

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MOBILEIRON, INC.,

Petitioner,

v.

BLACKBERRY CORPORATION and BLACKBERRY, LTD.,

Patent Owners.

Case IPR2020-XXX

Patent 7,372,961

Title: Method of Public Key Generation

**DECLARATION OF DANIELE MICCIANCIO IN SUPPORT OF
PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 7,372,961**

I, Daniele Micciancio, declare:

I make this declaration of my own personal knowledge, and if called upon as a witness could and would testify competently to the matters stated herein.

1. I am currently a Professor of Computer Science and Engineering employed by the University of California: San Diego (“UCSD”), and I specialize in cryptography. I am also an International Association of Cryptography Research (“IACR”) fellow, and have served as the IACR program chair of CRYPTO 2019 and CRYPTO 2020. As part of my profession, I author papers on various topics relevant to cryptography.

2. While I was a graduate student at the Massachusetts Institute of Technology, I co-authored with Mihir Bellare and Shafi Goldwasser a paper titled “ ‘Pseudo-Random’ Number Generation Within Cryptographic Algorithms: The DDS Case,” which was published by Springer as a part of the Lecture Notes in Computer Science (“LNCS”) book series in proceedings of the Annual International Cryptology Conference (“CRYPTO”) in 1997.¹

3. The paper discusses the ramifications arising from the fact that if numbers for the Digital Signal Standard (“DSS”) algorithm are generated using a linear congruential pseudorandom number generator (“LCG”), then the secret key can be quickly recovered after seeing a few signatures.

4. The publisher Springer is a well-known publication that releases one of the primary series of volumes in the cryptography space. Any library that offered the Springer series in 1997 would likely have indexed this volume too, and made it available shortly after publication to any member of the public, particularly those interested in the topic of cryptography. I have personal knowledge that several libraries indexed Springer in the period 1997-99, because I myself used Springer in my research during this period.

¹ Citation to this paper can be found in the bibliography, available for download as “Back Matter” on Springer’s book publication page available at <https://link.springer.com/content/pdf/bbm%3A978-3-662-12521-2%2F1.pdf>.

5. On August 19, 1997, I presented my paper at CRYPTO, which is held in Santa Barbara, California.² My presentation was public, and was not made subject to any confidentiality restrictions.

6. CRYPTO is the premier cryptography event and has been held annually since the 1980s. Its popularity and fame in the field of cryptography can be likened to the “Oscars of cryptography.” I myself have chaired CRYPTO twice – in 2019 and 2020 – and am very familiar with its procedures, including how rapidly papers presented at the conference are disseminated to and made publicly available to researchers and practitioners in the field of cryptography.

7. In 1997, when I presented my paper, 514 people registered to attend the conference and I believe at least 400 were in attendance during my presentation.³ I believe that this constitutes a large fraction of the cryptography research community worldwide. Anyone could register to attend CRYPTO and, to my knowledge, there were no specific confidentiality requirements on the use of materials presented at the conference. At CRYPTO, printed materials of all of the conference workshops, including my paper, were distributed to all attendees without any restrictions on their further dissemination. They were also widely disseminated and made publicly available immediately after the conference, throughout the next two years.

8. It is common practice in academia to bolster work product on personal websites and to make it widely available to others in the scientific and engineering field to which the paper relates. I recall that I made my 1997 CRYPTO paper available in 1997 on my personal MIT student page, but that webpage no longer exists. However, a version of my paper, dated May 1997, is available online on my UCSD webpage⁴ and on an MIT publication listing.⁵ My

² The full program is available online at <https://www.iacr.org/conferences/c97/c97prog.html>.

³ The IACR keeps statistics of its attendees and makes them publicly available at <https://secure.iacr.org/membership/statistics/conferences.php>.

⁴ <http://cseweb.ucsd.edu/~daniele/papers/BGM.html>.

⁵ <http://groups.csail.mit.edu/cis/cis-publications.html>.

1997 CRYPTO paper has been locatable since shortly after its presentation in 1997 through common Internet search engines.

9. Additionally, I have personal knowledge that my paper disseminated world-wide to others in the field of cryptography between my presentation at CRYPTO in 1997 and 1999. For instance, the following citations to my paper were published by other researchers located in Europe, Japan, China, and the United States who were interested in and involved with cryptography during this period:

- a. December 9, 1997 thesis, “Digital Signature Schemes,” written by Nick Carruthers while a student at Middlebury College, p. 32 & n.5 (copy attached);⁶
- b. May 1998 doctoral dissertation, “Design of an Efficient Public-Key Cryptographic Library for RISC-Based Smart Cards,” written by Jean-François Dhem while a student at the Université Catholique de Louvain (p. 154 & n. [BGM97], p. 1999 (excerpts attached));⁷
- c. Kosheba Takeshi, Unpredictability of Pseduorandom Number Generators on Public Key Cryptosystems with Models of Computation and Algorithms (in Japanese), RIMS Kokyuroku (1093), 162-167, 1999-04 (Kyoto University), at p. 167 n.1 (copy attached);⁸
- d. June 1998 Master’s thesis, “Study on Elliptic Curve Public Key Cryptosystems with Application of Pseudorandom Number Generator,” written by Yuen Ching Wah while a student at The Chinese University of Hong Kong;⁹ and
- e. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*, a book written by notable cryptographer, Oded Goldreich, which was published in 1999.¹⁰

⁶ <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.100.1506&rep=rep1&type=pdf>.

⁷ http://users.belgacom.net/dhem/these/these_public.pdf.

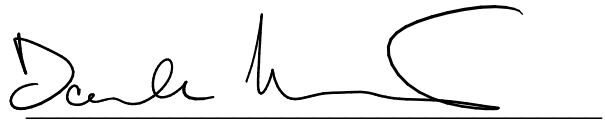
⁸ <https://hdl.handle.net/2433/62954> & <https://ci.nii.ac.jp/naid/110000163518/>.

⁹ <https://core.ac.uk/download/pdf/48534838.pdf>.

¹⁰ <https://link.springer.com/book/10.1007/978-3-662-12521-2>.

10. Thus, based on my personal knowledge and experience, my paper was published, indexed and readily locatable to persons interested in the subject matter of applied mathematics and cryptography prior to 1999 using at least common keyword searches on internet search engines. It was also published and disseminated in the materials made public during the 1997 CRYPTO conference, and was later further made available to libraries and similar repositories via the Springer publication.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my information, knowledge and belief after reasonable investigation, and this declaration was executed on September 28, 2020 in San Diego, CA, USA.

A handwritten signature in black ink, appearing to read 'Daniele Micciancio', is written over a horizontal line.

Daniele Micciancio