-6 from Matyas as providing the motivation to combine the references. In this passage Matyas merely states that it is not possible to invert the hash to determine the required input SEED(s). Applicant believes that this does not provide sufficient motivation since the mere acknowledgement that a hash function is theoretically irreversible does not teach how to implement the hash in generating a key as recited in claim 1. There is simply no suggestion or motivation to make such a leap of logic.

Applicants respectfully submit that not only do Schneier and Matyas, either in combination or alone, fail to teach every element recited in claim 1, but there is no suggestion or motivation to even make such a combination. Therefore, Applicants believe that claim 1 clearly and patentably distinguishes over the combination of Schneier in view of Matyas and as such is in condition for allowance.

Claims 2 and 4-5 being ultimately dependent on claim 1 are also believed to distinguish over the prior art cited.

#### **Regarding Claims 7-13:**

Claims 7-13 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Matyas, in further view of Backal. Applicant respectfully traverses the rejections as follows.

Backal teaches a virtual key method using a virtual matrix to avoid sending large keys over a communication channel. Claims 7-8 are ultimately dependent on claim 1, which Applicant submits, distinguishes over Schneier in view of Matyas. Therefore, Backal must not only teach the subject matter of claims 7-8 but also what is missing from Schneier and Matyas. Backal does not teach determining whether an output is less than a number of order  $q$ , where the output is provided by performing a hash function on a seed number generated from a random number generator. Therefore, Backal at least fails to teach what is missing from Schneier and Matyas, and as such, claims 7-8 are believed to distinguish over the Schneier in view of Matyas,

Appl. No. 10/025,924  
Reply to Office Action of: December 6, 2005

in further view of Backal, for at least that reason.

Claim 9 is an independent claim that, similar to claim 1, determines whether an output is less than a number of order  $q$ , where the output is provided in part by performing a hash function on a seed number generated from a random number generator. Therefore, arguments made regarding claim 1 over Schneier and Matyas equally apply to claim 9. As noted above, Backal does not teach what is missing from Schneier and Matyas. Therefore, claim 9 is believed to patentably distinguish over Schneier, in view of Matyas, in further view of Backal for at least that reason.

Claims 10-13 being ultimately dependent on claim 9 are also believed to distinguish over the prior art cited.

**Regarding Claims 3 and 6:**

Claims 3 and 6 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Matyas, in further view of Nel. Applicant respectfully traverses the rejections as follows.

Nel teaches key generation for the DSS, specifically, a summary of the private key generation method found in the original draft DSA proposal by NIST. Claims 3 and 6 are ultimately dependent on claim 1, which Applicant submits, distinguishes over Schneier in view of Matyas. Therefore, Nel must not only teach the subject matter of claims 3 and 6 but also what is missing from Schneier and Matyas. Nel does not teach determining whether an output is less than a number of order  $q$ , where the output is provided by performing a hash function on a seed number generated from a random number generator. Therefore, Nel at least fails to teach what is missing from Schneier and Matyas, and as such, claims 3 and 6 are believed to distinguish over the Schneier in view of Matyas, in further view of Nel, for at least that reason.

**Regarding Claim 14:**

Claim 14 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over Schneier in view of Backal, in further view of Nel. Applicant respectfully traverses the rejections as follows. Applicant notes that the Examiner also mentions Matyas in this rejection. Applicant assumes that the Examiner intended to include Matayas, and thus claim 14 is assumed to have been rejected over Schneier, in view of Matyas, in further view of Backal, in further view of Nel.



Appl. No. 10/025,924  
Reply to Office Action of: December 6, 2005

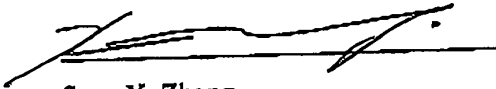
Claim 14 is ultimately dependent on claim 9, which Applicant submits, distinguishes over Schneier in view of Matyas, in further view of Backal. Therefore, Nel must not only teach the subject matter of claim 14 but also what is missing from Schneier, Matyas, and Backal. As noted above, Nel does not teach determining whether an output is less than a number of order  $q$ , where the output is provided by performing a hash function on a seed number generated from a random number generator. Therefore, Nel at least fails to teach what is missing from Schneier, Matyas, and Backal, and as such, claim 14 is believed to distinguish over Schneier, in view of Matyas, in further view of Backal, in further view of Nel, for at least that reason.

Summary

In view of the foregoing, Applicant respectfully submits that all pending claims, namely claims 1-14 patentably distinguish over the prior art cited by the Examiner, and as such are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



Sean X. Zhang  
Agent for Applicant  
Registration No. 56,058

Date: March 3, 2006

BLAKE, CASSELS & GRAYDON LLP  
Suite 2800, P.O. Box 25  
199 Bay Street, Commerce Court West  
Toronto, Ontario M5L 1A9  
CANADA

Tel: 416.863.5839  
SZH/BSL

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.  
**PATENT APPLICATION FEE DETERMINATION RECORD**  
Substitute for Form PTO-875

Application or Docket Number  
**10/125924**

**APPLICATION AS FILED - PART I**  
(Column 1) (Column 2)

FOR	NUMBER FILED	NUMBER EXTRA
BASIC FEE (37 CFR 1.16(a), (b), or (c))		
SEARCH FEE (37 CFR 1.16(d), (f), or (m))		
EXAMINATION FEE (37 CFR 1.16(e), (p), or (q))		
TOTAL CLAIMS (37 CFR 1.16(i))	14 minus 20 =	•
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	•
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).	
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))		

SMALL ENTITY	
RATE (\$)	FEE (\$)
X	=
X	=
TOTAL	

OTHER THAN SMALL ENTITY	
RATE (\$)	FEE (\$)
	<b>740</b>
X	<b>18</b> =
X	<b>84</b> =
	<b>+250</b>
	<b>+280</b>
TOTAL	

\* If the difference in column 1 is less than zero, enter "0" in column 2.

**APPLICATION AS AMENDED - PART II**

**9-22-05** (Column 1) (Column 2) (Column 3)

AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total (37 CFR 1.16(i))	<b>14</b> Minus	<b>20</b>	=
Independent (37 CFR 1.16(h))	<b>2</b> Minus	<b>3</b>	=
Application Size Fee (37 CFR 1.16(s))			
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))			

SMALL ENTITY	
RATE (\$)	ADDITIONAL FEE (\$)
X	=
X	=
TOTAL ADD'L FEE	

OTHER THAN SMALL ENTITY	
RATE (\$)	ADDITIONAL FEE (\$)
X	<b>50</b> =
X	<b>200</b> =
	<b>+360</b>
TOTAL ADD'L FEE	

**3306** (Column 1) (Column 2) (Column 3)

AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total (37 CFR 1.16(i))	<b>14</b> Minus	<b>20</b>	=
Independent (37 CFR 1.16(h))	<b>2</b> Minus	<b>3</b>	=
Application Size Fee (37 CFR 1.16(s))			
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))			

SMALL ENTITY	
RATE (\$)	ADDITIONAL FEE (\$)
X	=
X	=
TOTAL ADD'L FEE	

OTHER THAN SMALL ENTITY	
RATE (\$)	ADDITIONAL FEE (\$)
X	=
X	=
TOTAL ADD'L FEE	

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.  
\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".  
\*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".  
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632
27871	7590	04/13/2006	EXAMINER	
BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA			GELAGAY, SHEWAYE	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 04/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/025,924	VANSTONE ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Shewaye Gelagay	2137	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 1-14 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) ☒ Responsive to communication(s) filed on 03 March 2006.

2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) ☒ Claim(s) 1-14 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.

6) ☒ Claim(s) 1-14 is/are rejected.

7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.

8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All    b) ☐ Some \*    c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_

4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

1. This office action is in response to Applicant's amendment filed on March 3, 2006. Claims 1 and 9 have been amended. Claims 1-14 are pending.

### ***Claim Rejections - 35 USC § 112***

2. In view of the amendment filed March 3, 2006, the Examiner withdraws the rejection of claim 1 under 35 USC 112.

### ***Response to Arguments***

3. Applicant's arguments filed March 3, 2006 have been fully considered but they are not persuasive. In response to the arguments concerning the previously rejected claims, the following comments are made:

The applicant argued Matyas does not teach, "performing a hash". The Examiner disagrees. Matyas teaches generating a seed value and hashing each of these seed values with SHA-1 to produce corresponding hash values. Therefore, Matyas teaches generating a seed and generating hash value by performing a hash function on the seed value. (Col. 5, line 65- Col. 6, line 8). In addition, Matyas further disclose the seed values are also kept secret. (Col. 6, line 24)

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention

where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have been obvious to a person having ordinary skill in the art in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed. Matyas (Col. 7, lines 5-6) This way, further protection is given to the generated key.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "recognize minimize the bias in selection of k and use this bias not provide any steps to avoid the bias") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In this case, Schneier teaches generating a seed value and determining if it is less than order q and Matyas teaches generating a seed value and performing a hash. Therefore, the combination of Schneier and Matyas teaches the limitations of claim 1.

Therefore, all the elements of the claims limitation are explicitly or implicitly or inherently suggested and disclosed by the combination of the references on the record and the previous rejection remains valid unless and otherwise the Applicant added a specific limitation in to the present independent claims, to overcome the rejection without introducing a new matter.

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-2, 4-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Matyas, Jr. et al. (hereinafter Matyas) United States Letter Patent Number 6,307,938.

As per claim 1:

Schneier teaches a method of generating a key over a group of order  $q$ , said method including the steps of:

generating a seed value from a random number generator; (Page 487, line 11; Page 489, lines 15-16)

accepting said output for use as a key if the value thereof is less than said prime number  $q$ ; (Page 487, lines 12-15) and



rejecting said output as a key if said value is not less than said order  $q$ . (Page 487, line 11)

In addition, Schneier further discloses performing a hash function (Page 487, lines 7-8; Page 489, lines 17-18) and determining whether a random number is less than  $q$ . (Page 487, line 11; ... $k$  less than  $q$ )

Schneier does not explicitly disclose a method of performing a hash function on seed number to provide an output and determining whether said output is less than said prime number  $q$ .

Matyas in analogous art, however, discloses a method of performing a hash of each of seed values with SHA-1 to produce hash values; (Col. 6, lines 7-9) and generating seed involving a test to ensure that it falls within a specified range of allowed values and until it satisfies primality test. (Col. 6, line 65-Col. 8, line 35)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Schneier to include a method of performing a hash function on seed number to provide an output and determining whether said output is less than said prime number  $q$ . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Matyas (Col. 7, lines 5-6) in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed.

As per claim 2:

The combination of Schneier and Matyas teach all the subject matter as discussed above. In addition, Schneier further discloses a method wherein another seed value is generated by said random number generator if said output is rejected. (Page 487, line 11; Page 489, line 22)

As per claim 4:

The combination of Schneier and Matyas teach all the subject matter as discussed above. In addition, Schneier discloses a method wherein said key is used for generation of a public key. (Page 487, lines 8-15; Page 488, line 3-8)

As per claim 5:

The combination of Schneier and Matyas teach all the subject matter as discussed above. In addition, Schneier further discloses a method wherein said order  $q$  is prime number represented by a bit string of predetermined length  $l$ . (Page 487, line 1 and Page 488, line 5)

6. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Matyas, Jr. et al. (hereinafter Matyas) United States Letter Patent Number 6,307,938 and further in view of Backal United States Letter Patent Number 6,219,421.

As per claim 7:

The combination of Schneier and Matyas teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein if said output is rejected, said output is incremented by a deterministic function and a hash

function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

Backal in analogous art, however, disclose a method wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key. (Col. 5, lines 61-67)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method of wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Backal (Col. 1, lines 50-51) in order to provide an exceptional degree of security. This way, the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document.

As per claim 8:

The combination of Schneier, Matyas and Backal teach all the subject matter as discussed above. In addition, Backal further discloses a method wherein said step of incrementing includes a further step of adding a particular value to said seed value. (Col. 5, lines 61-67)

As per claim 9:

Schneier teaches a method of generating a key over a group of order  $q$ , said method including the steps of:

generating a seed value from a random number generator; (Page 487, line 11; Page 489, lines 15-16)

accepting said new output as a key  $k$  if said new output has a value less than order  $q$ ; (Page 487, line 11; ... $k$  less than  $q$ ) and

rejecting said new output as a key if said new output has a value less than order  $q$ . (Page 487, line 11)

In addition, Schneier further discloses performing a hash function (Page 487, lines 7-8; Page 489, lines 17-18) and determining whether a random number is less than  $q$ . (Page 487, line 11; ... $k$  less than  $q$ )

Schneier does not explicitly disclose a method of performing a hash function on seed number to provide an output; determining whether said output is less than said prime number  $q$ ; incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ .

Matyas in analogous art, however, discloses a method of performing a hash of each of seed values with SHA-1 to produce hash values; (Col. 6, lines 7-9) and generating seed involving a test to ensure that it falls within a specified range of allowed values and until it satisfies primality test. (Col. 6, line 65-Col. 8, line 35)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner to include a method of performing a hash function on seed number to provide an output and determining whether said output is less than said prime number  $q$ . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Matyas (Col. 7, lines 5-6) in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed.

Both references do not explicitly disclose incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ .

Backal in analogous art, however, disclose a method of incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; (Col. 5, lines 61-67) and

combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ ; (Col. 5, lines 54-60)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and

Matyas to include a method of incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by, Backal (Col. 1, lines 50-51) in order to provide an exceptional degree of security. This way, the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document.

As per claim 10:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein upon rejection of said new output a new seed value is generated by said random number generator. (Page 487, line 11; Page 489, line 22)

As per claim 11:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Backal further discloses a method wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained. (Col. 5, lines 61-67)

As per claim 12:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein a bit string greater than a predetermined length  $l$  is obtained and an  $l$  bit string selected therefrom for comparison with said order  $q$ . (Page 487, line 1 and Page 488, line 5)

As per claim 13:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. In addition, Schenier further discloses a method wherein upon rejection of said bit string of predetermined length  $l$ , a further  $l$  bit string is selected. (Page 487, line 1 and Page 488, line 5)

7. Claims 3 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Matyas, Jr. et al. (hereinafter Matyas) United States Letter Patent Number 6,307,938 in view of Nel et al. (hereinafter Nel) "Generation of Keys for use with the Digital Signature Standard (DSS)" (Pages 6-10).

As per claim 3:

The combination of Schneier and Matyas teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein the step of accepting said output as a key includes a further step of storing said key.

Nel in analogous art, however, discloses a method wherein the step of accepting said output as a key includes a further step of storing said key. (Page 10, Col. 1, lines 3-4)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method wherein the step of accepting said output as a key includes a further step of storing said key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so in order to be able to reuse the key and also to perform auditing on the key generation process.

As per claim 6:

The combination of Schneier, Matyas and Nel teach all the subject matter as discussed above. Both references do not explicitly disclose a method wherein said output from said hash function is a bit string of predetermined length L.

Nel in analogous art, however, discloses a method wherein said output from said hash function is a bit string of predetermined length L. (Page 8, Col. 2, lines 8-11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method wherein said output from said hash function is a bit string of predetermined length L. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Nel et al. (Page 8, Col. 2, lines 6-7) in order to prevent constructing a message which will yield a known value of message digest.

8. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier "Applied Cryptography", (Pages 483-490) in view of Backal United States Letter Patent



Number 6,219,421 and further in view of Nel et al. (hereinafter Nel) "Generatiion of Keys for use with the Digital Signature Standard (DSS)" (Pages 6-10).

As per claim 14:

The combination of Schenier, Matyas and Backal teach all the subject matter as discussed above. Both references do not explicitly disclose method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $l$ .

Nel in analogous art, however, discloses a method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $l$ . (Page 8, Col. 2, lines 8-11)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Scheiner and Matyas to include a method wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $l$ . This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so as suggested by Nel (Page 8, Col. 2, lines 6-7) in order to prevent constructing a message which will yield a known value of message digest.

### ***Conclusion***

**THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Application/Control Number: 10/025,924  
Art Unit: 2137

Page 15

Shewaye Gelagay  
4/4/06




EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER

<b>Search Notes</b> 	<b>Application No.</b>		<b>Applicant(s)</b>	
	10/025,924		VANSTONE ET AL.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Shewaye Gelagay		2133	

SEARCHED			
Class	Subclass	Date	Examiner
380	44	3/4/2005	SG
380	277	3/4/2005	SG
708	250	3/4/2005	SG

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
East Searched	3/4/2005	sg
ACM searched (incrementing seed value)	3/4/2005	SG
IEEE searched (increment and combine seed value)	3/4/2005	SG
Updated East search	11/30/2005	SG
STIC (Fast and Focus) search	11/30/2005	sg
updated East search	4/4/2006	SG

<b>Index of Claims</b> 		<b>Application No.</b> 10/025,924 <b>Examiner</b> Shewaye Gelagay		<b>Applicant(s)</b> VANSTONE ET AL. <b>Art Unit</b> 2133	
---	--	--	--	---	--

✓ Rejected  = Allowed	- (Through numeral) Cancelled  + Restricted	N Non-Elected  I Interference	A Appeal  O Objected
-----------------------------	--	-------------------------------------	----------------------------

Claim	Date
Final	Original
1	3/19/05
2	4/4/05
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	

Claim	Date
Final	Original
51	
52	
53	
54	
55	
56	
57	
58	
59	
60	
61	
62	
63	
64	
65	
66	
67	
68	
69	
70	
71	
72	
73	
74	
75	
76	
77	
78	
79	
80	
81	
82	
83	
84	
85	
86	
87	
88	
89	
90	
91	
92	
93	
94	
95	
96	
97	
98	
99	
100	

Claim	Date
Final	Original
101	
102	
103	
104	
105	
106	
107	
108	
109	
110	
111	
112	
113	
114	
115	
116	
117	
118	
119	
120	
121	
122	
123	
124	
125	
126	
127	
128	
129	
130	
131	
132	
133	
134	
135	
136	
137	
138	
139	
140	
141	
142	
143	
144	
145	
146	
147	
148	
149	
150	



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632
27871	7590	05/05/2006	EXAMINER	
BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA			GELAGAY, SHEWAYE	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 05/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/025,924	VANSTONE ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Shewaye Gelagay	2137	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) ☒ Responsive to communication(s) filed on 03 March 2006.

2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) ☒ Claim(s) 1-14 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.

6) ☒ Claim(s) 1-14 is/are rejected.

7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.

8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) ☐ All    b) ☐ Some \* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.

3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_

4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: \_\_\_\_\_

<b>Interview Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/025,924	VANSTONE ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Shewaye Gelagay	2137	

All participants (applicant, applicant's representative, PTO personnel):

(1) Shewaye Gelagay. (3) \_\_\_\_\_.

(2) Brett Slaney. (4) \_\_\_\_\_.

Date of Interview: 27 April 2006.

Type: a) ☒ Telephonic b) ☐ Video Conference  
c) ☐ Personal [copy given to: 1) ☐ applicant 2) ☐ applicant's representative]

Exhibit shown or demonstration conducted: d) ☐ Yes e) ☐ No.  
If Yes, brief description: \_\_\_\_\_.

Claim(s) discussed: NONE.

Identification of prior art discussed: NONE.

Agreement with respect to the claims f) ☒ was reached. g) ☐ was not reached. h) ☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: Examiner discussed with Mr. Slaney the 1-14 months Reply Date in the final office action mailed 4/13/06 is a typo. The correct Reply Date is 3 months instead of 1-14 months. Examiner has attached herewith the corrected Office Action Summary PTOL-326.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

  
**EMMANUEL L. MOISE**  
SUPERVISORY PATENT EXAMINER

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

\_\_\_\_\_  
Examiner's signature, if required



## Summary of Record of Interview Requirements

### Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

### Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews

#### Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

#### 37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,  
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

### Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632
27871	7590	06/20/2006	EXAMINER	
BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA			GELAGAY, SHEWAYE	
			ART UNIT	PAPER NUMBER
			2137	
DATE MAILED: 06/20/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Interview Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	10/025,924		VANSTONE ET AL.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Shewaye Gelagay		2137	

All participants (applicant, applicant's representative, PTO personnel):

(1) Shewaye Gelagay. (3) \_\_\_\_\_

(2) Brett J. Slaney. (4) \_\_\_\_\_

Date of Interview: 6/16/06.

Type: a) ☒ Telephonic b) ☐ Video Conference  
c) ☐ Personal [copy given to: 1) ☐ applicant 2) ☐ applicant's representative]

Exhibit shown or demonstration conducted: d) ☐ Yes e) ☒ No.  
If Yes, brief description: \_\_\_\_\_

Claim(s) discussed: 1.


Identification of prior art discussed: Schneider and Matyas.

Agreement with respect to the claims f) ☐ was reached. g) ☒ was not reached. h) ☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: Applicant argued the reference applied do not teach accepting the output if it is less than order q and rejecting it otherwise. The Examiner explained the combination of Schneider and Matyas still reads on the claim limitations. Applicant agreed to file a response for the final office action.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

  
**EMMANUEL L. MOISE**  
**SUPERVISORY PATENT EXAMINER**

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

\_\_\_\_\_  
Examiner's signature, if required

## Summary of Record of Interview Requirements

### Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

### Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews

#### Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

#### 37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,  
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

### Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

JUN. 28. 2006 4:40PM

NO. 0351 P. 3

Doc Code:

PTO/SB/21 (09-04)

Approved for use through 07/31/2008, OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



# TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

8

Application Number

10/025,924

Filing Date

12/26/2001

First Named Inventor

VANSTONE, Scott A.

Art Unit

2137

Examiner Name

GELAGAY, Shewaye

Attorney Docket Number

67539/00421

## ENCLOSURES (Check all that apply)

<input type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to TC
<input type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input checked="" type="checkbox"/> Amendment / Reply	<input type="checkbox"/> Petition	<input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input checked="" type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declaration(s)	<input type="checkbox"/> Power of Attorney, Revocation Change of Correspondence Address	<input type="checkbox"/> Status Letter
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Terminal Disclaimer	<input type="checkbox"/> Other Enclosure(s) (please identify below):
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> CD, Number of CD(s) _____	
<input type="checkbox"/> Certified Copy of Priority Document(s)	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Response to Missing Parts/Incomplete Application	Remarks	
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53		

## SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name Blake, Cassels & Graydon LLP

Signature

Printed name John A.S. Orange

Date

26 June 06Reg. No. 29,725

## CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature

Typed or printed name

Date

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

JUN. 28. 2006 4:40PM

NO. 0351 P. 4

Appl. No. 10/025,924

Reply to Office Action of: April 13, 2006



**IN THE UNITED STATES PATENT & TRADEMARK OFFICE**

Appl. No.: 10/025,924

Applicant: VANSTONE, Scott et al.

Filed: December 26, 2001

Title: METHOD OF PUBLIC KEY GENERATION

Art Unit: 2137

Examiner: GELGAY, Shewaye

Docket No.: 67539/00421

Mail Stop AF  
U.S. Patent & Trademark Office  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**RESPONSE AFTER FINAL REJECTION**

Sir:

This is further to the Final Office Action mailed April 13, 2006. Applicant wishes to amend the above-identified application as follows:

**Amendments to the Claims:** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks:** begin on page 5 of this paper.

Appl. No. 10/025,924

Reply to Office Action of: April 13, 2006

**Amendments to the Claims**

This listing of claims will replace all prior versions and listings of claims in the application:

**Listing of claims:**

1. (currently amended) A method of generating a key  $k$  for use in a cryptographic function performed over a group of order  $q$ , said method including the steps of:
  - generating a seed value  $SV$  from a random number generator;
  - performing a hash function  $H()$  on said seed value  $SV$  to provide an output  $H(SV)$ ;
  - determining whether said output  $H(SV)$  is less than said order  $q$ ;
  - accepting said output  $H(SV)$  for use as [[a]] said key  $k$  if the value thereof of said output  $H(SV)$  is less than said order  $q$ ; [[and]]
  - rejecting said output  $H(SV)$  as [[a]] said key if said value is not less than said order  $q$ [[.]]; if said output  $H(SV)$  is rejected, repeating said method; and
  - if said output  $H(SV)$  is accepted, providing said key  $k$  for use in performing said cryptographic function, wherein said key  $k$  is equal to said output  $H(SV)$ .
2. (original) The method of claim 1 wherein another seed value is generated by said random number generator if said output is rejected.
3. (original) The method of claim 1 wherein the step of accepting said output as a key includes a further step of storing said key.
4. (original) The method of claim 1 wherein said key is used for generation of a public key.
5. (previously presented) The method of claim 1 wherein said order  $q$  is a prime number represented by a bit string of predetermined length  $L$ .
6. (previously presented) The method of claim 5 wherein said output from said hash function is a bit string of predetermined length  $L$ .
7. (original) The method of claim 1 wherein if said output is rejected, said output is incremented

Appl. No. 10/025,924

Reply to Office Action of: April 13, 2006

by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

8. (original) The method of claim 7, wherein said step of incrementing includes a further step of adding a particular value to said seed value.

9. (currently amended) A method of generating a key  $k$  for use in a cryptographic function performed over a group of order  $q$ , said method including the steps of:

generating a seed value  $SV$  from a random number generator;

performing a hash function  $HQ$  on said seed number  $SV$  to provide a first output  $H(SV)$ ;

incrementing said seed value  $SV$  by a predetermined function  $fQ$  and performing said

hash function  $HQ$  on said incremented seed value to provide a second output

$H(f(SV))$ ;

combining said first output  $H(SV)$  and second output  $H(f(SV))$  to produce a new output;

determining whether said new output has a value less than said order  $q$ ;

accepting said new output for use as  $[[a]]$  said key  $[[k]]$   $k$  if said new output has a value less than said order  $q$ ;  $[[and]]$

rejecting said new output as  $[[a]]$  said key  $k$  if said new output has a value is not less than said order  $q[[.]]$

if said new output is rejected, repeating said method, and

if said new output is accepted, providing said key  $k$  for use in performing said cryptographic function, wherein said key  $k$  is equal to said new output.

10. (original) The method of claim 9 wherein upon rejection of said new output a new seed value is generated by said random number generator.

11. (original) The method of claim 9 wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained.



Appl. No. 10/025,924

Reply to Office Action of: April 13, 2006

12. (previously presented) The method of claim 9 wherein a bit string greater than a predetermined length  $L$  is obtained and an  $L$  bit string selected therefrom for comparison with said order  $q$ .

13. (previously presented) The method of claim 12 wherein upon rejection of said bit string of predetermined length  $L$ , a further  $L$  bit string is selected.

14. (previously presented) The method of claim 9 wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $L$ .

Appl. No. 10/025,924

Reply to Office Action of: April 13, 2006

**REMARKS**

Applicant wishes to thank the Examiner for reviewing the present application.

Applicant also wishes to thank the Examiner for taking the time to participate in the Applicant initiated telephone interview of June 16, 2006. In the telephone interview, the inventiveness of the claims of the present application was discussed, in particular, arguments were presented with respect to the rejections under 35 U.S.C. 103 regarding Schneier in view of Matyas. In summary, it was argued that neither of the references cited by the Examiner recognize the source of the bias discovered by Daniel Bleichenbacher, as the Applicants have recognized, let alone teach choosing a key such that an output not less than  $q$  is rejected for use as the key as claimed in the present application. The Examiner suggested that the claims be amended to include linking language for the key and the steps that are used to generate the key, in order to emphasize this distinction and to put the claims in better form for reconsideration.

Applicant believes that the amendments made to claims 1 and 9, described below and outlined above, serve to clarify the nature of the methods claimed and to clearly distinguish over the references cited by the Examiner.

**Claim Amendments**

Claim 1 is amended to identify the key by " $k$ ", the seed value by " $SV$ ", and the output by " $H(SV)$ ".

Claim 1 is also amended inserting " $k$  for use in a cryptographic function performed" following "key" on line 1, and inserting the steps "if said output  $H(SV)$  is rejected, repeating said method; and if said output  $H(SV)$  is accepted, providing said key  $k$  for use in performing said cryptographic function, wherein said key  $k$  is equal to said output  $H(SV)$ ." at the end of the claim.

Claim 9 is amended to identify the key by " $k$ ", the seed value by " $SV$ ", and the first output by " $H(SV)$ ", and the second output by " $H(f(SV))$ ".

Claim 9 is also amended inserting " $k$  for use in a cryptographic function performed" following "key" on line 1, and inserting the steps "if said new output is rejected, repeating said method; and if said new output is accepted, providing said key  $k$  for use in performing said cryptographic function, wherein said key  $k$  is equal to said new output." at the end of the claim.

Appl. No. 10/025,924  
Reply to Office Action of: April 13, 2006

### **Claim Rejections**

Claims 1-2 and 4-5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Matyas. Applicant respectfully traverses the rejections as follows.

The present application describes and claims a method of generating a key that avoids the bias discovered by Daniel Bleichenbacher. Applicant has discovered the source of the bias, namely the way in which the key is chosen. Claim 1, as amended, includes determining if the output (hash of seed value) is less than the order  $q$  and if so, the output is accepted as the key. However, if the output is not less than  $q$ , the output is rejected. Accordingly, the bias is avoided by rejecting the key if not less than  $q$ . Applicant advises that amended claim 1 includes the steps of repeating the method if the output is rejected and, if the output is accepted, the key  $k$  is provided for use in performing the cryptographic function whereby the key  $k$  is equal to the output that has been compared to  $q$ . Applicant believes that these additional steps clearly specify how the key is generated, namely by comparing the output with  $q$  until it has a value that is less than  $q$ .

In previous cryptosystems, e.g. DSS, if the value chosen to be used as the key is greater than  $q$  then a mod reduction is performed, which is susceptible to the bias identified by Bleichenbacher. Applicant has recognized the source of the bias and rejects the output instead of performing a reduction to avoid potential attacks. The references relied upon have not recognized this let alone provide any suggestion as to how the bias could be avoided (i.e. the source of the bias). Further, the references cited by the Examiner also do not teach repeating the generation of a seed value and hash thereof until the output is less than  $q$  and do not teach providing the output as the key  $k$  if the output is less than  $q$ . Both Schneier and Matyas are entirely silent in that regard.

Therefore, Applicant believes that the amendments made to claim 1 clearly emphasize the above distinction and as such, claims 1-2 and 4-5 are believed to be patentable over the references cited by the Examiner.

Claims 7-13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Matyas, in further view of Backal; claims 3 and 6 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Matyas, in further view of Nel; and claim 14 has been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Backal, in further view of Nel.

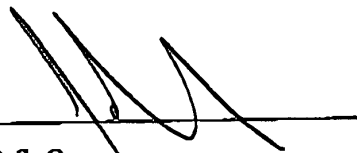
Appl. No. 10/025,924  
Reply to Office Action of: April 13, 2006

As noted above, claim 9 is amended in a manner similar to claim 1 and also includes rejecting an output for use as the key if the output is not less than  $q$ . Claims 7-8, and 10-14 are ultimately dependent on one of claims 1 and 9. Applicant respectfully submits that neither Backal nor Nel teach rejecting an output for use as the key if the output is not less than  $q$ . Accordingly, neither Backal nor Nel teach what Applicant is believed to have shown is missing from both Schneier and Matyas. Therefore, for at least that reason, claims 3, 6 and 7-14 are believed to be patentable over the references cited by the Examiner.

In view of the foregoing, Applicant respectfully submits that all pending claims, namely claims 1-14, are patentably distinguished over the references cited by the Examiner and, as such, are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



John R. S. Orange  
Agent for Applicant  
Registration No. 29,725

Date: 26 July 2006

BLAKE, CASSELS & GRAYDON LLP  
Suite 2800, P.O. Box 25  
199 Bay Street, Commerce Court West  
Toronto, Ontario M5L 1A9  
CANADA

Tel: 416.863.3164  
JRO/BSL

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD						Application or Docket Number	
Substitute for Form PTO-875						10/025 924	
<div style="display: flex; justify-content: space-between;"> <div> <b>CLAIMS AS FILED - PART I</b>            6-28-06 (Column 1)         </div> <div> <b>Amended</b>            (Column 2)         </div> </div>							
FOR		NUMBER FILED		NUMBER EXTRA			
BASIC FEE (37 CFR 1.16(a))							
TOTAL CLAIMS (37 CFR 1.16(c))		14 minus 20 = *		0			
INDEPENDENT CLAIMS (37 CFR 1.16(b))		2 minus 3 = *		0			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(d))				0			
* If the difference in column 1 is less than zero, enter "0" in column 2.							
CLAIMS AS AMENDED - PART II							
(Column 1)		(Column 2)		(Column 3)			
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		
	Total (37 CFR 1.16(c))		Minus **		=		
	Independent (37 CFR 1.16(b))		Minus ***		=		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(d))						
(Column 1)		(Column 2)		(Column 3)			
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		
	Total (37 CFR 1.16(c))		Minus **		=		
	Independent (37 CFR 1.16(b))		Minus ***		=		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(d))						
(Column 1)		(Column 2)		(Column 3)			
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		PRESENT EXTRA		
	Total (37 CFR 1.16(c))		Minus **		=		
	Independent (37 CFR 1.16(b))		Minus ***		=		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(d))						
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.							

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632
27871	7590	08/14/2006	EXAMINER	
BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA			SCHUBERT, KEVIN R	
			ART UNIT	PAPER NUMBER
			2137	
DATE MAILED: 08/14/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

**Advisory Action  
Before the Filing of an Appeal Brief**

Application No.

10/025,924

Applicant(s)

VANSTONE ET AL.

Examiner

Kevin Schubert

Art Unit

2137

**--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

THE REPLY FILED 28 June 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) ☐ The period for reply expires \_\_\_\_\_ months from the mailing date of the final rejection.  
b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**NOTICE OF APPEAL**

2. ☐ The Notice of Appeal was filed on \_\_\_\_\_. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

**AMENDMENTS**

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because  
(a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);  
(b) ☐ They raise the issue of new matter (see NOTE below);  
(c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or  
(d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: See Continuation Sheet. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).  
5. ☐ Applicant's reply has overcome the following rejection(s): \_\_\_\_\_.  
6. ☐ Newly proposed or amended claim(s) \_\_\_\_\_ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).  
7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.  
The status of the claim(s) is (or will be) as follows:  
Claim(s) allowed: \_\_\_\_\_.  
Claim(s) objected to: \_\_\_\_\_.  
Claim(s) rejected: \_\_\_\_\_.  
Claim(s) withdrawn from consideration: \_\_\_\_\_.

**AFFIDAVIT OR OTHER EVIDENCE**

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).  
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).  
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

**REQUEST FOR RECONSIDERATION/OTHER**

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: \_\_\_\_\_.  
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). \_\_\_\_\_.  
13. ☐ Other: \_\_\_\_\_.

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER

Continuation of 3. NOTE: Independent claims 1 and 9 have been amended to recite new limitations. Such amendment of the claims requires further search and/or consideration.



JUN. 28. 2006 4:40PM

NO. 0351 P. 4

Appl. No. 10/025,924

Reply to Office Action of: April 13, 2006



**IN THE UNITED STATES PATENT & TRADEMARK OFFICE**

Appl. No.: 10/025,924

Applicant: VANSTONE, Scott et al.

Filed: December 26, 2001

Title: METHOD OF PUBLIC KEY GENERATION

Art Unit: 2137

Examiner: GELGAY, Shewaye

Docket No.: 67539/00421

Mail Stop AF  
U.S. Patent & Trademark Office  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**RESPONSE AFTER FINAL REJECTION**

Sir:

This is further to the Final Office Action mailed April 13, 2006. Applicant wishes to amend the above-identified application as follows:

Amendments to the Claims: are reflected in the listing of claims which begins on page 2 of this paper.

Remarks: begin on page 5 of this paper.

Do not enter  
KS  
8/7/06

Doc Code:

PTO/SB/30 (04-05)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

# REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL

Address to:  
Mail Stop RCE  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

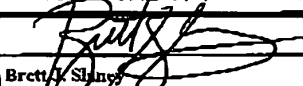
Application Number	10/025,924
Filing Date	12/26/2001
First Named Inventor	VANSTONE, Scott A.
Art Unit	2137
Examiner Name	SCHUBERT, Kevin R.
Attorney Docket Number	67539/00421

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application. Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

- Submission required under 37 CFR 1.114** Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).
  - ☒ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.
    - ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on \_\_\_\_\_
    - ☐ Other \_\_\_\_\_
  - ☐ Enclosed
    - ☐ Amendment/Reply
    - ☐ Affidavit(s)/Declaration(s)
    - ☐ Information Disclosure Statement (IDS)
    - ☐ Other \_\_\_\_\_
- Miscellaneous**
  - ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of \_\_\_\_\_ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(f) required)
  - ☐ Other \_\_\_\_\_
- Fees** The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
  - ☒ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments to Deposit Account No. 02-2553. I have enclosed a duplicate copy of this sheet.
    - ☒ RCE fee required under 37 CFR 1.17(e) 08/31/2006 MAHME1 00000034 022553 10025924
    - ☒ Extension of time fee (37 CFR 1.136 and 1.17) 01 FC:1801 790.00 DA
    - ☐ Other \_\_\_\_\_
  - ☐ Check in the amount of \$ \_\_\_\_\_ enclosed
  - ☐ Payment by credit card (Form PTO-2038 enclosed)

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

## SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature		Date	August 29, 2006
Name (Print / Type)	Brett J. Shiner	Registration No.	58,772

## CERTIFICATE OF MAILING OR TRANSMISSION

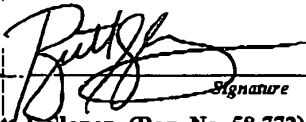
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner For Patents, P.O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature		Date	
Name (Print / Type)			

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete. Including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing the burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

BEST AVAILABLE COPY

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b> (Large Entity)				Docket No. 67539/00421	
In Re Application Of: VANSTONE, Scott A.					
Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
10/025,924	12/26/2001	SCHUBERT, Kevin R.	27871	2137	7632
Invention: <b>METHOD OF PUBLIC KEY GENERATION</b>					
<u>COMMISSIONER FOR PATENTS:</u>					
This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a response to the Office Action of <u>04/13/2006</u> in the above-identified application. <span style="display: block; text-align: center;"><small>Date</small></span>					
The requested extension is as follows (check time period desired):					
<input type="checkbox"/> One month <input checked="" type="checkbox"/> Two months <input type="checkbox"/> Three months <input type="checkbox"/> Four months <input type="checkbox"/> Five months					
from: <u>July 13, 2006</u>		until: <u>September 13, 2006</u>			
<span style="display: block; text-align: center;"><small>Date</small></span>		<span style="display: block; text-align: center;"><small>Date</small></span>			
The fee for the extension of time is \$450 and is to be paid as follows:					
<input type="checkbox"/> A check in the amount of the fee is enclosed. <input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. 02-2553 <input type="checkbox"/> If an additional extension of time is required, please consider this a petition therefor and charge any additional fees which may be required to Deposit Account No. 02-2553 <input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.					
<b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b>					
 Signature		Dated: August 29, 2006			
Brett J. Slaney (Reg. No. 58,772) Blake, Cassels & Graydon LLP Box 25, Commerce Court West 199 Bay Street Toronto, Ontario M5L 1A9 Canada Tel: (416) 863-2518 Fax: (416) 863-2653		08/31/2006: KWH/MSH 02 FC:1252      450.00 DA      10025924			
cc:		<div style="border: 1px solid black; padding: 5px;">         I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on          _____          (Date)          _____          Signature of Person Mailing Correspondence          _____          Typed or Printed Name of Person Mailing Correspondence       </div>			

P12LARGE/REV10

BEST AVAILABLE COPY

PTO/SB/21 (09-04)

Doc Code:

Approved for use through 07/31/2008. OMB 0651-0031  
U.S. Patent and Trademark Office U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



# TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

4

Application Number

10/025,924

Filing Date

12/26/2001

First Named Inventor

VANSTONE, Scott A.

Art Unit

2137

Examiner Name

SCHUBERT, Kevin R.

Attorney Docket Number

67539/00421

## ENCLOSURES (Check all that apply)

☐ Fee Transmittal Form☐ Fee Attached☐ Amendment / Reply☐ After Final☐ Affidavits/declarations☒ Extension of Time Request☐ Express Abandonment Request☐ Information Disclosure Statement☐ Certified Copy of Priority Document(s)☐ Response to Missing Parts/ Incomplete Application☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53☐ Drawing(s)☐ Licensing-related Papers☐ Petition☐ Petition to Convert to a Provisional Application☐ Power of Attorney, Revocation Change of Correspondence Address☐ Terminal Disclaimer☐ Request for Refund☐ CD, Number of CD(s) \_\_\_\_\_☐ Landscape Table on CD☐ After Allowance Communication to TC☐ Appeal Communication to Board of Appeals and Interferences☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)☐ Proprietary Information☐ Status Letter☒ Other Enclosure(s) (please identify below):

1) Request for Continued Examination (RCE) Transmittal

Remarks

## SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name Blake, Cassels &amp; Gonyon LLP

Signature

Printed name

Brett A. Shaffer

Date

August 29, 2006

Reg. No.

58,772

## CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature

Typed or printed name

Date

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	861	(VANSTONE near SCOTT) (VADEKAR near ASHOK) (LAMBERT near ROBERT) (GALLANT near ROBERT) (BROWN near DANIEL) (MENEZES near ALFRED)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 09:44
L3	32	2 and hash\$4 same order	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 09:45
L4	781	380/44.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 09:45
L5	1110	380/277.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 09:46
L6	636	708/250.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 09:46
S1	0	hash\$4 same key with generat\$4 same repeat\$4 with reject\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:14
S2	10	key with generat\$4 same repeat\$4 with reject\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:15
S3	10	key with generat\$4 same repeat\$4 same reject\$4 with (key output)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:18
S4	148	debellis.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:17

## EAST Search History

S5	9	S4 and hash\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:17
S6	42	key with generat\$4 and repeat\$4 same reject\$4 with (key output)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:19
S7	25	S6 and @ad<"20001227"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:21
S8	3340	hash\$4 with key with generat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:21
S9	110	S8 same repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:27
S10	44	S9 and @ad<"20001227"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:21
S11	0	S8 and repeat\$4 with weak	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:27
S12	10	key with generat\$4 same repeat\$4 with weak	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 06:27
S13	19	weak with key with repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 06:34
S14	37	weak with key same repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 06:36

10/10/06 9:46:35 AM

C:\Documents and Settings\mpyzocha1\My Documents\EAST\Workspaces\10025924.wsp

Page 2

## EAST Search History

S15	40	(insecure invalid) with key with repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 06:57
S16	0	hash\$4 with seed same repeat\$4 with (weak reject\$4 invalid insecure)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 06:58
S17	44	hash\$4 with seed same repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 07:04
S18	1	(PRNG ("psuedo random number generator")) same hash\$4 same seed same repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 07:07
S19	4	(PRNG ("psuedo random number generator")) and hash\$4 same seed same repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 07:07
S20	0	hash\$4 same seed same repeat\$4 with (reject\$4 weak)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/10/10 07:07
S21	0	(PRNG ("psuedo random number generator")) same hash\$4 same seed same weak	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 07:07
S22	0	(PRNG ("psuedo random number generator")) same weak	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 07:08
S23	50	(PRNG ("psuedo random number generator")) and weak	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/10/10 07:44
S24	1	("6307938").PN.	US-PGPUB; USPAT	OR	OFF	2006/10/10 07:46
S25	1	("6219421").PN.	US-PGPUB; USPAT	OR	OFF	2006/10/10 07:46



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632
27871	7590	11/03/2006	EXAMINER	
BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA			PYZOCHA, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2137	
DATE MAILED: 11/03/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.



<b>Office Action Summary</b>	<b>Application No.</b> 10/025,924	<b>Applicant(s)</b> VANSTONE ET AL.	
	<b>Examiner</b> Michael Pyzocha	<b>Art Unit</b> 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 29 August 2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-14 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-14 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. Claims 1-14 are pending.
2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 08/29/2006 has been entered.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 2, 4, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (US 6195433) (hereinafter Vanstone) in view of Schneier (Applied

Art Unit: 2137

Cryptography) and further in view of Matyas Jr. et al. (US 6307938) (hereinafter Matyas).

As per claim 1, Vanstone discloses a method for generating a  $k$  for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see column 3 lines 37-39); performing a hash function on said seed value to provide an output (see column 3 lines 41-45); determining if the outputted value is accepted or rejected (see column 3 line 51 through column 4 line 44); repeating the method if the output is rejected (see column 3 line 51 through column 4 line 44); and if the output is accepted, providing the key for use in performing said cryptographic function wherein said key is equal to said output (see column 3 lines 37-45).

Vanstone fails to disclose the steps of determining and accepting/rejecting based on an order  $q$ .

However, Schneier teaches the steps of accepting/rejecting based on an order  $q$  (see page 487 lines 12-15 and line 11) and Matyas teaches determining whether an output is less than a prime number  $q$  (see column 6 line 65 through column 8 line 35).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the tests of Schneier and Matyas in the key generation system of Vanstone.

Motivation to do so would have been to use the well-known DSA (see Schneier pages 486-487) and in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed (see Matyas column 7 lines 5-6).

As per claim 2, the modified Vanstone, Schneier, and Matyas system discloses another seed value is generated by said random number generator if said output is rejected (see Schneier page 487 line 11; Page 489, line 22 and Vanstone column 3 line 51 through column 4 line 44).

As per claim 4, the modified Vanstone, Schneier, and Matyas system discloses said key is used for generation of a public key (see Schneier page 487 lines 8-15; page 488 lines 3-8 and Vanstone column 4 lines 45-48).

As per claim 5, the modified Vanstone, Schneier, and Matyas system discloses a method wherein said order  $q$  is prime number represented by a bit string of predetermined length  $L$  (see Schneier age 487, line 1 and Page 488, line 5).

5. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Vanstone, Schneier, and Matyas system as applied to claim 1 above, and further in view of Backal (US 6219421).

As per claim 7, the modified Vanstone, Schneier, and Matyas system fails to disclose if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

However, Backal teaches this limitation (see column 5 lines 61-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incremental by a deterministic function in the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 8, the modified Vanstone, Schneier, Matyas, and Backal system incrementing includes a further step of adding a particular value to said seed value (see Backal column 5, lines 61-67).

As per claim 9, the modified Vanstone, Schneier, and Matyas system discloses a method for generating a  $k$  for use in a

Art Unit: 2137

cryptographic function including the steps of: generating a seed value from a random number generator (see Vanstone column 3 lines 37-39); performing a hash function on said seed value to provide an output (see Vanstone column 3 lines 41-45); determining if the outputted value is accepted or rejected (see Vanstone column 3 line 51 through column 4 line 44); repeating the method if the output is rejected (see Vanstone column 3 line 51 through column 4 line 44); and if the output is accepted, providing the key for use in performing said cryptographic function wherein said key is equal to said output (see Vanstone column 3 lines 37-45). The determination and accepting/rejection based on the order  $q$  being taught by Schneier and Matyas as applied to claim 1.

The modified Vanstone, Schneier, and Matyas system fails to disclose incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ .

However, Backal teaches incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output (see column 5, lines 61-67); and combining said first output and second output

Art Unit: 2137

to produce a new output; determining whether said new output has a value less than said order  $q$  (see column 5, lines 54-60).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incrementing and combining of Backal in the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 10, the modified Vanstone, Schneier, Matyas, and Backal system discloses wherein upon rejection of said new output a new seed value is generated by said random number generator (see Schneier page 487, line 11 and Page 489, line 22).

As per claim 11, the modified Vanstone, Schneier, Matyas, and Backal system discloses wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained (see Backal column 5, lines 61-67).

As per claim 12, the modified Vanstone, Schneier, Matyas, and Backal system wherein a bit string greater than a

Art Unit: 2137

predetermined length L is obtained and an L bit string selected therefrom for comparison with said order q (see Schneier age 487, line 1 and Page 488, line 5).

As per claim 13, the modified Vanstone, Schneier, Matyas, and Backal system wherein upon rejection of said bit string of predetermined length L, a further L bit string is selected (see Schneier age 487, line 1 and Page 488, line 5).

6. Claims 3, 6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Vanstone, Schneier, and Matyas system (alone or in combination with Backal) as applied to claims 1 and 9 above, and further in view of Nel et al. (Generation of Keys for use with the Digital Signature Standard (DSS)) (hereinafter Nel).

As per claim 3, the modified Vanstone, Schneier, and Matyas system fails to disclose storing the key.

However, Nel teaches storing the key (see page 10 column 1 lines 3-4).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store the key of the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to be able to reuse the key and also perform auditing on the key generation process.



As per claim 6, the modified Vanstone, Schneier, and Matyas system fails to disclose the output from said hash function is a bit string of predetermined length L.

However, Nel teaches the output from said hash function is a bit string of predetermined length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the predetermined output length in the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

As per claim 14, the modified Vanstone, Schneier, Matyas, and Backal system fails to disclose combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L.

However, Nel teaches combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to reject excess bits to

form a predetermined length in the modified Vanstone, Schneier, Matyas, and Backal system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

7. Claims 1, 2, 4, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier (Applied Cryptography) in view of Matyas Jr. et al. (US 6307938) (hereinafter Matyas) and further in view of Patel (US 6327660).

As per claim 1, Schneier discloses a method for generating a  $k$  for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see page 487 line 11 and page 489 lines 15-16); determining if the outputted value is accepted or rejected based on an order  $q$  (see page 487 lines 12-15).

Schneier fails to disclose performing a hash function on seed number to provide an output, determining whether said output is less than said prime number  $q$  and repeating the method if the key is rejected and using the accepted key to perform a cryptographic function.

However, Matyas teaches performing a hash of each of seed values with SHA-I to produce hash values (see column 6, lines 7-

9) and determining whether an output is less than a prime number  $q$  (see column 6 line 65 through column 8 line 35) and Patel teaches repeating the method if the key is rejected and using the accepted key to perform a cryptographic function (see column 6 lines 26-47).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the tests of Matyas and the repeating of Patel in the system of Schneier.

Motivation to do so would have been to and in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed (see Matyas column 7 lines 5-6) and to produce keys which are not weak (see Patel column 6 lines 26-47).

As per claim 2, the modified Schneier, Matyas, and Patel system discloses another seed value is generated by said random number generator if said output is rejected (see Schneier page 487 line 11; Page 489, line 22).

As per claim 4, the modified Schneier, Matyas, and Patel system discloses said key is used for generation of a public key (see Schneier page 487 lines 8-15; page 488 lines 3-8).

As per claim 5, the modified Schneier, Matyas, and Patel system discloses a method wherein said order  $q$  is prime number

Art Unit: 2137

represented by a bit string of predetermined length L (see Schneier age 487, line 1 and Page 488, line 5).

8. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Matyas, and Patel system as applied to claim 1 above, and further in view of Backal (US 6219421).

As per claim 7, the modified Schneier, Matyas, and Patel system fails to disclose if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

However, Backal teaches this limitation (see column 5 lines 61-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incremental by a deterministic function in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 8, the modified Schneier, Matyas, Patel, and Backal system incrementing includes a further step of adding a particular value to said seed value (see Backal column 5, lines 61-67).

As per claim 9, the modified Schneier, Matyas, and Patel system discloses a method for generating a  $k$  for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see page 487 line 11 and page 489 lines 15-16); determining if the outputted value is accepted or rejected based on an order  $q$  (see page 487 lines 12-15). The hashing, determining and repeating are as taught in claim 1 by Matyas and Patel.

The modified Schneier, Matyas, and Patel system fails to disclose incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ .

However, Backal teaches incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output (see column 5, lines 61-67); and combining said first output and second output

to produce a new output; determining whether said new output has a value less than said order  $q$  (see column 5, lines 54-60).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incrementing and combining of Backal in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 10, the modified Schneier, Matyas, Patel, and Backal system discloses wherein upon rejection of said new output a new seed value is generated by said random number generator (see Schneier page 487, line 11 and Page 489, line 22).

As per claim 11, the modified Schneier, Matyas, Patel, and Backal system discloses wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained (see Backal column 5, lines 61-67).

As per claim 12, the modified Schneier, Matyas, Patel, and Backal system wherein a bit string greater than a predetermined

length L is obtained and an L bit string selected therefrom for comparison with said order q (see Schneier age 487, line 1 and Page 488, line 5).

As per claim 13, the modified Schneier, Matyas, Patel, and Backal system wherein upon rejection of said bit string of predetermined length L, a further L bit string is selected (see Schneier age 487, line 1 and Page 488, line 5).

9. Claims 3, 6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Matyas, and Patel system (alone or in combination with Backal) as applied to claims 1 and 9 above, and further in view of Nel et al. (Generation of Keys for use with the Digital Signature Standard (DSS)) (hereinafter Nel).

As per claim 3, the modified Schneier, Matyas, and Patel system fails to disclose storing the key.

However, Nel teaches storing the key (see page 10 column 1 lines 3-4).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store the key of the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to be able to reuse the key and also perform auditing on the key generation process.

As per claim 6, the modified Schneier, Matyas, and Patel system fails to disclose the output from said hash function is a bit string of predetermined length L.

However, Nel teaches the output from said hash function is a bit string of predetermined length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the predetermined output length in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

As per claim 14, the modified Schneier, Matyas, and Patel system fails to disclose combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L.

However, Nel teaches combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to reject excess bits to



Art Unit: 2137

form a predetermined length in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

#### ***Response to Arguments***

10. Applicant's arguments with respect to claims 1-14 have been considered but are moot in view of the new ground(s) of rejection.

#### ***Conclusion***

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Krasinski et al. (US 20030084332) and Chen et al. (US 20020116527) teach a method of repeating a method when a key is rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be

Art Unit: 2137

reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER

<b>Notice of References Cited</b>	Application/Control No. 10/025,924	Applicant(s)/Patent Under Reexamination VANSTONE ET AL.	
	Examiner Michael Pyzocha	Art Unit 2137	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,195,433 B1	02-2001	Vanstone et al.	380/285
*	B	US-6,327,660 B1	12-2001	Patel, Baiju V.	713/193
*	C	US-2003/0084332 A1	05-2003	Krasinski et al.	713/200
*	D	US-2002/0116527 A1	08-2002	Chen et al.	709/245
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

**FOREIGN PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

# Index of Claims



Application/Control No.

10/025,924

Examiner

Michael Pyzocha

Applicant(s)/Patent under Reexamination

VANSTONE ET AL.

Art Unit

2137

✓	Rejected
=	Allowed

—	(Through numeral) Cancelled
+	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claim		Date											
Final	Original	10/10/06											
	1	✓											
	2	✓											
	3	✓											
	4	✓											
	5	✓											
	6	✓											
	7	✓											
	8	✓											
	9	✓											
	10	✓											
	11	✓											
	12	✓											
	13	✓											
	14	✓											
	15												
	16												
	17												
	18												
	19												
	20												
	21												
	22												
	23												
	24												
	25												
	26												
	27												
	28												
	29												
	30												
	31												
	32												
	33												
	34												
	35												
	36												
	37												
	38												
	39												
	40												
	41												
	42												
	43												
	44												
	45												
	46												
	47												
	48												
	49												
	50												

Claim		Date											
Final	Original												
	51												
	52												
	53												
	54												
	55												
	56												
	57												
	58												
	59												
	60												
	61												
	62												
	63												
	64												
	65												
	66												
	67												
	68												
	69												
	70												
	71												
	72												
	73												
	74												
	75												
	76												
	77												
	78												
	79												
	80												
	81												
	82												
	83												
	84												
	85												
	86												
	87												
	88												
	89												
	90												
	91												
	92												
	93												
	94												
	95												
	96												
	97												
	98												
	99												
	100												

Claim		Date											
Final	Original												
	101												
	102												
	103												
	104												
	105												
	106												
	107												
	108												
	109												
	110												
	111												
	112												
	113												
	114												
	115												
	116												
	117												
	118												
	119												
	120												
	121												
	122												
	123												
	124												
	125												
	126												
	127												
	128												
	129												
	130												
	131												
	132												
	133												
	134												
	135												
	136												
	137												
	138												
	139												
	140												
	141												
	142												
	143												
	144												
	145												
	146												
	147												
	148												
	149												
	150												

**Search Notes**

Application/Control No.

10/025,924

Examiner

Michael Pyzocha

Applicant(s)/Patent under  
Reexamination

VANSTONE ET AL.

Art Unit

2137

**SEARCHED**

Class	Subclass	Date	Examiner
380	44	10/10/2006	MJP
380	277	10/10/2006	MJP
708	250	10/10/2006	MJP

**INTERFERENCE SEARCHED**

Class	Subclass	Date	Examiner

**SEARCH NOTES  
(INCLUDING SEARCH STRATEGY)**

	DATE	EXMR
BRS search USPAT, USPGPUB, EPO, JPO, IBM, DERWENT see attached search history	10/10/2006	MJP
all claims have been reviewed for 35 USC non-statutory subject matter	10/10/2006	MJP

Appl. No. 10/025,924  
Reply to Office Action of: November 3, 2006

**IN THE UNITED STATES PATENT & TRADEMARK OFFICE**

Appl. No.: **10/025,924**  
Applicant: **VANSTONE, Scott et al.**  
Filed: **December 26, 2001**  
Title: **METHOD OF PUBLIC KEY GENERATION**  
Art Unit: **2137**  
Examiner: **PYZOCHA, Michael J.**  
Docket No.: **67539/00421**

Mail Stop Amendment  
U.S. Patent & Trademark Office  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**RESPONSE**

Sir:

This is further to the Office Action dated November 3, 2006. Applicant advises that a request for a one-month extension of time is being filed concurrently herewith. Applicant wishes to present the following remarks:

**Remarks:** begin on page 2 of this paper.

### **REMARKS**

Claims 1, 2, 4 and 5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone (US 6,195,433), in view of Schneier (Applied Cryptography), in further view of Matyas (6,307,938). Applicant respectfully traverses the rejections as follows.

Vanstone teaches a private key validation scheme that comprises generating a private key from a random number and testing the number against a predetermined set of criteria. As noted by the Examiner, Vanstone teaches generating a seed value, hashing the seed value and then shaping the output of the hash to be used as a private key. The Examiner acknowledges that Vanstone does not teach accepting/rejecting the key based on an order  $q$ . However, the Examiner turns to Schneier and Matyas as teaching accepting/rejecting a key based on an order  $q$ .

Upon a careful review of Vanstone (as explained below), it is clear that not only does Vanstone not teach choosing a key that is less than  $q$  but there is clear direction to do the opposite. Also, even if, for the sake of argument, one were to combine Vanstone with either or both Schneier and Matyas, neither Schneier nor Matyas teach testing an output to be used as a key if the value is less than an order  $q$ .

As Applicant has noted several times in previous responses, the present application describes and claims a method of generating a key that avoids the bias discovered by Daniel Bleichenbacher. The inventors have recognized the source of the bias, namely in how the key is chosen and have recognized that by choosing the key to be of an order less than  $q$ , the bias can be avoided.

Vanstone does not acknowledge this bias and is not concerned with choosing a key if the computed output is less than an order  $q$ . In fact, upon a careful read of Vanstone, it is clear that one of the tests for choosing the key involves validating the length of the seed (which is hashed to generate the key), to ensure that it is larger than  $n$  - the prime order of the generating point  $G$  (see col. 5, lines 16-17). Therefore, not only does Vanstone not teach determining whether to choose an output as a key based on whether the output is less than an order  $q$ , but clearly teaches adopting a criterion that looks for quite the opposite relationship. As such, there is nothing to suggest that the key be accepted if less than a prime order only to accept the seed value if it is larger than a prime order.

Notwithstanding the above, Applicant also believes that the Examiner has misconstrued

the secondary reference Schneier and the tertiary reference Matyas. In particular, the Examiner points again to page 487 of Schneier (lines 12-15). However, in this passage, Schneier teaches choosing a random value  $k$  that is less than  $q$  which is used to generate signature components  $r$  and  $s$ . Applicant believes that the Examiner has again made a leap of logic in modifying the teachings of Schneier to fit with what is missing from the primary reference Vanstone. Vanstone teaches choosing a key whereas the passage in Schneier teaches choosing a random value used in generating signature components. Schneier does not suggest that the value  $k$  can be used as a key. In fact, on page 487 of Schneier, the private key is said to be  $x$  and the public key is said to be  $y$ , not  $k$ .

In any event, Vanstone still teaches accepting a seed value used to generate the key based on the seed value being larger than an order  $n$ . As such, there would be no motivation to combine the teachings relied on by the Examiner as they would be contradictory. Moreover, there is no suggestion in Schneier that the random number  $k$  should be used for anything other than generating signature components  $r$  and  $s$ . Accordingly, Applicant believes that the Examiner has combined the cited references without fully considering how the respective teachings would work together. It is believed that the Examiner has read too much into the references cited on the basis of hindsight in view of Applicant's disclosure.

None of the cited references have recognized the bias recognized by the inventors let alone teach how such bias can be avoided. It is therefore believed that claims 1, 2, 4 and 5 clearly and patentably distinguish over the combination of cited references.

Claims 7-13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, in view of Schneier, in further view of Matyas (Vanstone/Schneier/Matyas), in further view of Backal (US 6,219,421). Applicant respectfully traverses the rejections as follows.

Backal appears to have been cited as teaching incrementing a seed value by a predetermined function. Claims 7 and 8 are dependent on claim 1, which Applicant is believed to have shown distinguishes over Vanstone/Schneier/Matyas. Therefore, Backal must at least teach what is missing from Vanstone/Schneier/Matyas. Applicant respectfully submits that Backal does not teach choosing a key based on whether or not it is less than an order  $q$ .

Therefore, Backal does not teach what is missing from Vanstone/Schneier/Matyas and claims 7 and 8 are believed to distinguish over Vanstone/Schneier/Matyas in further view of Backal. Similar arguments apply with respect to claims 9-13. As such, claims 7-13 are believed



to be patentably distinguished over the references cited by the Examiner.

Claims 3, 6 and 14 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, in view of Schneier, in further view of Matyas (Vanstone/Schneier/Matyas), in further view of Nel (Generation of Keys for use with the Digital Signature Standard (DSS)). Applicant respectfully traverses the rejections as follows.

Claims 3, 6 and 14 are dependent on either claim 1 or claim 9, which Applicant is believed to have shown distinguish over Vanstone/Schneier/Matyas. Therefore, Nel must at least teach what is missing from Vanstone/Schneier/Matyas. Applicant respectfully submits that Nel does not teach choosing a key based on whether or not it is less than an order  $q$ . Therefore, Nel does not teach what is missing from Vanstone/Schneier/Matyas and claims 3, 6 and 14 are believed to distinguish over Vanstone/Schneier/Matyas in further view of Nel. As such, claims 3, 6 and 14 are believed to be patentably distinguished over the references cited by the Examiner.

Claims 1, 2, 4 and 5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, in view of Matyas, in further view of Patel (US 6,327,660)

As noted above, the present application describes and claims a method of generating a key that avoids the bias discovered by Daniel Bleichenbacher. The inventors have recognized the source of the bias, namely in how the key is chosen and have recognized that by choosing the key to be of an order less than  $q$ , the bias can be avoided.

Again, the Examiner points to page 487 of Schneier (lines 12-15) as teaching choosing a key based on a value being less than an order  $q$ . However, in this passage, Schneier teaches choosing a random value  $k$  that is less than  $q$  which is used to generate signature components  $r$  and  $s$ . The Examiner acknowledges that Schneier does not teach computing a hash of a seed value and points to Matyas as teaching such a feature. However, Applicant again points out that there is nothing in Matyas to suggest modifying Schneier such that the value  $k$  is used as a key. It is believed that the Examiner has again made a leap of logic in saying that it would be obvious to combine and/or modify these references to fit what is claimed. None of the references suggest the claimed feature of determining whether an output is less than an order  $q$  and if so, using that output as a key.

Patel teaches securing a communication link before boot. However, Patel clearly does not teach what Applicant believes is missing from Schneier and Matyas. Therefore, the arguments regarding Vanstone/Schneier/Matyas equally apply to Schneier/Matyas/Patel and

Applicant believes these rejections are no more relevant than those regarding Vanstone/Schneier/Matyas.


None of the cited references have recognized the bias recognized by the inventors let alone teach how such bias can be avoided. It is therefore believed that claims 1, 2, 4 and 5 also clearly and patentably distinguish over Schneier/Matyas/Patel.

Claims 7-13 have been rejected under 35 U.S.C. 103(a) regarding Schneier, Matyas, Patel and Backal; and claims 3, 6 and 14 have been rejected under 35 U.S.C. 103(a) regarding Schneier, Matyas, Patel and Nel. As noted above, the combination of Schneier/Matyas/Patel is believed to be no more relevant than the combination of Vanstone/Schneier/Matyas and, as such, similar arguments presented above equally apply in respect of claims 7-13 and 3, 6 and 14.

In view of the foregoing, Applicant believes that claims 1-14 clearly and patentably distinguish over the references cited by the Examiner and are in condition for allowance.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,

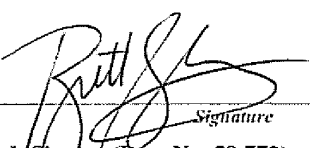


Brett J. Slaney  
Agent for Applicant  
Registration No. 58,772

Date: March 5, 2007

BLAKE, CASSELS & GRAYDON LLP  
Suite 2800, P.O. Box 25  
199 Bay Street, Commerce Court West  
Toronto, Ontario M5L 1A9  
CANADA

Tel: 416-863-2518  
BSL/

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b> <b>(Large Entity)</b>				Docket No. 67539/00421	
In Re Application Of: VANSTONE, Scott A.; et al.					
Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
10/025,924	Dec. 26, 2001	PYZOCHA, Michael J.	27871	2137	7632
Invention: METHOD OF PUBLIC KEY GENERATION					
<u>COMMISSIONER FOR PATENTS:</u>					
This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a response to the Office Action of <u>11/03/2006</u> in the above-identified application. <div style="text-align: center; font-size: small;">Date</div>					
The requested extension is as follows (check time period desired): <div style="display: flex; justify-content: space-between; align-items: flex-start;"> <div style="width: 45%;"> <input checked="" type="checkbox"/> One month     <input type="checkbox"/> Two months     <input type="checkbox"/> Three months     <input type="checkbox"/> Four months     <input type="checkbox"/> Five months </div> <div style="width: 50%;"> from: <u>February 3, 2007</u>     until: <u>March 3, 2007</u>  <div style="display: flex; justify-content: space-between; font-size: x-small;"> <span>Date</span> <span>Date</span> </div> </div> </div>					
The fee for the extension of time is \$120 and is to be paid as follows: <input type="checkbox"/> A check in the amount of the fee is enclosed. <input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. 02-2553 <input checked="" type="checkbox"/> If an additional extension of time is required, please consider this a petition therefor and charge any additional fees which may be required to Deposit Account No. 02-2553 <input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.					
<b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b>					
 Brett J. Slaney (Reg. No. 58,772) Blake, Cassels & Graydon LLP Box 25, Commerce Court West, 199 Bay Street Toronto, Ontario, M5L 1A9, Canada  Tel: (416) 863-2518 Fax: (416) 863-2653			Dated: March 5, 2007		
CC:			I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 [37 CFR 1.8(a)] on _____. <div style="text-align: center; font-size: x-small;">(Date)</div> <div style="text-align: center; font-size: x-small;">Signature of Person Mailing Correspondence</div> <div style="text-align: center; font-size: x-small;">Typed or Printed Name of Person Mailing Correspondence</div>		

P12LARGE/REV11

Electronic Patent Application Fee Transmittal				
Application Number:		10025924		
Filing Date:		26-Dec-2001		
Title of Invention:		Method of public key generation		
First Named Inventor/Applicant Name:		Scott A. Vanstone		
Filer:		Brett Joseph Slaney/Judith Martin		
Attorney Docket Number:		00001-0417		
Filed as Large Entity				
Utility      Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with \$0 paid	1251	1	120	120

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				120

Electronic Acknowledgement Receipt	
<b>EFS ID:</b>	1563424
<b>Application Number:</b>	10025924
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7632
<b>Title of Invention:</b>	Method of public key generation
<b>First Named Inventor/Applicant Name:</b>	Scott A. Vanstone
<b>Customer Number:</b>	27871
<b>Filer:</b>	Brett Joseph Slaney/Judith Martin
<b>Filer Authorized By:</b>	Brett Joseph Slaney
<b>Attorney Docket Number:</b>	00001-0417
<b>Receipt Date:</b>	05-MAR-2007
<b>Filing Date:</b>	26-DEC-2001
<b>Time Stamp:</b>	13:16:32
<b>Application Type:</b>	Utility

### Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 120
RAM confirmation Number	1721
Deposit Account	022553
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)				
1		certicom421_OAresponse_w_ext.pdf	254573	yes	6				
	<b>Multipart Description/PDF files in .zip description</b>								
	<b>Document Description</b>		<b>Start</b>	<b>End</b>					
	Amendment - After Non-Final Rejection		1	1					
	Applicant Arguments/Remarks Made in an Amendment		2	5					
	Extension of Time		6	6					
<b>Warnings:</b>									
<b>Information:</b>									
2	Fee Worksheet (PTO-06)	fee-info.pdf	8135	no	2				
<b>Warnings:</b>									
<b>Information:</b>									
<b>Total Files Size (in bytes):</b>			262708						
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>									

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875					Application or Docket Number <b>10/025924</b>	
<b>CLAIMS AS FILED - PART I</b>						
<b>6-28-06</b>		(Column 1)	(Column 2)		SMALL ENTITY OR OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA		RATE	FEE	RATE FEE
BASIC FEE (37 CFR 1.16(a))						
TOTAL CLAIMS (37 CFR 1.16(c))						
14		minus 20 =		0		0
INDEPENDENT CLAIMS (37 CFR 1.16(b))						
2		minus 3 =		0		0
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(d))						
* If the difference in column 1 is less than zero, enter "0" in column 2.						
<b>CLAIMS AS AMENDED - PART II</b>						
<b>3-5-07</b>		(Column 1)	(Column 2)	(Column 3)	SMALL ENTITY OR OTHER THAN SMALL ENTITY	
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE	ADDITIONAL FEE
	Total (37 CFR 1.16(c))	14	Minus	20	=	1
	Independent (37 CFR 1.16(b))	2	Minus	3	=	1
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(d))					
	TOTAL ADD'L FEE					
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE	ADDITIONAL FEE
	Total (37 CFR 1.16(c))	0	Minus	0	=	0
	Independent (37 CFR 1.16(b))	0	Minus	0	=	0
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(d))					
	TOTAL ADD'L FEE					
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE	ADDITIONAL FEE
	Total (37 CFR 1.16(c))	0	Minus	0	=	0
	Independent (37 CFR 1.16(b))	0	Minus	0	=	0
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(d))					
	TOTAL ADD'L FEE					
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p>						

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-0199 and select option 2.



## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	839	380/44.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 09:28
L3	8	L2 and @ad<"20001227" and @pd>"20061010"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 09:28
L4	1180	380/277.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 09:28
L5	9	L4 and @ad<"20001227" and @pd>"20061010"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:28
L6	662	708/250.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 09:28
L7	1	L6 and @ad<"20001227" and @pd>"20061010"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:28
L8	10	key with generat\$4 same repeat\$4 with reject\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:28
L9	0	L8 and @ad<"20001227" and @pd>"20061010"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:29
L10	45	key with generat\$4 and repeat\$4 same reject\$4 with (key output)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:29

## EAST Search History

L11	0	L10 and @ad<"20001227" and @pd>"20061010"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:29
L12	3711	hash\$4 with key with generat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:29
L13	123	L12 same repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:29
L14	1	L13 and @ad<"20001227" and @pd>"20061010"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:29
L15	10	key with generat\$4 same repeat\$4 with weak	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:29
L16	0	L15 and @ad<"20001227" and @pd>"20061010"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:29
L17	19	weak with key with repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 09:29
L18	0	L17 and @ad<"20001227" and @pd>"20061010"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:29
L19	54	(PRNG ("psuedo random number generator")) and weak	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 09:29
L20	0	L19 and @ad<"20001227" and @pd>"20061010"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:29

3/15/07 9:31:13 AM

C:\Documents and Settings\mpyzocha1\My Documents\EAST\Workspaces\10025924-1.wsp

Page 2

## EAST Search History

L21	928	(VANSTONE near SCOTT) (VADEKAR near ASHOK) (LAMBERT near ROBERT) (GALLANT near ROBERT) (BROWN near DANIEL) (MENEZES near ALFRED)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 09:29
L22	36	L21 and hash\$4 same order	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/03/15 09:29
L23	102	generat\$4 with key same less with order	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:30
L24	50	L23 and @ad<"20001227"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:30
L25	677	generat\$4 with key and less near3 order	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:30
L26	12	generat\$4 with key and less near3 order same hash\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/03/15 09:30



mn

# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632
27871 7590 03/20/2007 BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA			EXAMINER PYZOCHA, MICHAEL J	
			ART UNIT 2137	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE		MAIL DATE	DELIVERY MODE	
3 MONTHS		03/20/2007	PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

<b>Office Action Summary</b>	Application No. 10/025,924	Applicant(s) VANSTONE ET AL.	
	Examiner Michael Pyzocha	Art Unit 2137	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) ☒ Responsive to communication(s) filed on 05 March 2007.

2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) ☒ Claim(s) 1-14 is/are pending in the application.

4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.

5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.

6) ☒ Claim(s) 1-14 is/are rejected.

7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.

8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
       Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
       Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
       a) ☐ All    b) ☐ Some \* c) ☐ None of:  
           1. ☐ Certified copies of the priority documents have been received.  
           2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
           3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
       \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
       Paper No(s)/Mail Date \_\_\_\_\_

4) ☐ Interview Summary (PTO-413)  
       Paper No(s)/Mail Date. \_\_\_\_\_

5) ☐ Notice of Informal Patent Application

6) ☐ Other: \_\_\_\_\_

**DETAILED ACTION**

1. Claims 1-14 are pending.
2. Response filed 03/05/2007 has been received and considered.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 2, 4, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (US 6195433) (hereinafter Vanstone) in view of Schneier (Applied Cryptography) and further in view of Matyas Jr. et al. (US 6307938) (hereinafter Matyas).

As per claim 1, Vanstone discloses a method for generating a k for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see column 3 lines 37-39); performing a hash function on said seed value to provide an output (see column 3 lines 41-45); determining if the outputted value is accepted or rejected (see

column 3 line 51 through column 4 line 44); repeating the method if the output is rejected (see column 3 line 51 through column 4 line 44); and if the output is accepted, providing the key for use in performing said cryptographic function wherein said key is equal to said output (see column 3 lines 37-45).

Vanstone fails to disclose the steps of determining and accepting/rejecting based on an order  $q$ .

However, Schneier teaches the steps of accepting/rejecting based on an order  $q$  (see page 487 lines 12-15 and line 11) and Matyas teaches determining whether an output is less than a prime number  $q$  (see column 6 line 65 through column 8 line 35).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the tests of Schneier and Matyas in the key generation system of Vanstone.

Motivation to do so would have been to use the well-known DSA (see Schneier pages 486-487) and in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed (see Matyas column 7 lines 5-6).

As per claim 2, the modified Vanstone, Schneier, and Matyas system discloses another seed value is generated by said random number generator if said output is rejected (see Schneier page

Art Unit: 2137

487 line 11; Page 489, line 22 and Vanstone column 3 line 51 through column 4 line 44).

As per claim 4, the modified Vanstone, Schneier, and Matyas system discloses said key is used for generation of a public key (see Schneier page 487 lines 8-15; page 488 lines 3-8 and Vanstone column 4 lines 45-48).

As per claim 5, the modified Vanstone, Schneier, and Matyas system discloses a method wherein said order  $q$  is prime number represented by a bit string of predetermined length  $L$  (see Schneier page 487, line 1 and Page 488, line 5).

5. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Vanstone, Schneier, and Matyas system as applied to claim 1 above, and further in view of Backal (US 6219421).

As per claim 7, the modified Vanstone, Schneier, and Matyas system fails to disclose if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

However, Backal teaches this limitation (see column 5 lines 61-67).



At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incremental by a deterministic function in the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 8, the modified Vanstone, Schneier, Matyas, and Backal system incrementing includes a further step of adding a particular value to said seed value (see Backal column 5, lines 61-67).

As per claim 9, the modified Vanstone, Schneier, and Matyas system discloses a method for generating a k for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see Vanstone column 3 lines 37-39); performing a hash function on said seed value to provide an output (see Vanstone column 3 lines 41-45); determining if the outputted value is accepted or rejected (see Vanstone column 3 line 51 through column 4 line 44); repeating the method if the output is rejected (see Vanstone column 3 line 51 through column 4 line 44); and if the output is accepted,

Art Unit: 2137

providing the key for use in performing said cryptographic function wherein said key is equal to said output (see Vanstone column 3 lines 37-45). The determination and accepting/rejection based on the order  $q$  being taught by Schneier and Matyas as applied to claim 1.

The modified Vanstone, Schneier, and Matyas system fails to disclose incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ .

However, Backal teaches incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output (see column 5, lines 61-67); and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$  (see column 5, lines 54-60).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incrementing and combining of Backal in the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using

Art Unit: 2137

the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 10, the modified Vanstone, Schneier, Matyas, and Backal system discloses wherein upon rejection of said new output a new seed value is generated by said random number generator (see Schneier page 487, line 11 and Page 489, line 22).

As per claim 11, the modified Vanstone, Schneier, Matyas, and Backal system discloses wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained (see Backal column 5, lines 61-67).

As per claim 12, the modified Vanstone, Schneier, Matyas, and Backal system wherein a bit string greater than a predetermined length  $L$  is obtained and an  $L$  bit string selected therefrom for comparison with said order  $q$  (see Schneier age 487, line 1 and Page 488, line 5).

As per claim 13, the modified Vanstone, Schneier, Matyas, and Backal system wherein upon rejection of said bit string of predetermined length  $L$ , a further  $L$  bit string is selected (see Schneier age 487, line 1 and Page 488, line 5).

Art Unit: 2137

6. Claims 3, 6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Vanstone, Schneier, and Matyas system (alone or in combination with Backal) as applied to claims 1 and 9 above, and further in view of Nel et al. (Generation of Keys for use with the Digital Signature Standard (DSS)) (hereinafter Nel).

As per claim 3, the modified Vanstone, Schneier, and Matyas system fails to disclose storing the key.

However, Nel teaches storing the key (see page 10 column 1 lines 3-4).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store the key of the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to be able to reuse the key and also perform auditing on the key generation process.

As per claim 6, the modified Vanstone, Schneier, and Matyas system fails to disclose the output from said hash function is a bit string of predetermined length L.

However, Nel teaches the output from said hash function is a bit string of predetermined length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the

Art Unit: 2137

predetermined output length in the modified Vanstone, Schneier, and Matyas system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

As per claim 14, the modified Vanstone, Schneier, Matyas, and Backal system fails to disclose combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L.

However, Nel teaches combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to reject excess bits to form a predetermined length in the modified Vanstone, Schneier, Matyas, and Backal system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

7. Claims 1, 2, 4, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier (Applied Cryptography) in

view of Matyas Jr. et al. (US 6307938) (hereinafter Matyas) and further in view of Patel (US 6327660).

As per claim 1, Schneier discloses a method for generating a  $k$  for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see page 487 line 11 and page 489 lines 15-16); determining if the outputted value is accepted or rejected based on an order  $q$  (see page 487 lines 12-15).

Schneier fails to disclose performing a hash function on seed number to provide an output, determining whether said output is less than said prime number  $q$  and repeating the method if the key is rejected and using the accepted key to perform a cryptographic function.

However, Matyas teaches performing a hash of each of seed values with SHA-1 to produce hash values (see column 6, lines 7-9) and determining whether an output is less than a prime number  $q$  (see column 6 line 65 through column 8 line 35) and Patel teaches repeating the method if the key is rejected and using the accepted key to perform a cryptographic function (see column 6 lines 26-47).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the tests of Matyas and the repeating of Patel in the system of Schneier.

Motivation to do so would have been to and in order to provide a system to avoid attack because it is not possible to invert the hash function to determine the required input seed (see Matyas column 7 lines 5-6) and to produce keys which are not weak (see Patel column 6 lines 26-47).

As per claim 2, the modified Schneier, Matyas, and Patel system discloses another seed value is generated by said random number generator if said output is rejected (see Schneier page 487 line 11; Page 489, line 22).

As per claim 4, the modified Schneier, Matyas, and Patel system discloses said key is used for generation of a public key (see Schneier page 487 lines 8-15; page 488 lines 3-8).

As per claim 5, the modified Schneier, Matyas, and Patel system discloses a method wherein said order  $q$  is prime number represented by a bit string of predetermined length  $L$  (see Schneier page 487, line 1 and Page 488, line 5).

8. Claims 7-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Matyas, and Patel system as applied to claim 1 above, and further in view of Backal (US 6219421).

As per claim 7, the modified Schneier, Matyas, and Patel system fails to disclose if said output is rejected, said output is incremented by a deterministic function and a hash function

Art Unit: 2137

is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

However, Backal teaches this limitation (see column 5 lines 61-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incremental by a deterministic function in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using the above method of seed value generation will protect any unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 8, the modified Schneier, Matyas, Patel, and Backal system incrementing includes a further step of adding a particular value to said seed value (see Backal column 5, lines 61-67).

As per claim 9, the modified Schneier, Matyas, and Patel system discloses a method for generating a  $k$  for use in a cryptographic function including the steps of: generating a seed value from a random number generator (see page 487 line 11 and page 489 lines 15-16); determining if the outputted value is



accepted or rejected based on an order  $q$  (see page 487 lines 12-15). The hashing, determining and repeating are as taught in claim 1 by Matyas and Patel.

The modified Schneier, Matyas, and Patel system fails to disclose incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output; and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$ .

However, Backal teaches incrementing said seed value by a predetermined function and performing said hash function on said incremented seed value to provide a second output (see column 5, lines 61-67); and combining said first output and second output to produce a new output; determining whether said new output has a value less than said order  $q$  (see column 5, lines 54-60).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the incrementing and combining of Backal in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to provide an exceptional degree of security because the keys generated using the above method of seed value generation will protect any

Art Unit: 2137

unauthorized person from having access to the digitally signed document (see Backal column 1 lines 50-51).

As per claim 10, the modified Schneier, Matyas, Patel, and Backal system discloses wherein upon rejection of said new output a new seed value is generated by said random number generator (see Schneier page 487, line 11 and Page 489, line 22).

As per claim 11, the modified Schneier, Matyas, Patel, and Backal system discloses wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained (see Backal column 5, lines 61-67).

As per claim 12, the modified Schneier, Matyas, Patel, and Backal system wherein a bit string greater than a predetermined length  $L$  is obtained and an  $L$  bit string selected therefrom for comparison with said order  $q$  (see Schneier age 487, line 1 and Page 488, line 5).

As per claim 13, the modified Schneier, Matyas, Patel, and Backal system wherein upon rejection of said bit string of predetermined length  $L$ , a further  $L$  bit string is selected (see Schneier age 487, line 1 and Page 488, line 5).

9. Claims 3, 6 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Schneier, Matyas, and Patel

Art Unit: 2137

system (alone or in combination with Backal) as applied to claims 1 and 9 above, and further in view of Nel et al. (Generation of Keys for use with the Digital Signature Standard (DSS)) (hereinafter Nel).

As per claim 3, the modified Schneier, Matyas, and Patel system fails to disclose storing the key.

However, Nel teaches storing the key (see page 10 column 1 lines 3-4).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to store the key of the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to be able to reuse the key and also perform auditing on the key generation process.

As per claim 6, the modified Schneier, Matyas, and Patel system fails to disclose the output from said hash function is a bit string of predetermined length L.

However, Nel teaches the output from said hash function is a bit string of predetermined length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the predetermined output length in the modified Schneier, Matyas, and Patel system.

Art Unit: 2137

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

As per claim 14, the modified Schneier, Matyas, and Patel system fails to disclose combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L.

However, Nel teaches combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length L (see page 8, column 2, lines 8-11).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to reject excess bits to form a predetermined length in the modified Schneier, Matyas, and Patel system.

Motivation to do so would have been to prevent constructing a message, which will yield a known value of message digest (see Nel page 8, column 2, lines 6-7).

#### ***Response to Arguments***

10. Applicant's arguments filed 03/05/2007 have been fully considered but they are not persuasive. Applicant argues Schneier fails to teach using the output value as a key;

Vanstone teaches checking that the order is greater than a value, not lower; and the remaining references fail to make up for these deficiencies.

With respect to Applicant's argument that Schneier (when combine with Vanstone and Matyas or Matyas and Patel) fails to use the random value  $k$  as a key, this section of Schneier is describing the DSA algorithm and the value  $k$  is an ephemeral key. Applicant's specification also describes the DSA algorithm in a similar manner as Schneier and in line 16 specifically discloses that the value  $k$  is an ephemeral key. Therefore, the value  $k$  in Schneier is used as a key for use in a cryptographic function.

With respect to Applicant's argument that Vanstone teaches checking that the order is greater than a value, not lower, Examiner agrees, but when combined with Schneier (and Matyas) the system teaches choosing a value to be a key when it is greater than a value and less than a value. Therefore, the combination of Vanstone, Schneier and Matyas teach all of the limitations of claims 1, 2, 4, and 5.

Applicant's arguments that the remaining references fail to make up for the described deficiencies are moot in view of the above response.

**Conclusion**

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Shimbo and Pastor disclose methods of checking the order of a value before using it in a cryptographic system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner

Art Unit: 2137

can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER

<b>Notice of References Cited</b>	Application/Control No. 10/025,924	Applicant(s)/Patent Under Reexamination VANSTONE ET AL.	
	Examiner Michael Pyzocha	Art Unit 2137	Page 1 of 1

**U.S. PATENT DOCUMENTS**

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,088,798 A	07-2000	Shimbo, Atsushi	713/176
*	B	US-5,073,935 A	12-1991	Pastor, Jose	380/30
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

**FOREIGN PATENT DOCUMENTS**


*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

**NON-PATENT DOCUMENTS**

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

\*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)  
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.



<b>Index of Claims</b> 	<b>Application/Control No.</b> 10025924	<b>Applicant(s)/Patent Under Reexamination</b> VANSTONE ET AL.
	<b>Examiner</b> Pyzocha, Michael	<b>Art Unit</b> 2137


✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant				<input type="checkbox"/> CPA		<input type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47	
CLAIM		DATE							
Final	Original	03/15/2007	03/15/2007						
	1	✓	✓						
	2	✓	✓						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	✓						
	7	✓	✓						
	8	✓	✓						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						
	14	✓	✓						

<b>Search Notes</b>  	<b>Application/Control No.</b>  10025924	<b>Applicant(s)/Patent Under Reexamination</b>  VANSTONE ET AL.
	<b>Examiner</b>  Pyzocha, Michael	<b>Art Unit</b>  2137

SEARCHED			
Class	Subclass	Date	Examiner
380	44	10/10/06	MJP
380	277	10/10/06	MJP
708	250	10/10/06	MJP
updated	search	3/15/07	MJP

SEARCH NOTES		
Search Notes	Date	Examiner
BRS search USPAT, USPGPUB, EPO, JPO, IBM, DERWENT see attached search history	10/10/06	MJP
all claims have been reviewed for 35 USC non-statutory subject matter	10/10/06	MJP
new and updated BRS search, see attached search history	3/15/07	MJP

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

**NOTICE OF APPEAL FROM THE PRIMARY EXAMINER TO  
THE BOARD OF PATENT APPEALS AND INTERFERENCES (Large Entity)**

Docket No.  
67539/00421

In Re Application Of: VANSTONE, Scott A., et al.

Application No.	Filing Date	Examiner	Customer No.	Group Art Unit	Confirmation No.
10/025,924	12/26/2001	PYZOCHA, Michael J.	27871	2137	7632

Invention: **METHOD OF PUBLIC KEY GENERATION**

COMMISSIONER FOR PATENTS:

Applicant(s) hereby appeal(s) to the Board of Patent Appeals and Interferences from the decision of the Primary Examiner dated **03/20/2007** finally rejecting Claim(s) **1-14**

The fee for this Notice of Appeal is: **\$500.00**

- ☐ A check in the amount of the fee is enclosed.
- ☐ The Director has already been authorized to charge fees in this application to a Deposit Account.
- ☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **02-2553**
- ☐ Payment by credit card. Form PTO-2038 is attached.

**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

  
Signature

Dated: July 17, 2007

Brett J. Slaney (Reg. No. 58,772)  
Blake, Cassels & Graydon LLP  
Box 25, Commerce Court West, 199 Bay Street  
Toronto, Ontario, M5L 1A9, Canada

Tel: (416) 863-2518

Fax: (416) 863-2653

CC:


I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to the "Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450" [37 CFR 1.8(a)] on

(Date)

Signature of Person Mailing Correspondence

Typed or Printed Name of Person Mailing Correspondence

P13LARGE/REV09

<b>PETITION FOR EXTENSION OF TIME TO FILE NOTICE OF APPEAL (Large Entity)</b>				Docket No. 67539/00421	
In Re Application Of: <b>VANSTONE, Scott A., et al.</b>					
Application No. <b>10/025,924</b>	Filing Date <b>12/26/2001</b>	Examiner <b>PYZOCHA, Michael J.</b>	Customer No. <b>27871</b>	Group Art Unit <b>2137</b>	Confirmation No. <b>7632</b>
Invention: <b>METHOD OF PUBLIC KEY GENERATION</b>					
<div style="text-align: center;"> <u>COMMISSIONER FOR PATENTS:</u> </div> <p>This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a response to the Office Action of <u>03/20/2007</u> in the above-identified application. <span style="margin-left: 100px;"><i>Date</i></span></p> <p>The requested extension is as follows (check time period desired):</p> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div> <input checked="" type="checkbox"/> One month  from: <u>June 20, 2007</u>  <span style="margin-left: 100px;"><i>Date</i></span> </div> <div> <input type="checkbox"/> Two months  until: <u>July 20, 2007</u>  <span style="margin-left: 100px;"><i>Date</i></span> </div> <div> <input type="checkbox"/> Three months </div> <div> <input type="checkbox"/> Four months </div> <div> <input type="checkbox"/> Five months </div> </div> <p>The fee for the extension of time is <b>\$120</b> and is to be paid as follows:</p> <div style="margin-left: 20px;"> <input type="checkbox"/> A check in the amount of the fee is enclosed.  <input checked="" type="checkbox"/> The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account No. <b>02-2553</b>  <input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached. </div> <p><b>WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.</b></p> <div style="display: flex; justify-content: space-between; align-items: flex-start; margin-top: 20px;"> <div style="width: 45%;">   <hr style="border: 0; border-top: 1px solid black; margin-top: 5px;"/> <p><b>Brett J. Slaney (Reg. No. 58,772)</b>  <b>Blake, Cassels &amp; Graydon LLP</b>  <b>Box 25, Commerce Court West, 199 Bay Street</b>  <b>Toronto, Ontario, M5L 1A9, Canada</b></p> <p><b>Tel: (416) 863-2518</b>  <b>Fax: (416) 863-2653</b></p> <p>CC:</p> </div> <div style="width: 45%; text-align: right;"> Dated: July 17, 2007 </div> </div> <div style="border: 1px solid black; padding: 5px; margin-top: 20px; width: fit-content;"> I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 [37 CFR 1.8(a)] on _____  <div style="text-align: center; margin-top: 10px;"> <i>(Date)</i> </div> <div style="text-align: center; margin-top: 10px;"> <i>Signature of Person Mailing Correspondence</i> </div> <div style="text-align: center; margin-top: 10px;"> <i>Typed or Printed Name of Person Mailing Correspondence</i> </div> </div>					

P14LARGE/REV08

Electronic Patent Application Fee Transmittal				
Application Number:		10025924		
Filing Date:		26-Dec-2001		
Title of Invention:		Method of public key generation		
First Named Inventor/Applicant Name:		Scott A. Vanstone		
Filer:		Brett Joseph Slaney/Judith Martin		
Attorney Docket Number:		00001-0417		
Filed as Large Entity				
Utility      Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Notice of appeal	1401	1	500	500
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 1 month with \$0 paid	1251	1	120	120
<b>Miscellaneous:</b>				
<b>Total in USD (\$)</b>				<b>620</b>

Electronic Acknowledgement Receipt	
<b>EFS ID:</b>	1978480
<b>Application Number:</b>	10025924
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7632
<b>Title of Invention:</b>	Method of public key generation
<b>First Named Inventor/Applicant Name:</b>	Scott A. Vanstone
<b>Customer Number:</b>	27871
<b>Filer:</b>	Brett Joseph Slaney/Judith Martin
<b>Filer Authorized By:</b>	Brett Joseph Slaney
<b>Attorney Docket Number:</b>	00001-0417
<b>Receipt Date:</b>	17-JUL-2007
<b>Filing Date:</b>	26-DEC-2001
<b>Time Stamp:</b>	11:14:25
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 620
RAM confirmation Number	5081
Deposit Account	022553

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1		certicom421_noticeappeal_w_ext.pdf	94204 114c31eb1ae61a0b38736dc25aedf0c00a11ae32	yes	2
	<b>Multipart Description/PDF files in .zip description</b>				
	<b>Document Description</b>		<b>Start</b>	<b>End</b>	
	Notice of Appeal Filed		1	1	
	Extension of Time		2	2	
<b>Warnings:</b>					
<b>Information:</b>					
2	Fee Worksheet (PTO-06)	fee-info.pdf	8289 63474974ad1307f32d0f499219cf81aecf6949c1	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			102493		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



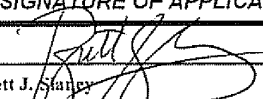
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL</b>  Address to: Mail Stop RCE Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450	Application Number	10/025,924
	Filing Date	Dec. 26, 2001
	First Named Inventor	VANSTONE, Scott A.
	Art Unit	2137
	Examiner Name	PYZOCHA, Michael J.
	Attorney Docket Number	67539/00421

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application. Request for Continued Examination(RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. **Submission required under 37 CFR 1.114** Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).
- a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.
- i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on \_\_\_\_\_
- ii. ☐ Other \_\_\_\_\_
- b. ☒ Enclosed
- i. ☒ Amendment/Reply iii. ☐ Information Disclosure Statement (IDS)
- ii. ☐ Affidavit(s)/Declaration(s) iv. ☐ Other \_\_\_\_\_
2. **Miscellaneous**
- a. ☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of \_\_\_\_\_ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)
- b. ☐ Other \_\_\_\_\_
3. **Fees** The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
- a. ☒ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments to Deposit Account No. 02-2553. I have enclosed a duplicate copy of this sheet.
- i. ☒ RCE fee required under 37 CFR 1.17(e)
- ii. ☒ Extension of time fee (37 CFR 1.136 and 1.17)
- iii. ☐ Other \_\_\_\_\_
- b. ☐ Check in the amount of \$ \_\_\_\_\_ enclosed
- c. ☐ Payment by credit card (Form PTO-2038 enclosed)

**WARNING:** Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED			
Signature		Date	October 30, 2007
Name (Print / Type)	Brett J. Stanley	Registration No.	58,772

CERTIFICATE OF MAILING OR TRANSMISSION			
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.			
Signature			
Name (Print / Type)		Date	

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing the burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

<b>PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)</b> <b>FY 2006</b> <i>(Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).)</i>		Docket Number (Optional) 67539/00421
Application Number 10/025,924		Filed Dec. 26, 2001
For VANSTONE, Scott A. et al		
Art Unit 2137		Examiner PYZOCHA, M

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	<u>Fee</u>	<u>Small Entity Fee</u>	
<input type="checkbox"/> One month (37 CFR 1.17(a)(1))	\$120	\$60	\$ 0
<input checked="" type="checkbox"/> Two months (37 CFR 1.17(a)(2))	\$460	\$230	\$ 460
<input type="checkbox"/> Three months (37 CFR 1.17(a)(3))	\$1050	\$525	\$ 0
<input type="checkbox"/> Four months (37 CFR 1.17(a)(4))	\$1640	\$820	\$ 0
<input type="checkbox"/> Five months (37 CFR 1.17(a)(5))	\$2230	\$1115	\$ 0

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check in the amount of the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 02-2553. I have enclosed a duplicate copy of this sheet.

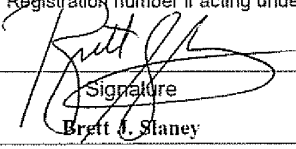
**WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.**

I am the ☐ applicant/inventor

☐ assignee of record of the entire interest. See 37 CFR 3.71.  
Statement under 37 CFR 3.73(b) is enclosed (Form PTO/SB/96).

☒ attorney or agent of record. Registration Number 58,772

☐ attorney or agent under 37 CFR 1.34.  
Registration number if acting under 37 CFR 1.34 \_\_\_\_\_

  
 Signature  
 Brett A. Stanley  
 Typed or printed name

October 30, 2007  
 Date  
 416-863-2518  
 Telephone Number

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☒ Total of \_\_\_\_\_ forms are submitted.

This collection of information is required by 37 CFR 1.136(a). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you are required to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Electronic Patent Application Fee Transmittal				
Application Number:		10025924		
Filing Date:		26-Dec-2001		
Title of Invention:		Method of public key generation		
First Named Inventor/Applicant Name:		Scott A. Vanstone		
Filer:		Brett Joseph Slaney/Judith Martin		
Attorney Docket Number:		00001-0417		
Filed as Large Entity				
Utility      Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	1202	10	50	500
Independent claims in excess of 3	1201	1	210	210
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Extension-of-Time:</b>				
Extension - 2 months with \$0 paid	1252	1	460	460
<b>Miscellaneous:</b>				
Request for continued examination	1801	1	810	810
<b>Total in USD (\$)</b>				<b>1980</b>

<b>Electronic Acknowledgement Receipt</b>	
<b>EFS ID:</b>	2396454
<b>Application Number:</b>	10025924
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7632
<b>Title of Invention:</b>	Method of public key generation
<b>First Named Inventor/Applicant Name:</b>	Scott A. Vanstone
<b>Customer Number:</b>	27871
<b>Filer:</b>	Brett Joseph Slaney/Judith Martin
<b>Filer Authorized By:</b>	Brett Joseph Slaney
<b>Attorney Docket Number:</b>	00001-0417
<b>Receipt Date:</b>	30-OCT-2007
<b>Filing Date:</b>	26-DEC-2001
<b>Time Stamp:</b>	17:25:18
<b>Application Type:</b>	Utility under 35 USC 111(a)

### **Payment information:**

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 1980
RAM confirmation Number	3524
Deposit Account	022553
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

### **File Listing:**

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1		certicom421_OAresponse.pdf	476553	yes	11
		f	32085678b51e05b0e3c73e8e0ede851ea9d9b65c		
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment After Final		1	1	
	Claims		2	6	
	Applicant Arguments/Remarks Made in an Amendment		7	9	
	Request for Continued Examination (RCE)		10	10	
	Extension of Time		11	11	
Warnings:					
Information:					
2	Fee Worksheet (PTO-06)	fee-info.pdf	8548	no	2
			fbec6d41684ff386418b039e6651e6f254156def		
Warnings:					
Information:					
Total Files Size (in bytes):			485101		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Application No. 10/025,924  
Reply to Office Action of: March 20, 2007

**IN THE UNITED STATES PATENT & TRADEMARK OFFICE**

Appl. No.: 10/025,924  
Applicant: VANSTONE, Scott et al.  
Filed: December 26, 2001  
Title: METHOD OF PUBLIC KEY GENERATION  
Art Unit: 2137  
Examiner: PYZOCHA, Michael J.  
Docket No.: 67539/00421

Mail Stop AF  
U.S. Patent & Trademark Office  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**RESPONSE AFTER FINAL REJECTION**

Sir:

This is further to the Office Action dated March 20, 2007. Applicant advises that a request for continued examination and a request for a two-month extension of time are being filed concurrently herewith. Applicant wishes to amend the above-identified application as follows:

**Amendments to the Claims:** are reflected in the listing of claims which begins on page 2 of this paper.

**Remarks:** begin on page 7 of this paper.

**Amendments to the Claims**

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of generating a key  $k$  for use in a cryptographic function performed over a group of order  $q$ , said method including the steps of:
  - generating a seed value  $SV$  from a random number generator;
  - performing a hash function  $H()$  on said seed value  $SV$  to provide an output  $H(SV)$ ;
  - determining whether said output  $H(SV)$  is less than said order  $q$  prior to reducing mod  $q$ ;
  - accepting said output  $H(SV)$  for use as said key  $k$  if the value of said output  $H(SV)$  is less than said order  $q$ ;
  - rejecting said output  $H(SV)$  as said key if said value is not less than said order  $q$ ;
  - if said output  $H(SV)$  is rejected, repeating said method; and
  - if said output  $H(SV)$  is accepted, providing said key  $k$  for use in performing said cryptographic function, wherein said key  $k$  is equal to said output  $H(SV)$ .
2. (original) The method of claim 1 wherein another seed value is generated by said random number generator if said output is rejected.
3. (original) The method of claim 1 wherein the step of accepting said output as a key includes a further step of storing said key.
4. (original) The method of claim 1 wherein said key is used for generation of a public key.
5. (previously presented) The method of claim 1 wherein said order  $q$  is a prime number represented by a bit string of predetermined length  $L$ .
6. (previously presented) The method of claim 5 wherein said output from said hash function is a bit string of predetermined length  $L$ .
7. (original) The method of claim 1 wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to



produce a new output; a determination being made as to whether said new output is acceptable as a key.

8. (original) The method of claim 7, wherein said step of incrementing includes a further step of adding a particular value to said seed value.

9. (currently amended) A method of generating a key  $k$  for use in a cryptographic function performed over a group of order  $q$ , said method including the steps of:

- generating a seed value  $SV$  from a random number generator;
- performing a hash function  $H()$  on said seed number  $SV$  to provide a first output  $H(SV)$ ;
- incrementing said seed value  $SV$  by a predetermined function  $f()$  and performing said hash function  $H()$  on said incremented seed value to provide a second output  $H(f(SV))$ ;
- combining said first output  $H(SV)$  and second output  $H(f(SV))$  to produce a new output;
- determining whether said new output has a value less than said order  $q$  prior to reducing mod  $q$ ;
- accepting said new output for use as said key  $k$  if said new output has a value less than said order  $q$ ;
- rejecting said new output as said key  $k$  if said value is not less than said order  $q$ ;
- if said new output is rejected, repeating said method, and
- if said new output is accepted, providing said key  $k$  for use in performing said cryptographic function, wherein said key  $k$  is equal to said new output.

10. (original) The method of claim 9 wherein upon rejection of said new output a new seed value is generated by said random number generator.

11. (original) The method of claim 9 wherein upon rejection of said new output said seed value is incremented by a predetermined function and revised values for said first output and said second output are obtained.

12. (previously presented) The method of claim 9 wherein a bit string greater than a predetermined length  $L$  is obtained and an  $L$  bit string selected therefrom for comparison with said order  $q$ .

13. (previously presented) The method of claim 12 wherein upon rejection of said bit string of predetermined length  $L$ , a further  $L$  bit string is selected.

14. (previously presented) The method of claim 9 wherein said step of combining said first and second outputs includes a further step of rejecting excess bits such that said new output is a bit string of length  $L$ .

15. (new) A computer readable medium comprising computer executable instructions for generating a key  $k$  for use in a cryptographic function performed over a group of order  $q$ , said instructions including instructions for:

- generating a seed value  $SV$  from a random number generator;
- performing a hash function  $H()$  on said seed value  $SV$  to provide an output  $H(SV)$ ;
- determining whether said output  $H(SV)$  is less than said order  $q$  prior to reducing mod  $q$ ;
- accepting said output  $H(SV)$  for use as said key  $k$  if the value of said output  $H(SV)$  is less than said order  $q$ ;
- rejecting said output  $H(SV)$  as said key if said value is not less than said order  $q$ ;
- if said output  $H(SV)$  is rejected, repeating said method; and
- if said output  $H(SV)$  is accepted, providing said key  $k$  for use in performing said cryptographic function, wherein said key  $k$  is equal to said output  $H(SV)$ .

16. (new) The computer readable medium of claim 15 wherein another seed value is generated by said random number generator if said output is rejected.

17. (new) The computer readable medium of claim 15 wherein the step of accepting said output as a key includes a further step of storing said key.

18. (new) The computer readable medium of claim 15 wherein said key is used for generation of a public key.

19. (new) The computer readable medium of claim 15 wherein said order  $q$  is a prime number represented by a bit string of predetermined length  $L$ .

20. (new) The computer readable medium of claim 19 wherein said output from said hash

function is a bit string of predetermined length  $L$ .

21. (new) The computer readable medium of claim 15 wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

22. (new) The computer readable medium of claim 21, wherein said step of incrementing includes a further step of adding a particular value to said seed value.

23. (new) A cryptographic unit configured for generating a key  $k$  for use in a cryptographic function performed over a group of order  $q$ , said cryptographic unit having access to computer readable instructions for:

- generating a seed value  $SV$  from a random number generator;
- performing a hash function  $H()$  on said seed value  $SV$  to provide an output  $H(SV)$ ;
- determining whether said output  $H(SV)$  is less than said order  $q$  prior to reducing mod  $q$ ;
- accepting said output  $H(SV)$  for use as said key  $k$  if the value of said output  $H(SV)$  is less than said order  $q$ ;
- rejecting said output  $H(SV)$  as said key if said value is not less than said order  $q$ ;
- if said output  $H(SV)$  is rejected, repeating said method; and
- if said output  $H(SV)$  is accepted, providing said key  $k$  for use in performing said cryptographic function, wherein said key  $k$  is equal to said output  $H(SV)$ .

24. (new) The cryptographic unit of claim 23 wherein another seed value is generated by said random number generator if said output is rejected.

25. (new) The cryptographic unit of claim 23 wherein the step of accepting said output as a key includes a further step of storing said key.

26. (new) The cryptographic unit of claim 23 wherein said key is used for generation of a public key.

27. (new) The cryptographic unit of claim 23 wherein said order  $q$  is a prime number

represented by a bit string of predetermined length L.

28. (new) The cryptographic unit of claim 27 wherein said output from said hash function is a bit string of predetermined length L.

29. (new) The cryptographic unit of claim 23 wherein if said output is rejected, said output is incremented by a deterministic function and a hash function is performed on said incremented output to produce a new output; a determination being made as to whether said new output is acceptable as a key.

30. (new) The cryptographic unit of claim 29, wherein said step of incrementing includes a further step of adding a particular value to said seed value.

## **REMARKS**

Applicant wishes to thank the Examiner for reviewing the present application.

### **Personal Interview**

Applicant wishes to also thank the Examiner for taking the time to meet with the undersigned, John R.S. Orange (29,725), and Dr. Scott Vanstone in a personal interview on October 18, 2007. In the personal interview, proposed claim amendments were discussed to clarify the distinctions over the references previously cited against the current claims. It was agreed that the references cited do not recognize the bias that may be introduced by the selection of  $k$ . To clarify this distinction, amendments to claims 1 and 9 were proposed that specify that the step of determining whether or not the output is less than the order  $q$  is done prior to reducing mod  $q$ . The Schneier reference does not teach accepting or rejecting a key by checking that it is less than  $q$  before reducing mod  $q$ . As explained by Dr. Vanstone, and discussed in the background of the present application, the Schneier reference, which refers to DSA and the DSS, requires the reduction of the integer mod  $q$  which can expect that more values will lie in the first interval than the second, hence the bias. It has been recognized by Applicant that by first checking that the output to be used as the key is less than  $q$  and then accepting or rejecting based on this determination can avoid the bias altogether. Again, the proposed amendments are believed to clarify this distinction. It was agreed in the personal interview that neither the Vanstone reference, nor the Schneier paper recognize the bias let alone teach the making such a determination prior to reducing mod  $q$ . As such, it is believed that the amendments outlined above clearly and patentably distinguish over the references cited in the final rejection.

### **Status of Application**

Applicant advises that a Notice of Appeal was filed on July 17, 2007 along with a request for a one-month extension of time. The present response is being filed concurrently with a request for continued examination (RCE) and a request for a two-month extension of time to reopen prosecution. It is believed that the present application should now be taken out of the appeal process and that in view of the present response, the RCE is proper. As such, the above-noted amendments should be entered and prosecution be continued on the basis of such amendments.

### **Claim Amendments**

As discussed above, claims 1 and 9 have been amended to clarify that the step of determining if the output is less than the order  $q$  is done "prior to reducing mod  $q$ ". New claims

15-22 have been added, which are directed to a computer readable medium with instructions for performing the steps which are believed to be allowable in claims 1-14. New claims 23-30 have been added, which are similar to claims 15-22 but are directed to a cryptographic unit.

No new subject matter is believed to have been added by way of these amendments.

#### **Claim Rejections**

Claims 1, 2, 4 and 5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone (US 6,195,433) in view of Schneier (Applied Cryptography). As discussed above, claim 1 has been amended to specify that the step of determining whether or not the output is less than the order  $q$  is done prior to reducing mod  $q$ . The Schneier reference does not teach accepting or rejecting a key by checking that it is less than  $q$  before reducing mod  $q$ . As explained by Dr. Vanstone in the personal interview, and discussed in the background of the present application, the Schneier reference, which refers to DSA and the DSS, requires the reduction of the integer mod  $q$  which can expect that more values will lie in the first interval than the second, hence the bias. It has been recognized by Applicant that by first checking that the output to be used as the key is less than  $q$  and then accepting or rejecting based on this determination can avoid the bias altogether. As such, claim 1, as amended, is believed to clearly and patentably distinguish over the cited references. Claims 2, 4 and 5 being ultimately dependent on claim 1 are also believed to be distinguished.

Claims 7-13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, in view of Schneier, in further view of Matyas, in further view of Backal. It is believed to have been shown above that claims 1 and 9 clearly and patentably distinguish over Vanstone in view of Schneier. As previously argued, neither Matyas nor Backal have recognized the bias discussed above, let alone teach accepting or rejecting an output to be used as a key prior to reducing mod  $q$ . As such, neither Matyas nor Backal teach what is missing from Vanstone and Schneier. Claims 7-13, are therefore also believed to be patentably distinguished over the cited references.

Claims 3, 6 and 14 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, in view of Schneier, in further view of Matyas (alone or in combination with Backal). Claims 3, 6 and 14 being ultimately dependent on either claim 1 or claim 9 are believed to be distinguished for reasons similar to those expressed above.

Claims 1, 2, 4 and 5 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Matyas, in further view of Patel (US 6,327,660). Again, as previously argued, Patel does not teach what is believed to have been shown to be missing from Schneier


Claims 7-13 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier view of Matyas, in further view of Patel, in further view of Backal. Similar arguments equally apply to this rejection as this is simply another combination of references that fails to teach the bias recognized by Applicant and the features recited in claims 1 and 9.

Claims 3, 6 and 14 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier view of Matyas, in further view of Patel (alone or in combination with Backal). Similar arguments equally apply to this rejection as this is simply another combination of references that fails to teach the bias recognized by Applicant and the features recited in claims 1 and 9.

**Summary**

In view of the foregoing, it is believed that claims 1, 9, as amended, and those claims dependent thereon, are clearly and patentably distinguished over the references cited by the Examiner and thus are in condition for allowance. New claims 15-30 are also believed to be patentably distinguished for similar reasons.

Applicant requests early reconsideration and allowance of the present application.  
Respectfully submitted,

  
\_\_\_\_\_  
Brett J. Slaney  
Agent for Applicant  
Registration No. 58,772

Date: October 30, 2007

BLAKE, CASSELS & GRAYDON LLP  
Suite 2800, P.O. Box 25  
199 Bay Street, Commerce Court West  
Toronto, Ontario M5L 1A9  
CANADA

Tel: 416-863-2518  
BS/

<b>PATENT APPLICATION FEE DETERMINATION RECORD</b> Substitute for Form PTO-875					Application or Docket Number <b>10/025,924</b>		Filing Date <b>12/26/2001</b>		<input type="checkbox"/> To be Mailed	
---	--	--	--	--	---	--	----------------------------------	--	---------------------------------------	--

APPLICATION AS FILED – PART I						OTHER THAN SMALL ENTITY			
(Column 1)		(Column 2)		SMALL ENTITY <input type="checkbox"/>		OR		SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)	
<input checked="" type="checkbox"/> BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A		N/A	<b>740</b>			
<input type="checkbox"/> SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A		N/A				
<input type="checkbox"/> EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A		N/A				
TOTAL CLAIMS (37 CFR 1.16(l))	minus 20 =	*	X \$ =		OR	X \$ =			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X \$ =		OR	X \$ =			
<input type="checkbox"/> APPLICATION SIZE FEE (37 CFR 1.16(s))			If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))									
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL <b>740</b>			

APPLICATION AS AMENDED – PART II						OTHER THAN SMALL ENTITY					
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR		SMALL ENTITY	
AMENDMENT	10/30/2007	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(o))	* 30	Minus	** 20	= 10	X \$ =		OR	X \$50=	500	
	Independent (37 CFR 1.16(h))	* 4	Minus	***3	= 1	X \$ =		OR	X \$210=	210	
<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))											
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	<b>710</b>	

(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OR		SMALL ENTITY	
AMENDMENT	10/30/2007	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(o))	*	Minus	**	=	X \$ =		OR	X \$ =		
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X \$ =		OR	X \$ =		
<input type="checkbox"/> Application Size Fee (37 CFR 1.16(s))											
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))											
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE		

\* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

\*\*\* If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

**Legal Instrument Examiner:**  
**/TAMMY MCBETH BROWN/**

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*



## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S60	6	key near generat\$4 same (reduc\$4 less\$6 small\$3) near mod	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 08:53
S61	121	key near generat\$4 and (reduc\$4 less\$6 small\$3) near mod	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 08:53
S62	13	S61 and @ad<"20001227"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 08:53
S63	0	(seed with hash\$4 with reduc\$4 near mod).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:11
S64	0	(seed same hash\$4 same reduc\$4 near mod).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:11
S65	7	(seed same hash\$4 same order).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:12
S66	18	(key same less near3 order).clm.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:12
S67	953	380/44.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/09 09:18
S68	12	S67 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18

## EAST Search History

S69	1343	380/277.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/09 09:18
S70	20	S69 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18
S71	711	708/250.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/09 09:18
S72	1	S71 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18
S73	11	key with generat\$4 same repeat\$4 with reject\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18
S74	0	S73 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18
S75	51	key with generat\$4 and repeat\$4 same reject\$4 with (key output)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18
S76	0	S75 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18
S77	4536	hash\$4 with key with generat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18
S78	142	S77 same repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18

1/9/08 2:01:37 PM

C:\Documents and Settings\mpyzocha1\My Documents\EAST\Workspaces\10025924-2.wsp

Page 2

## EAST Search History

S79	2	S78 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18
S80	11	key with generat\$4 same repeat\$4 with weak	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18
S81	0	S80 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:18
S82	21	weak with key with repeat\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/09 09:18
S83	0	S82 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:19
S84	67	(PRNG ("psuedo random number generator")). and weak	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/09 09:19
S85	0	S84 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:19
S86	117	generat\$4 with key same less with order	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:19
S87	0	S86 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:19
S88	13	generat\$4 with key and less near3 order same hash\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:19

## EAST Search History

S89	0	S88 and @ad<"20001227" and @pd>"20070315"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2008/01/09 09:19
S90	1034	(VANSTONE near SCOTT) (VADEKAR near ASHOK) (LAMBERT near ROBERT) (GALLANT near ROBERT) (BROWN near DANIEL) (MENEZES near ALFRED)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/09 09:19
S91	46	S90 and hash\$4 same order	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/09 09:20
S92	19	S90 and hash\$4 and reduc\$4 with mod	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2008/01/09 09:20



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

## NOTICE OF ALLOWANCE AND FEE(S) DUE

27871 7590 01/22/2008

BLAKE, CASSELS & GRAYDON LLP  
BOX 25, COMMERCE COURT WEST  
199 BAY STREET, SUITE 2800  
TORONTO, ON M5L 1A9  
CANADA

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT

PAPER NUMBER

2137

DATE MAILED: 01/22/2008

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632

TITLE OF INVENTION: METHOD OF PUBLIC KEY GENERATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1440	\$300	\$0	\$1740	04/22/2008

**THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.**

**THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.**

### HOW TO REPLY TO THIS NOTICE:

#### I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

**IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.**

# **PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to:** Mail **Mail Stop ISSUE FEE**  
**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, Virginia 22313-1450**  
**or Fax** **(571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27871 7590 01/22/2008

**BLAKE, CASSELS & GRAYDON LLP**  
**BOX 25, COMMERCE COURT WEST**  
**199 BAY STREET, SUITE 2800**  
**TORONTO, ON M5L 1A9**  
**CANADA**

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

## **Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632

TITLE OF INVENTION: METHOD OF PUBLIC KEY GENERATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1440	\$300	\$0	\$1740	04/22/2008

EXAMINER	ART UNIT	CLASS-SUBCLASS
PYZOCHA, MICHAEL J	2137	380-044000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).  
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.  
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list  
 (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 \_\_\_\_\_  
 (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 \_\_\_\_\_  
 3 \_\_\_\_\_

## 3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY AND STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

## 4a. The following fee(s) are submitted:

- ☐ Issue Fee  
☐ Publication Fee (No small entity discount permitted)  
☐ Advance Order - # of Copies \_\_\_\_\_

## 4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.  
☐ Payment by credit card. Form PTO-2038 is attached.  
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number \_\_\_\_\_ (enclose an extra copy of this form).

## 5. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature \_\_\_\_\_

Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_

Registration No. \_\_\_\_\_

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632
27871	7590	01/22/2008		
BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA				
			EXAMINER PYZOCHA, MICHAEL J	
			ART UNIT 2137	PAPER NUMBER
			DATE MAILED: 01/22/2008	

**Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)**  
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 563 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 563 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

2

<b>Notice of Allowability</b>	Application No.	Applicant(s)	
	10/025,924	VANSTONE ET AL.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to amendment filed 10/30/2007.
2. ☒ The allowed claim(s) is/are 1-30.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☒ All    b) ☐ Some\*    c) ☐ None    of the:
  1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
    - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
  - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- |  |   |
|--|---|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892)   | 5. <input type="checkbox"/> Notice of Informal Patent Application                     |
| 2. <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948)                        | 6. <input type="checkbox"/> Interview Summary (PTO-413),<br>Paper No./Mail Date _____ |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),<br>Paper No./Mail Date _____    | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment                   |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit<br>of Biological Material | 8. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance  |
|  | 9. <input type="checkbox"/> Other _____   |

  
**EMMANUEL L. BOISE**  
**SUPERVISORY PATENT EXAMINER**



Application/Control  
Number: 10/025,924  
Art Unit: 2137

Page 2

**EXAMINER'S AMENDMENT**

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Brett J. Slaney (Reg. No. 58,772) on 01/09/2008.

The application has been amended as follows:

23. A cryptographic unit configured for generating a key  $k$  for use in a cryptographic function performed over a group of order  $q$ , said cryptographic unit having access to computer readable instructions ~~for~~ and comprises:

an arithmetic processor for:

generating a seed value  $SV$  from a random number generator;

performing a hash function  $H()$  on said seed value  $SV$  to provide an output  $H(SV)$ ;

determining whether said output  $H(SV)$  is less than said order  $q$  prior to reducing mod  $q$ ;

accepting said output  $H(SV)$  for use as said key  $k$  if the value of said output  $H(SV)$  is less than said order  $q$ ;

rejecting said output  $H(SV)$  as said key if said value is not less than said order  $q$ ;

if said output  $H(SV)$  is rejected, repeating said method; and

if said output  $H(SV)$  is accepted, providing said key  $k$  for use in performing said cryptographic function, wherein said key  $k$  is equal to said output  $H(SV)$ .

***Allowable Subject Matter***

2. The following is an examiner's statement of reasons for allowance: Applicant's arguments put forth in the response filed 10/30/2007 are persuasive. Specifically the prior art generally teaches the steps of generating a key using a seed and hash function. However, the prior art fails to teach determining whether the output of the hash value is less than an order  $q$  prior to reducing mod  $q$ .

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the

Application/Control  
Number: 10/025,924  
Art Unit: 2137

Page 5

organization where this application or proceeding is  
assigned is 571-273-8300.

Information regarding the status of an application may  
be obtained from the Patent Application Information  
Retrieval (PAIR) system. Status information for published  
applications may be obtained from either Private PAIR or  
Public PAIR. Status information for unpublished  
applications is available through Private PAIR only. For  
more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to  
the Private PAIR system, contact the Electronic Business  
Center (EBC) at 866-217-9197 (toll-free). If you would like  
assistance from a USPTO Customer Service Representative or  
access to the automated information system, call 800-786-  
9199 (IN USA OR CANADA) or 571-272-1000.

MJP

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER



## UNITED STATES PATENT AND TRADEMARK OFFICE


UNITED STATES DEPARTMENT OF COMMERCE  
 United States Patent and Trademark Office  
 Address: COMMISSIONER FOR PATENTS  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 www.uspto.gov

## BIB DATA SHEET

CONFIRMATION NO. 7632

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
10/025,924	12/26/2001	380	2137	00001-0417		
<b>RULE</b>						
<b>APPLICANTS</b> Scott A. Vanstone, Campbellville, CANADA; Ashok Vadekar, Rockwood, CA; Robert J. Lambert, Cambridge, CANADA; Robert P. Gallant, Mississauga, CANADA; Daniel R. Brown, Toronto, CANADA; Alfred Menezes, West Canada, CANADA; <i>OK mjd 1/9/02</i>						
<b>** CONTINUING DATA *****</b> <i>NONE mjd 1/9/02</i>						
<b>** FOREIGN APPLICATIONS *****</b> CANADA 2,329,590 12/27/2000 <i>OK mjd 1/9/02</i>						
<b>** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **</b> 02/25/2002						
Foreign Priority claimed <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No 35 USC 119(a-d) conditions met <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No Verified and Acknowledged <i>[Signature]</i> Examiner's Signature		<input type="checkbox"/> Met after Allowance Initials	<b>STATE OR COUNTRY</b> CANADA	<b>SHEETS DRAWINGS</b> 7	<b>TOTAL CLAIMS</b> 14	<b>INDEPENDENT CLAIMS</b> 2
<b>ADDRESS</b> BLAKE, CASSELS & GRAYDON LLP BOX 25, COMMERCE COURT WEST 199 BAY STREET, SUITE 2800 TORONTO, ON M5L 1A9 CANADA						
<b>TITLE</b> Method of public key generation						
<b>FILING FEE RECEIVED</b> 1580	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees (Filing) <input type="checkbox"/> 1.17 Fees (Processing Ext. of time) <input type="checkbox"/> 1.18 Fees (Issue) <input type="checkbox"/> Other _____ <input type="checkbox"/> Credit		



<b>Index of Claims</b> 	<b>Application/Control No.</b> 10025924	<b>Applicant(s)/Patent Under Reexamination</b> VANSTONE ET AL.
	<b>Examiner</b> Pyzocha, Michael	<b>Art Unit</b> 2137


✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

<input checked="" type="checkbox"/> Claims renumbered in the same order as presented by applicant					<input type="checkbox"/> CPA	<input type="checkbox"/> T.D.	<input type="checkbox"/> R.1.47		
CLAIM		DATE							
Final	Original	03/15/2007	03/15/2007	01/09/2008					
	1	✓	✓	=					
	2	✓	✓	=					
	3	✓	✓	=					
	4	✓	✓	=					
	5	✓	✓	=					
	6	✓	✓	=					
	7	✓	✓	=					
	8	✓	✓	=					
	9	✓	✓	=					
	10	✓	✓	=					
	11	✓	✓	=					
	12	✓	✓	=					
	13	✓	✓	=					
	14	✓	✓	=					
	15			=					
	16			=					
	17			=					
	18			=					
	19			=					
	20			=					
	21			=					
	22			=					
	23			=					
	24			=					
	25			=					
	26			=					
	27			=					
	28			=					
	29			=					
	30			=					

<b>Search Notes</b>  	<b>Application/Control No.</b>  10025924	<b>Applicant(s)/Patent Under Reexamination</b>  VANSTONE ET AL.
	<b>Examiner</b>  Pyzocha, Michael	<b>Art Unit</b>  2137

SEARCHED			
Class	Subclass	Date	Examiner
380	44	10/10/06	MJP
380	277	10/10/06	MJP
708	250	10/10/06	MJP
updated	search	3/15/07	MJP
updated	search	1/9/08	MJP

SEARCH NOTES		
Search Notes	Date	Examiner
BRS search USPAT, USPGPUB, EPO, JPO, IBM, DERWENT see attached search history	10/10/06	MJP
all claims have been reviewed for 35 USC non-statutory subject matter	10/10/06	MJP
new and updated BRS search, see attached search history	3/15/07	MJP
new and updated BRS search, see attached search history	1/9/08	MJP

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner
380	44	1/9/08	MJP
380	277	1/9/08	MJP
708	250	1/9/08	MJP



## PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE  
**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, Virginia 22313-1450**  
**or Fax** (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

27871 7590 01/22/2008

BLAKE, CASSELS & GRAYDON LLP  
 BOX 25, COMMERCE COURT WEST  
 199 BAY STREET, SUITE 2800  
 TORONTO, ON M5L 1A9  
 CANADA

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

## Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417	7632

TITLE OF INVENTION: METHOD OF PUBLIC KEY GENERATION

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	\$1440	\$300	\$0	\$1740	04/22/2008
EXAMINER		ART UNIT	CLASS-SUBCLASS			
PYZOSHA, MICHAEL J		2137	380-044000			

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

- ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list

- (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
- (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1. Blake, Cassels & Graydon LLP  
 2. John R.S. Orange  
 3. Brett J. Slaney

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

CERTICOM CORP.

(B) RESIDENCE: (CITY AND STATE OR COUNTRY)

MISSISSAUGA, CANADA

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☒ Corporation or other private group entity ☐ Government

a. The following fee(s) are submitted:

- ☒ Issue Fee
- ☒ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 02-2553 (enclose an extra copy of this form).

4. Change in Entity Status (from status indicated above)

- ☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature

Typed or printed name

Brett J. Slaney

Date

Registration No.

April 11, 2008  
 58,772

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal				
Application Number:		10025924		
Filing Date:		26-Dec-2001		
Title of Invention:		METHOD OF PUBLIC KEY GENERATION		
First Named Inventor/Applicant Name:		Scott A. Vanstone		
Filer:		Brett Joseph Slaney/Judith Martin		
Attorney Docket Number:		00001-0417		
Filed as Large Entity				
Utility      Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	1501	1	1440	1440
Publ. Fee- early, voluntary, or normal	1504	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				1740

Electronic Acknowledgement Receipt	
<b>EFS ID:</b>	3139427
<b>Application Number:</b>	10025924
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7632
<b>Title of Invention:</b>	METHOD OF PUBLIC KEY GENERATION
<b>First Named Inventor/Applicant Name:</b>	Scott A. Vanstone
<b>Customer Number:</b>	27871
<b>Filer:</b>	Brett Joseph Slaney/Judith Martin
<b>Filer Authorized By:</b>	Brett Joseph Slaney
<b>Attorney Docket Number:</b>	00001-0417
<b>Receipt Date:</b>	11-APR-2008
<b>Filing Date:</b>	26-DEC-2001
<b>Time Stamp:</b>	12:54:13
<b>Application Type:</b>	Utility under 35 USC 111(a)

### Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$ 1740
RAM confirmation Number	7016
Deposit Account	022553
Authorized User	

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	----------------------------------	------------------	------------------

1	Issue Fee Payment (PTO-85B)	certicom421_issue_pub_fee s.pdf	94600  4e06e4abc8c1c53b5660d53ec0136877 3c1380d8	no	1
<b>Warnings:</b>					
<b>Information:</b>					
2	Fee Worksheet (PTO-06)	fee-info.pdf	8281  9b90538959619f34efff400c6ea101e91f 87cad7	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			102881		
<p><b>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</b></p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,924	05/13/2008	7372961	00001-0417	7632

27871 7590 04/23/2008  
BLAKE, CASSELS & GRAYDON LLP  
BOX 25, COMMERCE COURT WEST  
199 BAY STREET, SUITE 2800  
TORONTO, ON M5L 1A9  
CANADA

## ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

### **Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)** (application filed on or after May 29, 2000)

The Patent Term Adjustment is 563 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Scott A. Vanstone, Campbellville, CANADA;  
Ashok Vadekar, Rockwood, CA;  
Robert J. Lambert, Cambridge, CANADA;  
Robert P. Gallant, Mississauga, CANADA;  
Daniel R. Brown, Toronto, CANADA;  
Alfred Menezes, West Canada, CANADA;

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

Appl. No.: 10/025,924 Patent No.: 7,372,931  
Applicant: VANSTONE, Scott A. et al. Assignee: Certicom Corp.  
Filed: December 26, 2001 Issued: May 13, 2008  
Title: METHOD OF PUBLIC KEY GENERATION  
Docket No.: 67539/00421

U.S. Patent & Trademark Office  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Attention: Certificate of Correction Branch

REQUEST FOR CERTIFICATE OF CORRECTION

Sir:

Pursuant to 35 U.S.C. § 255 and 37 C.F.R. § 1.323, Applicant requests that a Certificate of Correction be issued in respect of the above-identified patent.

The Patentee corrects a number of mistakes as listed on the Certificate of Correction, which are explained in further detail below.

Applicant submits that the errors are of a clerical or typographical nature. The changes to correct the errors do not constitute new subject matter and do not require reexamination.

Correction of the Drawings

In the drawings, Sheet 7, Fig. 7, reverse the arrow between box "k'" and box "Combine k + k'", delete the box identified as "Combine" and replace with a box identified as "Comb". This correction is supported by page 7, lines 26-30 of the application as originally filed.

Correction of the Description

In column 1, line 35, delete "public key is known" and replace with "public key are known".

In column 2, line 21, delete " $r=x_{kp}$ " and replace with " $r=x_{kp}$ ".

In column 2, line 50, delete "else".

In column 2, line 51, add "else" at the beginning of the line to read "else  $k \leftarrow \text{SHA-1}(\text{seed})$ ."

In column 3, line 61, delete "is generated" and replace with "are generated".

In column 3, line 61, delete "it is stored" and replace with "k is stored".

In column 4, line 44, delete "cocatenation" and replace with "concatenation".

In column 4, line 44, delete "/" and replace with "l".

In column 4, line 45, delete boldfaced "157" and replace with normal font "157".

In column 5, line 2 and 3, delete "combining" and replace with "combing". This correction is supported by page 7, line 27 of the application as originally filed.

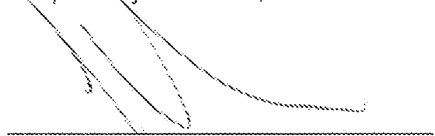
In column 5, line 14, delete "a" and replace with "a<sup>k</sup>". This correction is supported by page 8, line 3 of the application as originally filed.

#### Summary

Enclosed is a duly prepared Certificate of Correction, which the Patentee requests to be issued. Applicant requests that the Office charge the requisite \$100 fee to Deposit Account No. 02-2553. Please charge any additional fees that may be required to Deposit Account No. 02-2553.

The cooperation of the Office in this regard is appreciated.

Respectfully submitted,



John R.S. Orange  
Agent for Applicant  
Registration No. 29,725

Date: 3 June 11,

BLAKE, CASSELS & GRAYDON LLP  
199 Bay Street  
Suite 4000, Commerce Court West  
Toronto ON M5L 1A9  
Canada

Tel: 416-863-3164  
JO/avp



UNITED STATES PATENT AND TRADEMARK OFFICE  
CERTIFICATE OF CORRECTION

Page 1 of 1

PATENT NO. : 7,372,961  
APPLICATION NO : 10/025,924  
ISSUE DATE : May 13, 2008  
INVENTOR(S) : VANSTONE, Scott A. et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the drawings, Sheet 7, Fig. 7, reverse the arrow between box "k'" and box "Combine k + k' ". delete the box identified as "Combine" and replace with a box identified as "Comb".

In column 1, line 35, delete "public key is known" and replace with "public key are known".

In column 2, line 21, delete " $r=x_p$ " and replace with " $r=x_p$ ".

In column 2, line 50, delete "else".

In column 2, line 51, add "else" at the beginning of the line to read "else  $k \leftarrow \text{SHA-1}(\text{seed})$ ."

In column 3, line 61, delete "is generated" and replace with "are generated".

In column 3, line 61, delete "it is stored" and replace with "k is stored".

In column 4, line 44, delete "cocatenation" and replace with "concatenation".

In column 4, line 44, delete "/" and replace with "1".

In column 4, line 45, delete boldfaced "157" and replace with normal font "157".

In column 5, line 2 and 3, delete "combining" and replace with "combing".

In column 5, line 14, delete " $\alpha$ " and replace with " $\alpha^k$ ".

MAILING ADDRESS OF SENDER (Please do not use customer number below):

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

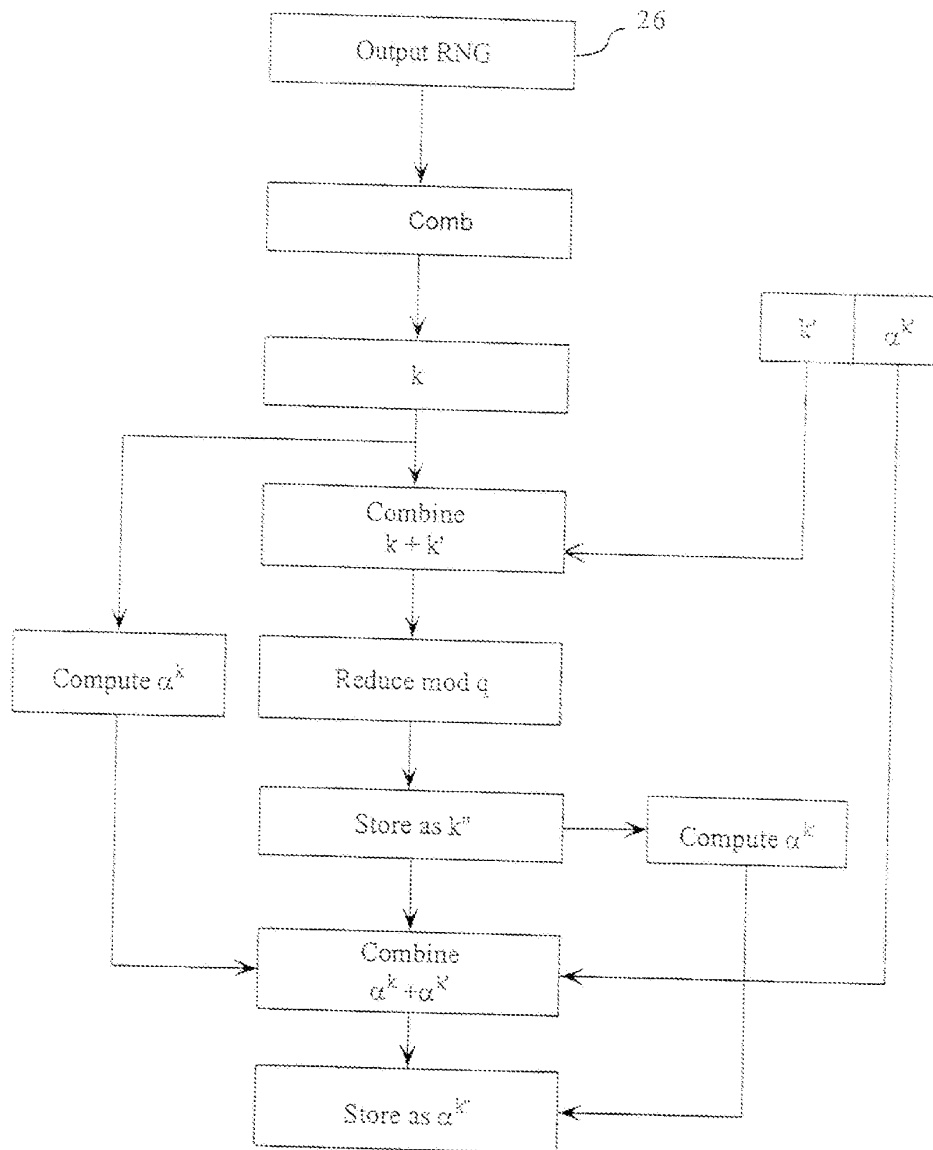


Fig. 7

Electronic Patent Application Fee Transmittal				
Application Number:		10025924		
Filing Date:		26-Dec-2001		
Title of Invention:		METHOD OF PUBLIC KEY GENERATION		
First Named Inventor/Applicant Name:		Scott A. Vanstone		
Filer:		John Robert Scoley Orange/Judith Martin		
Attorney Docket Number:		00001-0417		
Filed as Large Entity				
Utility under 35 USC 111(a) Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Certificate of correction	1811	1	100	100
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				100

<b>Electronic Acknowledgement Receipt</b>	
<b>EFS ID:</b>	10230542
<b>Application Number:</b>	10025924
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	7632
<b>Title of Invention:</b>	METHOD OF PUBLIC KEY GENERATION
<b>First Named Inventor/Applicant Name:</b>	Scott A. Vanstone
<b>Customer Number:</b>	27871
<b>Filer:</b>	John Robert Scoley Orange/Judith Martin
<b>Filer Authorized By:</b>	John Robert Scoley Orange
<b>Attorney Docket Number:</b>	00001-0417
<b>Receipt Date:</b>	03-JUN-2011
<b>Filing Date:</b>	26-DEC-2001
<b>Time Stamp:</b>	16:24:28
<b>Application Type:</b>	Utility under 35 USC 111(a)

**Payment information:**

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$100
RAM confirmation Number	3334
Deposit Account	022553
Authorized User	

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	-------------------------------------	------------------	------------------

1	Request for Certificate of Correction	35371-US-PAT_Request_Cert_Correction.pdf	1626044 3b41eab6fb89daba319edefb4bdf1dfd59c163c	no	4
<b>Warnings:</b>					
<b>Information:</b>					
2	Fee Worksheet (SB06)	fee-info.pdf	30245 c1008406fc048402f9a0602cf72a4f8c8b2b63b2	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			1656289		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

**SPE RESPONSE FOR CERTIFICATE OF CORRECTION**

**DATE** : 6/10/11

**TO SPE OF** : ART UNIT 2455

**SUBJECT** : Request for Certificate of Correction for Appl. No.: 10025924 Patent No.: 7372961

CofC mailroom date: 6/03/11

Please respond to this request for a certificate of correction within 7 days.

**FOR IFW FILES:**

Please review the requested changes/corrections as shown in the **COCIN** document(s) in the IFW application image. No new matter should be introduced, nor should the scope or meaning of the claims be changed.

Please complete the response (see below) and forward the completed response to scanning using document code **COCX**.

**FOR PAPER FILES:**

Please review the requested changes/corrections as shown in the attached certificate of correction. Please complete this form (see below) and forward it with the file to:

**Certificates of Correction Branch (CofC)  
Randolph Square – 9D10-A  
Palm Location 7580**

**For use by the Director's SPE response to 571-270-9990**

**Note:**

**Drawing**

*Lamonte Newsome*

**Certificates of Correction Branch**

**571-272-3421**

**Thank You For Your Assistance**

**The request for issuing the above-identified correction(s) is hereby:**

Note your decision on the appropriate box.

☐ **Approved**

**All changes apply.**

☐ **Approved in Part**

**Specify below which changes **do not** apply.**

☐ **Denied**

**State the reasons for denial below.**

**SPE RESPONSE FOR CERTIFICATE OF CORRECTION**

**Comments:** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_

**SPE**

**Art Unit**



**SPE RESPONSE FOR CERTIFICATE OF CORRECTION**

**DATE** : 6/10/11

**TO SPE OF** : ART UNIT 2455

**SUBJECT** : Request for Certificate of Correction for Appl. No.: 10025924 Patent No.: 7372961

**CofC mailroom date:** 6/03/11

Please respond to this request for a certificate of correction within 7 days.

**FOR IFW FILES:**

Please review the requested changes/corrections as shown in the **COCIN** document(s) in the IFW application image. No new matter should be introduced, nor should the scope or meaning of the claims be changed.

Please complete the response (see below) and forward the completed response to scanning using document code **COCX**.

**FOR PAPER FILES:**

Please review the requested changes/corrections as shown in the attached certificate of correction. Please complete this form (see below) and forward it with the file to:

**Certificates of Correction Branch (CofC)**  
**Randolph Square – 9D10-A**  
**Palm Location 7580**

**Note:**

Drawing

*Lamonte Newsome*

**Certificates of Correction Branch**

**571-272-3421**

**Thank You For Your Assistance**

**The request for issuing the above-identified correction(s) is hereby:**

Note your decision on the appropriate box.

☐ **Approved**

**All changes apply.**

☐ **Approved in Part**

**Specify below which changes **do not** apply.**

☐ **Denied**

**State the reasons for denial below.**

**SPE RESPONSE FOR CERTIFICATE OF CORRECTION**

**Comments:** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_

**SPE**

**Art Unit**

# UNITED STATES PATENT AND TRADEMARK OFFICE

## CERTIFICATE OF CORRECTION

Page 1 of 1

PATENT NO. : 7,372,961 **B2**  
 APPLICATION NO. : 10/025,924  
 ISSUE DATE : May 13, 2008  
 INVENTOR(S) : VANSTONE, Scott A. et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the drawings, Sheet 7, Fig. 7, reverse the arrow between box "k'" and box "Combine k + k'", delete the box identified as "Combine" and replace with a box identified as "Comb".

In column 1, line 35, delete "public key is known" and replace with "public key are known".

In column 2, line 21, delete " $r=x_{kp}$ " and replace with " $r=x_{kp}$ ".

In column 2, line 50, delete "else".

In column 2, line 51, add "else" at the beginning of the line to read "else  $k \leftarrow \text{SHA-1}(\text{seed})$ ."

In column 3, line 61, delete "is generated" and replace with "are generated".

In column 3, line 61, delete "it is stored" and replace with "k is stored".

In column 4, line 44, delete "cocatenation" and replace with "concatenation".

In column 4, line 44, delete "/" and replace with "|".

In column 4, line 45, delete boldfaced "157" and replace with normal font "157".

In column 5, line 2 and 3, delete "combining" and replace with "combing".

In column 5, line 14, delete " $\alpha$ " and replace with " $\alpha^k$ ".

MAILING ADDRESS OF SENDER (Please do not use customer number below):

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 7,372,961 B2  
APPLICATION NO. : 10/025924  
DATED : May 13, 2008  
INVENTOR(S) : Scott A. Vanstone et al.

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the drawings, Sheet 7, Fig. 7, reverse the arrow between box “k” and box “Combine k + k”, delete the box identified as “Combine” and replace with a box identified as “Comb”.

In column 1, line 35, delete “public key is known” and replace with “public key are known”.

In column 2, line 21, delete “ $r=x_{kp}$ ” and replace with “ $r=x_{kp}$ ”.

In column 2, line 50, delete “else”.

In column 2, line 51, add “else” at the beginning of the line to read “else  $k \leftarrow \text{SHA-1}(\text{seed})$ .”

In column 3, line 61, delete “is generated” and replace with “are generated”.

In column 3, line 61, delete “it is stored” and replace with “k is stored”.

In column 4, line 44, delete “cocatenation” and replace with “concatenation”.

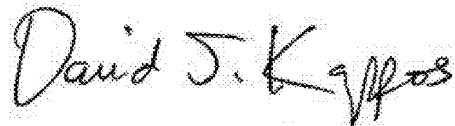
In column 4, line 44, delete “//” and replace with “11”.

In column 4, line 45, delete “157” and replace with “157”.

In column 5, line 2 and 3, delete “combining” and replace with “combing”.

In column 5, line 14, delete “ $\alpha$ ” and replace with “ $\alpha^k$ ”.

Signed and Sealed this  
Twelfth Day of July, 2011



David J. Kappos  
*Director of the United States Patent and Trademark Office*

**SPE RESPONSE FOR CERTIFICATE OF CORRECTION**

**DATE** : 6/10/11

**TO SPE OF** : ART UNIT 2455

**SUBJECT** : Request for Certificate of Correction for Appl. No.: 10025924 Patent No.: 7372961

CofC mailroom date: 6/03/11

Please respond to this request for a certificate of correction within 7 days.

**FOR IFW FILES:**

Please review the requested changes/corrections as shown in the **COCIN** document(s) in the IFW application image. No new matter should be introduced, nor should the scope or meaning of the claims be changed.

Please complete the response (see below) and forward the completed response to scanning using document code **COCX**.

**FOR PAPER FILES:**

Please review the requested changes/corrections as shown in the attached certificate of correction. Please complete this form (see below) and forward it with the file to:

**Certificates of Correction Branch (CofC)**  
**Randolph Square – 9D10-A**  
**Palm Location 7580**

**Note:**

**Drawing**

*Lamonte Newsome*

**Certificates of Correction Branch**

**571-272-3421**

**Thank You For Your Assistance**

**The request for issuing the above-identified correction(s) is hereby:**

Note your decision on the appropriate box.

☒ **Approved**

**All changes apply.**

☐ **Approved in Part**

**Specify below which changes **do not** apply.**

☐ **Denied**

**State the reasons for denial below.**

**SPE RESPONSE FOR CERTIFICATE OF CORRECTION**

**Comments:** \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Eleni Shiferaw \_\_\_\_\_ **2437** \_\_\_\_\_

**SPE**

**Art Unit**

<b>PATENT - POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS</b>	Patent Number	7,372,961
	Issue Date	05-13-2008
	First Named Inventor	Scott A. Vanstone
	Title	METHOD OF PUBLIC KEY GENERATION
	Attorney Docket No.	00001-0417

I hereby revoke all previous powers of attorney given in the above-identified patent.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the Customer Number identified in the box at right as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

54120

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) with respect to the patent identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified patent to:

☒ The address associated with the above-identified Customer Number.

OR

☐ The address associated with the Customer Number identified in the box at right:

OR

☐ Firm or

Individual Name

Address

City

State

Zip

Country

Telephone

Email

I am the:

☐ Applicant.

OR

☒ Patent owner.

Statement under 37 CFR 3.73(c) (Form PTO/AIA/96) submitted herewith or filed on \_\_\_\_\_

Signature		Date	
Name		Telephone	
Title and Company			

NOTE: Signatures of all the applicants or patent owners of the entire interest or their representative(s) are required. If more than one signature is required, submit multiple forms, check the box below, and identify the total number of forms submitted in the blank below.

☐ A total of \_\_\_\_\_ forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32, and 1.33. The information is required to obtain or retain a benefit by the public, which is to update (and by the USPTO to process) the file of a patent or reexamination proceeding. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Legal OK

MOBILEIRON, INC. - EXHIBIT 1003

**STATEMENT UNDER 37 CFR 3.73(c)**

Applicant/Patent Owner: BlackBerry Limited

Application No./Patent No.: 7,372,961

Filed/Issue Date: 05-13-2008

Titled: METHOD OF PUBLIC KEY GENERATION

BlackBerry Limited, a corporation

(Name of Assignee)

(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☒ The assignee of the entire right, title, and interest.
2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):
- ☐ The extent (by percentage) of its ownership interest is \_\_\_\_%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.
- ☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

- A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.
- B. ☒ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Inventors To: Certicom Corp.

The document was recorded in the United States Patent and Trademark Office at  
Reel 012725, Frame 0042, or for which a copy thereof is attached.

2. From: Certicom Corp. To: BlackBerry Limited

The document was recorded in the United States Patent and Trademark Office at  
Reel 039269, Frame 0856, or for which a copy thereof is attached.

[Page 1 of 2]

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

*If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.*



**STATEMENT UNDER 37 CFR 3.73(c)**

3. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

4. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

5. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

6. From: \_\_\_\_\_ To: \_\_\_\_\_

The document was recorded in the United States Patent and Trademark Office at  
Reel \_\_\_\_\_, Frame \_\_\_\_\_, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/David S. Furbeck/

Signature

David S. Furbeck

Printed or Typed Name

March 8, 2018

Date

72,197

Title or Registration Number

[Page 2 of 2]

## Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt	
EFS ID:	31997921
Application Number:	10025924
International Application Number:	
Confirmation Number:	7632
Title of Invention:	METHOD OF PUBLIC KEY GENERATION
First Named Inventor/Applicant Name:	Scott A. Vanstone
Customer Number:	27871
Filer:	David S. Furbeck/Krista Luft
Filer Authorized By:	David S. Furbeck
Attorney Docket Number:	00001-0417
Receipt Date:	08-MAR-2018
Filing Date:	26-DEC-2001
Time Stamp:	15:16:53
Application Type:	Utility under 35 USC 111(a)

**Payment information:**

Submitted with Payment	no
------------------------	----

**File Listing:**

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	35371-US-PAT_POA_Executed.pdf	89339 64aefa12a0e8392219b72105b54de43c718ec6d2	no	1

**Warnings:**

<b>Information:</b>					
2	Assignee showing of ownership per 37 CFR 3.73	35371-US-PAT_37CFR_executed.pdf	1629802	no	3
			e04982e372f15a465d4a1f6c1c76e6ae3ff7756b		
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			1719141		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><b><u>New Applications Under 35 U.S.C. 111</u></b>  If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><b><u>National Stage of an International Application under 35 U.S.C. 371</u></b>  If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><b><u>New International Application Filed with the USPTO as a Receiving Office</u></b>  If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417

**CONFIRMATION NO. 7632**

**POA ACCEPTANCE LETTER**



54120  
BlackBerry Limited - Direct Practice - (US Team)  
ATTN: PATENT TEAM  
2200 University Avenue E.  
Waterloo, ON N2K 0A7  
CANADA

Date Mailed: 03/12/2018

**NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 03/08/2018.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/tmwilliams/



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
10/025,924	12/26/2001	Scott A. Vanstone	00001-0417

27871  
BLAKE, CASSELS & GRAYDON LLP  
COMMERCE COURT WEST  
199 BAY STREET, SUITE 4000  
TORONTO, ON M5L 1A9  
CANADA

**CONFIRMATION NO. 7632**  
**POWER OF ATTORNEY NOTICE**



Date Mailed: 03/12/2018

**NOTICE REGARDING CHANGE OF POWER OF ATTORNEY**

This is in response to the Power of Attorney filed 03/08/2018.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at (571) 272-4000 or (571) 272-4200 or 1-888-786-0101.

/tmwilliams/