Trials@uspto.gov
571-272-7822

Paper 14
Date: November 5, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FACEBOOK, INC., INSTAGRAM, LLC, and WHATSAPP INC.,
Petitioner,

v.

BLACKBERRY LIMITED,
Patent Owner.

IPR2019-00923
Patent 7,372,961 B2

Before GARTH D. BAER, JACQUELINE T. HARLOW, and AARON W. MOORE *Administrative Patent Judges.*

HARLOW, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

INTRODUCTION

Facebook, Inc., Instagram, LLC, and WhatsApp Inc. (collectively, "Petitioner"), filed a Petition (Paper 2, "Pet."), requesting *inter partes* review of claims 1, 2, 5, 15, 16, 19, 23, 24, and 27 of U.S. Patent No. 7,372,961 B2 (Ex. 1001, "the '961 patent"). Blackberry Limited ("Patent Owner") timely filed a Preliminary Response (Paper 10, "Prelim. Resp."). Pursuant to our authorization, Petitioner additionally filed a Reply (Paper 11), and Patent Owner filed a Sur-Reply (Paper 13).

Under 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless the information presented in the petition "shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Having considered the evidence and arguments of record, for reasons discussed below, we deny the petition and do not institute *inter partes* review.

A. Related Matter

The '961 patent is the subject of a district court proceeding in the Central District of California, captioned *BlackBerry Ltd. v. Facebook, Inc.*, No. 2:18-cv-01844-GW-KS (C.D. Cal.). Pet. 1; Paper 4, 1–2.

B. The '961 Patent

The '961 patent, titled "Method of Public Key Generation" (Ex. 1001, code (54)), describes methods for key generation in public key cryptosystems (*id.* at 1:5–6). The '961 patent explains that public key cryptosystems use private keys and corresponding public keys to ensure data security. *Id.* at 1:10–14. The patent points out that the security of public key cryptosystems "depend[s] on the private key remaining secret" (*id.* at 1:37–38), and explains that such systems employ pairs of private and public

keys, known as long term and short term (or ephemeral) key pairs, to shield the long term private key from disclosure (*id.* at 1:38–42).

According to the '961 patent, the Digital Signature Algorithm ("DSA"), one "of the more popular protocols for signature" (Ex. 1001, 1:52–54), suffers from a vulnerability in that

> the implementation of the DSA may be done in such a way as to inadvertently introduce a bias in to the selection of [ephemeral private key] k. This small bias may be exploited to extract a value of the [long term] 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.

Id. at 2:32–38. With particular regard to DSS, the '961 patent explains that

> 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=SHA-1 (seed) mod q.

Id. at 2:38–46. The '961 patent goes on to observe that the "modular reduction [("mod")] 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." *Id.* at 2:56–61.

The '961 patent proposes an alternative algorithm for the generation of ephemeral private key k designed to avoid the above described vulnerability of the DSA implementation used in DSS. *Id.* at 3:64–4:17.

Figure 2 of the ’961 patent illustrates this algorithm and is reproduced below.

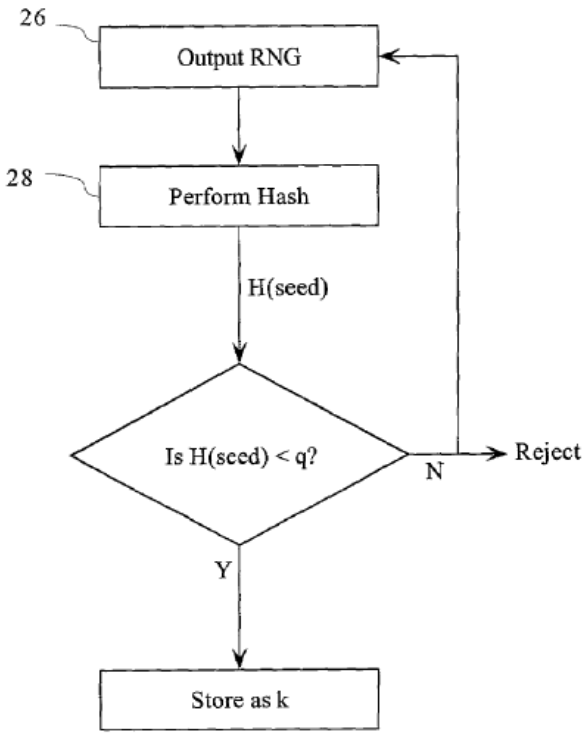

Figure 2 is a flow chart depicting the method for generation of ephemeral private key k disclosed by the ’961 patent. *Id.* at 3:12–13. As shown in Figure 2, the method begins by obtaining a seed value from a random number generator, and then performs a hash function on that seed value to produce an output H(seed). *Id.* at 3:64–4:10. To eliminate the potential bias in the selection of k observed in DSS, the ’961 patent discloses that

> [t]he resultant output H(seed) is tested against the value of q and a decision made based on the relative values. If H(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.

Id. at 4:11–17.

C. Challenged Claims

Petitioner challenges claims 1, 2, 5, 15, 16, 19, 23, 24, and 27 of the '961 patent. Pet. 3–4. Claims 1, 15, and 23 are independent. Claim 1, reproduced below, is representative.

> 1. 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).

Ex. 1001, 5:33–51. Independent claims 15 and 23 respectively recite a "computer readable medium" and a "cryptographic unit" for performing the method of claim 1. *Id.* at 6:48–67, 7:24–8:9.

D. Asserted Evidence and Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability (Pet. 3–4):

Claims Challenged	35 U.S.C. §	Basis
1, 2, 5, 15, 16, 19	103	DSS,[1] Schneier,[2] Rose[3]
1, 2, 5, 15, 16, 19	103	DSS, Schneier, Menezes[4]
23, 24, 27	103	DSS, Schneier, Rose, Rao,[5] Floyd[6]
23, 24, 27	103	DSS, Schneier, Menezes, Rao, Floyd

Petitioner relies on the Declaration of Dr. Jonathan Katz, Ph.D. (Ex. 1002) to support its patentability challenge. Patent Owner presents the Declaration of Dr. Markus Jakobsson, Ph.D. (Ex. 2001) in support of its position.

ANALYSIS

A. Level of Ordinary Skill

Petitioner contends that a person of ordinary skill in the art at the time of invention of the '961 patent "would have possessed at least a bachelor's degree in electrical engineering or computer science (or equivalent degree) and at least two years of experience with computer-based cryptographic techniques." Pet. 6 (citing Ex. 1002 ¶¶ 11–13). Patent Owner does not address the requisite level of skill in its Preliminary Response.

For purposes of this Decision, we adopt Petitioner's undisputed definition of the level of ordinary skill in the art, as it is consistent with the

[1] Federal Information Processing (FIPS) Publication 186, *Digital Signature Standard (DSS)* (May 19, 1994) (Ex. 1004).
[2] Schneier, Applied Cryptography (2d ed. 1996) (Ex. 1008).
[3] Rose, *Re: "Card-shuffling" algorithms*, USENET, sci.crypt, sci.math (March 10, 1993) (Ex. 1006).
[4] Menezes *et al.*, Handbook of Applied Cryptography (1997) (Ex. 1005).
[5] Rao, Error Coding for Arithmetic Processors (1974) (Ex. 1018).
[6] Floyd, Essentials of Data Processing (1987) (Ex. 1019).

level of skill reflected in the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

B. Claim Construction

In this *inter partes* review proceeding, the claims of the patent are construed using the same standard used in federal district court, including construing the claim in accordance with the ordinary and customary meaning of the claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340, 51,340, 51,358 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)).

Neither party requests construction of any claim term for purposes of this proceeding. Pet. 16–17; Prelim. Resp. 14–15. The parties note, however, that in response to their dispute in the related district court action concerning the construction of the claim term "reducing mod q," the district construed that term to mean "computing the remainder of dividing a value by q." Prelim. Resp. 14 (citing Ex. 2002, 31–35); Pet. 16–17.

We have considered the claim construction analysis and ruling of the district court, and agree that for purposes of this Decision, the district court's interpretation of "reducing mod q" as meaning "computing the remainder of dividing a value by q" is reasonable. As such, we adopt that interpretation here. We note, however, that our conclusion that Petitioner has not established a reasonable likelihood of prevailing as to any of the challenged claims does not turn on any particular construction of "reducing mod q."

C. References Relied Upon

1. DSS

DSS, the Digital Signature Standard, was published in 1994 and adopted by the U.S. Department of Commerce. Ex. 1004, 1. DSS describes "the Digital Signature Algorithm (DSA) for digital signature generation and verification." *Id.* at 5. DSS explains that "[t]he DSA authenticates the integrity of the signed data and the identity of the signatory. The DSA may also be used in proving to a third party that data was actually signed by the generator of the signature." *Id.* at 2–3.

Figure 1 of DSS is reproduced below.

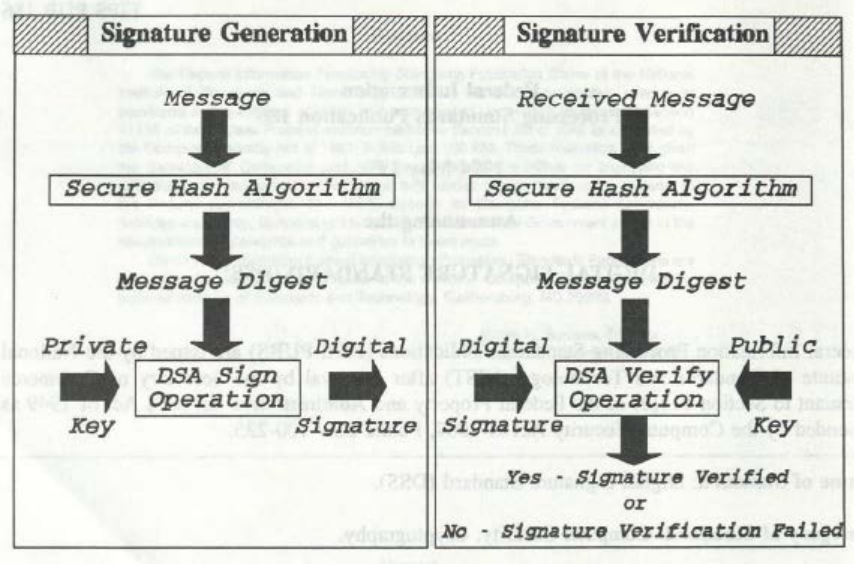

Figure 1 provides an overview of the methods for digital signature generation and verification taught by DSS. *Id.* at 1–2. As shown in Figure 1, each signatory has a private key and a public key. *Id.* at 5. A user's private key is used for signature generation, and the user's public key is used for signature verification. *Id.* "An adversary, who does not know the private key of the signatory, cannot generate the correct signature of the signatory. In other words, signatures cannot be forged. However, by using

the signatory's public key, anyone can verify a correctly signed message." *Id.*

DSA requires both long term and short term (i.e., ephemeral) private keys to generate a digital signature for a message. Ex. 1004, 10–11, 17–18. Of particular relevance here is the algorithm for computing ephemeral key k disclosed in Appendix 3.2 of DSS, which is reproduced, in part, below.

3.2. ALGORITHM FOR PRECOMPUTING ONE OR MORE k AND r VALUES

This algorithm can be used to precompute k, k^{-1}, and r for m messages at a time. Algorithm:

Step 1. Choose a secret initial value for the seed-key, KKEY.

Step 2. In hexadecimal notation let

t = EFCDAB89 98BADCFE 10325476 C3D2E1F0 67452301.

This is a cyclic shift of the initial value for $H_0 \| H_1 \| H_2 \| H_3 \| H_4$ in the SHS.

Step 3. For j = 0 to m - 1 do

a. k = G(t,KKEY) mod q.

b. Compute $k_j^{-1} = k^{-1} \bmod q$.

c. Compute $r_j = (g^k \bmod p) \bmod q$.

d. KKEY = (1 + KKEY + k) mod 2^b.

As shown in the above excerpt of Appendix 3.2, DSS discloses a method for computing an ephemeral key k by selecting a secret value for the seed-key, KKEY, performing a hash function, G(t,KKEY), on KKEY, and then performing a modular reduction ("modulo" or "mod") operation, mod q, on the output of the hash function. Ex. 1004, 14.

2. Rose

Rose is a document that was posted to the sci.crypt and sci.math newsgroups on USENET in 1993. Ex. 1006, 1; *see also* Ex. 1030 ¶¶ 4–5. Rose addresses a prior USENET post that suggested generating random

numbers from 0 to 2 by performing a mod 3 operation on the output of a random number generator. *Id.* at 1. According to Rose, such a method is flawed because "[w]hen the desired interval doesn't exactly divide the interval you already have, the smaller numbers are more likely than the larger ones. What you really have to do is throw away any result from the original generator that is too big." *Id.* at 2.

Rose discloses source code, reproduced below, designed to avoid the bias towards low numbers introduced by performing a mod 3 operation on the output of a random number generator. Ex. 1006, 2.

```
/*
 * Roll a random number [0..n-1].
 * Avoid the slight bias to low numbers.
 */
int
roll(int n)
{
    long        rval;
    long        biggest;
#define BIG 0x7FFFFFFFL /* biggest value returned by random() */

    if (n == 0)
        return 0;
    biggest = (BIG / n) * n;
    do {
        rval = random();
    } while (rval >= biggest);
    return rval % n;
}
```

As shown in the above source code excerpt, Rose discloses a method that generates a random number within a specified range [0, n-1]. Ex. 1006, 2. Rose's method first computes the largest multiple of n that is less than or equal to "BIG," i.e., "the biggest value returned by random ()," and assigns this value to the variable "biggest." Ex. 1006, 2. The method then enters a do-while loop that repeatedly determines a random number using the random() function until the output of the random() function is less than the

value of "biggest." *Id.* The method assigns final output of the random() function to "rval," and then computes rval mod n. *Id.*

3. Menezes

Menezes is a cryptography textbook published in 1997. Ex. 1005, ii. Of particular relevance to Petitioner's patentability challenge is Menezes's discussion of random bit generators. Menezes defines a "random bit generator" as "a device or algorithm which outputs a sequence of statistically independent and unbiased binary digits." Ex. 1005, 170. Menezes goes on to explain that

> [a] random bit generator can be used to generate (uniformly distributed) random numbers. For example, a random integer in the interval [0, *n*] can be obtained by generating a random bit sequence of length [lg *n*] + 1, and converting it to an integer; if the resulting integer exceeds *n*, one option is to discard it and generate a new random bit sequence.

Id.

4. Schneier

Schneier is a cryptography textbook published in 1996. Ex. 1008, iv. Schneier describes techniques for generating random and pseudorandom numbers. *Id.* at 421–428. According to Schneier,

> [s]ometimes cryptographically secure pseudo-random numbers are not good enough. Many times in cryptography, you want real random numbers. Key generation is a prime example. It's fine to generate random cryptographic keys based on a pseudo-random sequence generator, but if an adversary gets a copy of that generator and the master key, the adversary can create the same keys and break your cryptosystem, no matter how secure your algorithms are. A random-sequence generator's sequences cannot be reproduced. No one, not even you, can reproduce the bit sequence out of those generators.

Id. at 421–422.

5. Rao

Rao is an arithmetic coding textbook published in 1974. Ex. 1018, iv. Rao teaches that computers are divided into functional units or subsystems, including an "arithmetic processor." *Id.* at 39. Rao also discloses that "[a]n arithmetic processor is the part of a computer that provides the logic circuits required to perform arithmetic operations such as ADD, SUBTRACT, MULTIPLY, DIVIDE, SQUARE-ROOT, etc." *Id.* at 41.

6. Floyd

Floyd is a data processing textbook published by 1987. Ex. 1019, iv. Floyd teaches that in computers having a microprocessor, arithmetic processing is performed by a portion of a computer's central processing unit (CPU) known as an arithmetic/logic unit (ALU). *Id.* at 45–46.

D. Obviousness Grounds Based on Rose

Petitioner asserts that claims 1, 2, 5, 15, 16, and 19 of the '961 patent are rendered obvious by the combination of DSS, Schneier, and Rose. Pet. 19–47. Petitioner additionally asserts that claims 23, 24, and 27 are rendered obvious by the combination of DSS, Schneier, Rose, Rao, and Floyd. *Id.* at 57–63. To support its contentions, Petitioner cites to Dr. Katz's declaration testimony (Ex. 1002).

Patent Owner responds that Petitioner's proposed modification of DSS in view of Rose, which is essential to each of the asserted grounds of unpatentability based on Rose, is flawed and rooted in hindsight. Prelim. Resp. 16–39, 55–56. Patent Owner further asserts that the proffered combination of DSS and Rose would not have been obvious to try. *Id.* at 31–39, 55–56. Patent Owner refers to the declaration testimony of Dr. Jakobsson (Ex. 2001) to support its position.

In view of the record before us, we are not persuaded by Petitioner's arguments and evidence attempting to show that there is a reasonable likelihood that it would prevail in establishing that at least one of claims 1, 2, 5, 16, 16, 19, 23, 24, or 27 of the '961 patent is unpatentable over the combinations based on Rose.

Each challenged independent claim of the '961 patent requires evaluating the output of a hash function performed on a random number to determine if that output is less than a group of order q, and, if it is not, rejecting that value and repeating the method. More specifically, each of independent claims 1, 15, and 23 recites, in relevant part:

> 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;

Ex. 1001, 5:33–51, 6:48–67, 7:24–8:9.

For both asserted grounds of unpatentability based on Rose, Petitioner contends that the combination of DSS and Rose discloses or suggests the "determining," "accepting," "rejecting," and "repeating" steps of the challenged claims. Pet. 35–44, 59–63.

Petitioner acknowledges that "the '961 patent employs a different approach" for generating ephemeral private key k than that disclosed by DSS. Pet. 36. Petitioner likewise concedes that DSS does not disclose the

"determining," "accepting," "rejecting," or "repeating" steps of the challenged claims. *Id.* at 35. Rather, as Petitioner recognizes (Pet. 19–23), DSS simply performs a modulo operation on the output of the hash of a random value and stores that result as ephemeral private key k. Ex. 1004, 14 (Step 3.a.). DSS does not contemplate evaluating the output of the hash function prior to performing the modulo operation, much less iteratively repeating the process of selecting a new random number and performing a hash function on that number until a value less than q is obtained. *Id.* Indeed, in the context of describing a method for computing a batch of ephemeral private keys k, rather than select a new random number for use in computing each key k in the batch, DSS discloses updating the value of the seed-key (KKEY) and using that updated value to calculate k. *Id.* at 14 (Step 3.d.).

Rose likewise fails to disclose "determining," "accepting," "rejecting," or "repeating" steps performed on the output of a hash function as recited the challenged claims. Ex. 1006, 1–2. Rather, Rose describes a method for performing the basic task of random number generation within a specified range—absent any hashing step—that avoids the bias towards low numbers observed with other techniques. Ex. 1002, 2. More particularly, Rose's method determines a random number within the range [0, n-1] by: (1) computing the largest multiple of n that is less than or equal to the biggest value returned by the function random (); (2) entering a do-while loop that iteratively generates random numbers using the function random () until the output of that function is less than the largest multiple of n determined in step (1); and (3) performing a modulo n operation on the output of the do-while loop and returning the result of that operation as the result of the software routine. *Id.* Rose does not disclose hashing the

random number at any point in the method. *Id.* Nor does Rose contemplate, for example, how its technique might be applied to a cryptographic key generation algorithm, whether its technique might be useful in avoiding bias in the output of a hash function performed on a random number, or whether avoidance of modulo bias requires iteratively repeating both the selection of a random number and hashing that number. *Id.* at 1–2.

Petitioner does not adequately explain, in view of the gaps in DSS and Rose, why an ordinarily skilled artisan would have sought to modify DSS by applying Rose's technique for eliminating modulo bias in basic random number generation to accept or reject a hashed random number, or to iteratively generate and hash a new random number after each rejection. Instead, Petitioner presumes, without sufficient explanation, that because Rose identifies a solution for addressing the modulo bias problem in basic random number generation, and because it was known at the time of invention of the '961 patent that performance of a modulo operation on the output of a hash function, as disclosed by DSS, could create a bias towards lower values, an ordinarily skilled artisan would "have been motivated to use the technique in Rose to maintain a uniform distribution of random numbers over the range specified by q, resulting in a cryptographically stronger key k, in turn increasing the strength of the resulting digital signature scheme." Pet. 43–44 (emphasis omitted).

Petitioner's presumption is insufficient, however, to support institution of *inter partes* review. For example, Petitioner's inchoate explanation does not adequately address why an ordinarily skilled artisan would have understood that Rose's method for avoiding modulo bias in basic random number generation—absent any hashing—would have been transferable to mitigate modulo bias in the selection of an output of a hash

function after the random number has been transformed. The hindsight driven nature of Petitioner's proposed combination is further underscored by the fact that it iterates both the random number generation and the hashing steps without providing sufficient explanation as to why an ordinarily skilled artisan would have taken such an approach. Specifically, Petitioner asserts that the proffered combination would have resulted in the following method for generating ephemeral private key k:

> (1) Generate a random number for KKEY in accordance with DSS alone or in combination with Schneier[7] (the claimed "seed value SV"), as explained for claim 1[a];
>
> (2) perform a hash of KKEY, G(t,KKEY), according to DSS (the claimed "output H(SV)"), as explained for claim 1[b];
>
> (3) determine whether G(t,KKEY) ("output H(SV)") is less than order q (i.e. the value q),[] according to the teachings of Rose;
>
> (4) accept G(t,KKEY) ("output H(SV)") if G(t,KKEY) is less than q, according to the teachings of Rose;
>
> (5) reject G(t,KKEY) if it is not less than q, by repeating the method and going back to step (1), according to the teachings of Rose; and
>
> (6) if G(t,KKEY) ("output H(SV)") was accepted in step (4), perform a "mod q" operation on G(t,KKEY), pursuant

[7] Petitioner relies on Schneier solely to establish that an ordinarily skilled artisan would have employed a random—rather than pseudorandom—number generator to generate a cryptographic key. *See* Pet. 33–34. As Petitioner's assertions regarding Schneier are neither presently disputed by Patent Owner (Prelim. Resp. 17 n.5), nor germane to our discussion, we, like the parties, focus our analysis on the combination of DSS and Rose.

> to the teachings of Rose, and provide it as a key k for use in performing a cryptographic function, in accordance with DSS.

Pet. 41–42 (emphasis omitted) (citing Ex. 1002 ¶ 150). But Petitioner does not adequately explain why an ordinarily skilled artisan would have arrived at this combination given that (1) Rose does not address hashing; (2) neither DSS nor Rose contemplates repeating both the random number generation step and the hashing step; and (3) in the context of batch key generation, DSS does not suggest generating a new random number for each key k, but simply updating the original random number using a deterministic function. *See Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1069 (Fed. Cir. 2018) ("statements regarding preferences are relevant to a finding regarding whether a skilled artisan would be motivated to combine that reference with another reference").

Petitioner's contention that "Rose's technique would also have been obvious to try" (Pet. 44 (citing Ex. 1002 ¶ 158)) because "rejecting values that fall outside a desired range was a well-known way of obtaining a uniform distribution of random numbers within the range" (*id.*) is likewise unpersuasive. In view of the insufficiently explained gap between DSS's method for generating key k by performing a modulo operation on the hash of a random number and Rose's "simple and generic technique" (Pet. 40) for basic random number generation—absent any hashing—Petitioner cannot be said to have demonstrated that the proposed combination would have been obvious to try. For example, Petitioner does not adequately explain why it would have been obvious to try iteratively generating a new random number and hashing that number whenever the output of the hash function is greater than or equal to order q, given that neither DSS nor Rose contemplates performing and repeating both of those operations—each of which consumes

computational resources—every time the output of the hash function falls outside of the desired range.

> [A]n invention is not obvious to try where vague prior art does not guide an inventor toward a particular solution. A finding of obviousness would not obtain where "what was 'obvious to try' was to explore a new technology or general approach that seemed to be a promising field of experimentation, where the prior art gave only general guidance as to the particular form of the claimed invention or how to achieve it."

Bayer Schering Pharma AG v. Barr Labs., Inc., 575 F.3d 1341, 1347 (Fed. Cir. 2009) (quoting *In re O'Farrell*, 853 F.2d 894 (Fed. Cir. 1988)). Absent sufficient justification by Petitioner, and in view of the fact that Rose does not contemplate hashing, DSS does not contemplate iteratively generating and evaluating random numbers, and neither Rose nor DSS discusses iteratively performing random number generation and hashing steps, we cannot agree that Petitioner's proposal to modify DSS by inserting iterative random number generation and hashing steps in the method would have been obvious to try.

Accordingly, based on the record before us, we determine that Petitioner has not demonstrated a reasonable likelihood of establishing that an ordinarily skilled artisan would have had reason to combine DSS and Rose in the proposed manner. As such, we conclude that Petitioner has not shown a reasonable likelihood in prevailing in its assertion that any of claims 1, 2, 5, 15, 16, 19, 23, 24, or 27 would have been obvious in view of the combinations based on Rose.

E. Obviousness Grounds Based on Menezes

Petitioner asserts that claims 1, 2, 5, 15, 16, and 19 of the '961 patent are rendered obvious by the combination of DSS, Schneier, and Menezes. Pet. 47–57. Petitioner also asserts that claims 23, 24, and 27 are rendered

obvious by the combination of DSS, Schneier, Menezes, Rao, and Floyd. *Id.* at 57–63. To support its contentions, Petitioner cites to Dr. Katz's declaration testimony (Ex. 1002).

Patent Owner responds that Petitioner's proposed modification of DSS in view of Menezes, which is central to each asserted ground of unpatentability including Menezes, is flawed and rooted in hindsight. Prelim. Resp. 39–52, 55–56. Patent Owner further asserts that the proffered combination of DSS and Menezes would not have been obvious to try. *Id.* at 52–56. Patent Owner refers to the declaration testimony of Dr. Jakobsson (Ex. 2001) to support its position.

In view of the record before us, we are not persuaded by Petitioner's arguments and evidence attempting to show that there is a reasonable likelihood that it would prevail in establishing that at least one of claims 1, 2, 5, 16, 16, 19, 23, 24, or 27 of the '961 patent is unpatentable over the combinations based on Menezes.

For each asserted ground of unpatentability based on Menezes, Petitioner contends that the combination of DSS and Menezes discloses or suggests the "determining," "accepting," "rejecting," and "repeating" steps of the challenged claims. Pet. 50–55, 59–63.

Petitioner's contentions concerning the combination of DSS and Menezes are similar to those described above regarding the combination of DSS and Rose, and, thus, suffer from similar deficiencies. Like DSS and Rose, the portions of Menezes relied upon by Petitioner fail to disclose "determining," "accepting," "rejecting," and "repeating" steps performed on the output of a hash function as required by the challenged claims. Pet. 50–55; Ex. 1005, 170. The primary excerpt of Menezes cited by Petitioner explains that "a random integer in the interval [0, *n*] can be obtained by

generating a random bit sequence of length [lg *n*] + 1, and converting it to an integer; if the resulting integer exceeds *n*, one option is to discard it and generate a new random bit sequence." Ex. 1005, 170. It does not mention hashing, and does not contemplate, for example, whether its technique might be useful for accepting or rejecting the result of performing a hash function on a randomly generated seed value, or whether iterative repetition of both the generation of a random number and performance of a hash function on that number when the output of the hash function falls outside of a desired range would be appropriate. *Id.* Moreover, as Petitioner acknowledges (Pet. 54), the cited portions of Menezes do not address modulo bias. Ex. 1005, 170.

In view of these gaps, as with the combination of DSS and Rose, Petitioner does not adequately explain why an ordinarily skilled artisan would have sought to modify DSS by applying Menezes's technique for random number generation to accept or reject a hashed random number. As an initial matter, Petitioner acknowledges that, in contrast to Rose, "Menezes does not specifically describe the potential bias that can arise from performing a modulo reduction on a random number." Pet. 54. Accordingly, Petitioner contends that such an artisan would "have been motivated to use the technique in Menezes to solve a particular problem in implementing DSS – ensuring that the resulting **k** value falls within the desired range of 0 to q-1." *Id.* (citing Ex. 1002 ¶ 188). But Petitioner does not present evidence or argument sufficient to establish, for purposes of institution, that obtaining k values within the desired range was a "problem in implementing DSS" (*id.*). To the contrary, the evidence of record indicates that by performing a modulo q operation on the value obtained by hashing a random number, DSS reliably generated values for k within the

desired range. Ex. 1004, 14; Ex. 1001, 2:38–47. The flaw in DSS arose from the slight bias towards k values at the low end of the prescribed range caused by reliance on a modulo operation to ensure that k fell within the required range, not any difficulty in generating in-range k values in the first instance. Ex. 1004, 14; Ex. 1001, 2:38–47.

Petitioner's assertion that it would have been obvious to try modifying DSS to incorporate Menezes's random number generation technique (*see* Pet. 54–55) fails because Menezes's simplistic technique for basic random number generation—which does not include hashing—at most identifies a general approach for generating random numbers within a range. *See Bayer*, 575 F.3d at 1347. Menezes cannot be said, however, to guide an inventor toward the particular solution set forth in the '961 patent. *See id.* For example, Petitioner does not adequately explain why, based on Menezes's general method for generating uniformly distributed random numbers using a basic acceptance-rejection technique that does not involve hashing, it would have been obvious to try modifying DSS to iteratively generate a new random number and hash that number whenever the output of the hash function falls outside the desired range. Absent sufficient justification by Petitioner, and in view of the fact that Menezes does not contemplate hashing, DSS does not contemplate iteratively generating and evaluating random numbers, and neither Menezes nor DSS discusses iteratively performing both random number generation and hashing steps, Menezes cannot be said to guide an inventor toward the particular solution claimed in the '961 patent, but rather, identifies only a general approach (basic random number generation) that might merit exploration. *See Bayer*, 575 F.3d at 1347. Accordingly, the proposed combination would not have been obvious to try.

Petitioner's contention that an ordinarily skilled artisan would "have been motivated to use the technique in Menezes to obtain uniformly distributed random numbers, resulting in a cryptographically stronger key k for DSS and, in turn, a stronger digital signature" (Pet. 55 (citing Ex. 1002, ¶¶ 189–190)) is similarly unavailing. As explained above, Menezes discusses random number generation in a different context than the claimed invention—namely, one that does not involve hashing. Petitioner fails to present evidence or argument sufficient to establish, for purposes of institution, that Menezes's method for generating uniformly distributed random numbers via a random bit generator would have been useful in the context of evaluating hashes of random numbers that were output by a random number generator. Petitioner likewise fails to adequately justify why an ordinarily skilled artisan would have combined DSS and Menezes in the proposed fashion, such that each of the random number generation and hashing steps would be repeated whenever the output of the hash function fell outside of the desired range.

To the extent Petitioner asserts that an ordinarily skilled artisan would have turned to Menezes to avoid the known modulo bias problem, that argument fails for the same reasons described above concerning the combination of DSS and Rose. *See* Pet. 54 ("Accordingly, the modulo bias problem, and the reasons to avoid it, were already known."). Specifically, Petitioner does not adequately justify the proposed combination given that (1) Menezes does not address hashing; (2) neither DSS nor Menezes contemplates repeating both a random number generation step and a hashing step; and (3) in the context of batch key generation, DSS does not suggest generating a new random number for each key k, but simply updating the

original random number using a deterministic function. *See Polaris*, 882 F.3d at 1069.

Accordingly, based on the record before us, we determine that Petitioner has not demonstrated a reasonable likelihood of establishing that an ordinarily skilled artisan would have had reason to combine DSS and Menezes in the proposed manner. As such, we conclude that Petitioner has not shown a reasonable likelihood in prevailing in its assertion that any of claims 1, 2, 5, 15, 16, 19, 23, 24, or 27 would have been obvious in view of the combinations based on Menezes.

CONCLUSION

Having reviewed the record before us, we are not persuaded that Petitioner has demonstrated a reasonable likelihood of prevailing with respect to any one of the challenged claims. Therefore, we do not institute the requested *inter partes* review.

ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is *denied*; and

FURTHER ORDERED that the requested *inter partes* review is not instituted with respect to any claim of the ’961 patent.

PETITIONER:

Heidi L. Keefe
Andrew C. Mace
COOLEY LLP
hkeefe@cooley.com
amace@cooley.com

FOR PATENT OWNER:

Michael T. Hawkins
Nicholas Stephens
Kenneth W. Darby
Kim Leung
Craig A. Deutsch
FISH & RICHARDSON P.C.
hawkins@fr.com
nstephens@fr.com
kdarby@fr.com
kim.leung@gazpat.com
deutsch@fr.com

James M. Glass
Ogi Zivojnovic
QUINN EMANUEL URQUHART, & SULLIVAN, LLP
jimglass@quinnemanuel.com
ogizivojnovic@quinnemanuel.com