



Short Programs for Functions on Curves: A STOC Rejection

Victor S. Miller  

Computer Science Laboratory, SRI, Menlo Park, CA, USA

Abstract

In 1986 I submitted a note “Short Programs for functions on curves” to the STOC conference. It was rejected. Since it seemed to be a paper that would only be interesting to a very small group of people, I didn’t try to publish it, but instead circulated it among people who, I thought, would be interested in it. However, about 11 years later I was contacted by Dan Boneh, to whom I had given a copy a few years previously, who said that the algorithm in my paper had important applications. Since then it has become a core algorithm in the field of “Pairing Based Cryptography”.

2012 ACM Subject Classification Computing methodologies → Number theory algorithms; Security and privacy → Public key encryption

Keywords and phrases Elliptic Curves, Finite Fields, Weil Pairing, Straight Line Program

Digital Object Identifier 10.4230/LIPIcs.FUN.2024.34

Category Salon des Refusés

Related Version Short Programs for Functions on Curves: unpublished

Unpublished: <https://crypto.stanford.edu/miller/miller.pdf>

Full Version: <https://link.springer.com/article/10.1007/s00145-004-0315-8>

1 Prehistory

The paper that I want to discuss is “Short Programs for functions on curves” [16] which I wrote in 1986, while I was a member of the Mathematics Department at the IBM TJ Watson Research Center, and submitted to the STOC conference. It was rejected. Since it seemed to be a paper that would only be interesting to a very small group of people, I didn’t try to publish it, but instead circulated it among people whom I thought would be interested.

The main result of the paper was an efficient algorithm for the calculation of the **Weil Pairing** for Elliptic Curves over Finite Fields. At the time of writing, the field of Elliptic Curves was considered a very arcane branch of Number Theory. In 1985 I presented a paper “Use of Elliptic Curves in Cryptography” [15] at the annual Crypto conference in Santa Barbara. At the time, and for many years thereafter, using Elliptic Curves for cryptography seemed to be a very obscure niche. However, it eventually had great effect. For example a large percentage of the use of public key now uses Elliptic Curves.

The Weil Pairing was introduced by Andre Weil in 1940 [23], and has essential use in the Number Theoretic analysis of the arithmetic of Elliptic Curves. In response to a challenge of Manuel Blum, I tried to relate the discrete logarithm problem on Elliptic Curves to the more familiar problem in the multiplicative group of finite fields (which is what’s used in the original Diffie-Hellman key distribution protocol), I realized that the Weil pairing might be able to relate the two groups if it could be computed efficiently. Although it could be calculated as a ratio of two polynomials in the coordinates of the points, the degrees of the numerator and denominator were exponential in the size of the inputs. After seeing a talk by Erich Kaltofen [11], I realized that the needed result could be calculated by a short straight line program whose length was linear in the size of the inputs. The paper that I



© Victor S. Miller;

licensed under Creative Commons License CC-BY 4.0

12th International Conference on Fun with Algorithms (FUN 2024).

Editors: Andrei Z. Broder and Tami Tamir; Article No. 34; pp. 34:1–34:4

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

wrote described the algorithm. It also gave a partial answer to a question raised by Rene Schoof [19] (in another influential papers that was rejected by the FOCS conference in 1984) about the structure of an Elliptic Curve group.

2 Influence

The first mention of it was in a talk entitled “Elliptic Curves and Number Theoretic Algorithms” [12] given by Hendrik Lenstra at the International Congress of Mathematicians in Berkeley a few months later. I gave a copy of the paper to Burt Kaliski, then a graduate student at MIT, who used it in an essential way in his Ph.D. thesis “Elliptic Curves and Cryptography: A Pseudorandom bit generator and other tools” [10], and was the first (that I know of) to implement the algorithm. I gave a copy to Scott Vanstone at University of Waterloo who then used the algorithm in his influential paper with Menezes and Okamoto “Reducing elliptic curve logarithms to logarithms in a finite field” [14, 13].

I also gave a copy of the paper to Dan Boneh in 1994, when he was a graduate student at Princeton. A few years later, Dan got in touch and asked if it was ok with me for the Stanford CS department to make of copy of the paper available on the web. He told me that my algorithm had important applications. Indeed, using the algorithm was a crucial step in the realization of Shamir’s idea of “Identity Based Encryption” [21] described in the paper of Boneh and Franklin “Identity-based encryption from the Weil pairing” [4]. Antoine Joux in “A one round protocol for tripartite Diffie–Hellman” [8] also used my algorithm in an essential way. The three authors shared the Gödel prize [2] for their work.

3 Pairing Based Cryptography

Starting with the papers of Joux, and Boneh-Franklin, the field of “Pairing Based Cryptography” blossomed. For a number of years there was a conference on the subject “Pairing Based Cryptography” [22, 7, 20, 9, 1, 5] I gave the keynote address at the 2009 conference. Pairing based cryptography is still is a very lively field.

Because of its importance of my paper, Arjen Lenstra asked me in 2003 to write an extended version of the original paper for a special issue of the Journal of Cryptology, which appeared the next year [17]. According to Google Scholar, the unpublished manuscript has 483 citations in the published literature, and the extended version has 805 citations. Both are still being cited, with 28 citations in 2023.

4 Lasting Influence

Because it is now such an important part of the literature of cryptography, it has stopped being cited by many papers. A google search for “Miller’s algorithm” “pairing” produces 6250 hits. It has become standard terminology to speak of the “Miller loop” (which gets 5300 hits on google when “pairing” is included). The annual CFAIL conference [6], in 2019, gave me the inagural “Distinguished Failure Award” for keeping the original manuscript unpublished for so long. In 2008 NIST hosted a conference on Pairing Based Cryptography [18]. In the video “Pairings in Cryptography” [3] by Dan Boneh, at the 36 minute mark, there’s a discussion of my paper being rejected from STOC and its influence.

5 Intended Survey

I'll discuss the applications of the original paper, in particular give a survey of the field of pairing based cryptography.

References

- 1 Michael Abdalla and Tanja Lange, editors. *Pairing-Based Cryptography – Pairing 2012*, volume 7708 of *Lecture Notes in Computer Science*. Springer, May 2012. doi:10.1007/978-3-642-36334-4.
- 2 ACM. Gödel prize. URL: <https://www.acm.org/media-center/2013/may/acm-group-presents-godel-prize-for-advances-in-cryptography>.
- 3 Dan Boneh. Pairings in cryptography, July 2015. URL: <https://youtu.be/8WDOpzzxpTE?si=sXCoj8UFVBzzhxyF&t=2143>.
- 4 Dan Boneh and Matt Franklin. Identity-based encryption from the Weil pairing. In *Annual international cryptology conference*, pages 213–229. Springer, 2001. doi:10.1007/3-540-44647-8_13.
- 5 Zhenfu Cao and Fangguo Zhang, editors. *Pairing-Based Cryptography–Pairing 2013*, volume 8365 of *Lecture Notes in Computer Science*. Springer, November 2013. doi:10.1007/978-3-319-04873-4.
- 6 CFAIL. The conference for failed approaches and insightful losses in cryptology, 2019. URL: <https://www.cfail.org>.
- 7 Steven D. Galbraith and Kenneth G. Paterson, editors. *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*. Springer, September 2008. doi:10.1007/978-3-540-85538-5.
- 8 Antoine Joux. A one round protocol for tripartite Diffie–Hellman. In *International algorithmic number theory symposium*, volume 1838 of *Lecture Notes in Computer Science*, pages 385–393. Springer, 2000. doi:10.1007/10722028_23.
- 9 Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors. *Pairing-Based Cryptography–Pairing 2010*, volume 6487 of *Lecture Notes in Computer Science*. Springer, December 2010. doi:10.1007/978-3-642-17455-1.
- 10 Burton S. Kaliski. *Elliptic curves and cryptography: A pseudorandom bit generator and other tools*. PhD thesis, Massachusetts Institute of Technology, 1988. URL: <https://dspace.mit.edu/bitstream/handle/1721.1/14709/18494044-MIT.pdf>.
- 11 Erich Kaltofen. Computing with polynomials given by straight-line programs I: greatest common divisors. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing - STOC '85*. ACM Press, 1985. doi:10.1145/22145.22160.
- 12 Hendrik Willem Lenstra. Elliptic curves and number-theoretic algorithms. In Andrew M. Gleason, editor, *Proceedings of the International Congress of Mathematicians 1986*. Universiteit van Amsterdam Mathematisch Instituut, 1986. URL: www.math.leidenuniv.nl/~hw1/PUBLICATIONS/1988a/art.pdf.
- 13 A.J. Menezes, T. Okamoto, and S.A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5):1639–1646, 1993. doi:10.1109/18.259647.
- 14 Alfred Menezes, Tatsuaki Okamoto, and Scott Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. In *Proceedings of the twenty-third annual ACM symposium on Theory of computing*, pages 80–89, 1991. doi:10.1145/103418.103434.
- 15 Victor S Miller. Use of elliptic curves in cryptography. In *Conference on the theory and application of cryptographic techniques*, pages 417–426. Springer, 1985. doi:10.1007/3-540-39799-X_31.
- 16 Victor S. Miller. Short programs for functions on curves. STOC 1986 submission, May 1986. URL: <https://crypto.stanford.edu/miller/miller.pdf>.

34:4 Short Programs for Functions on Curves: A STOC Rejection

- 17 Victor S Miller. The Weil pairing, and its efficient calculation. *Journal of cryptology*, 17(4):235–261, 2004. doi:10.1007/s00145-004-0315-8.
- 18 NIST. Pairing based cryptography, June 2008. URL: <https://csrc.nist.gov/Projects/pairing-based-cryptography/events>.
- 19 René Schoof. Elliptic curves over finite fields and the computation of square roots mod p . *Mathematics of computation*, 44(170):483–494, 1985. doi:10.2307/2007968.
- 20 Hovav Shacham and Brent Waters, editors. *Pairing-Based Cryptography-Pairing 2009*, volume 5671 of *Lecture Notes in Computer Science*. Springer, August 2009. doi:10.1007/978-3-642-03298-1.
- 21 Adi Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology: Proceedings of CRYPTO 84*, pages 47–53. Springer, 1985. doi:10.1007/3-540-39568-7_5.
- 22 Tsuyoshi Takagi, Tatsuaki Okamoto, Eiji Okamoto, and Takeshi Okamoto, editors. *Pairing-Based Cryptography-Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*. Springer, July 2007. doi:10.1007/978-3-540-73489-5.
- 23 André Weil. Sur les fonctions algébriques a corps de constantes fini. *Comptes Rendus Acad. Sci. Paris*, 210(1940):592–594, 1940.