International Journal of Academic Research and Development
ISSN: 2455-4197, Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 2; Issue 4; July 2017; Page No. 201-205

Attacks on pairing based schemes in elliptic curve cryptography

Manoj Kumar

Department of Mathematics and Statistics, Gurukula Kangri Vishwavidyalaya, Haridwar, Uttarakhand, India

Abstract
Pairing-based cryptosystems have been one of the most active areas in elliptic curve cryptography since 2000. The pairings can be evaluated in polynomial time by Miller's algorithm. Many useful techniques have been suggested for optimizing the computation of the pairings. One of the most elegant techniques for computing the pairings efficiently is to shorten the iteration loop in Miller's algorithm. Pairing based schemes have been designed for various applications that have certain advantages over conventional RSA or discrete logarithm based encryption schemes. The concept of pairing was first introduced by Andre Weil in 1940. It plays an important role in the theoretical study of the arithmetic of elliptic curves and Abelian varieties. A lot of pairing based schemes exist in literature but all cannot be implemented in practice due to security reasons. In the present paper we shall study different types of attacks on pairing based schemes.

Keywords: pairing based cryptography, bilinear paring maps, security, elliptic curve cryptography, discrete logarithm problem, hyper elliptic curves

1. Introduction

The security of pairing-based cryptosystems relies on the difficulty of various computationally hard problems related to the discrete logarithm problem (DLP). However, there are also new attacks on the DLP on some groups [2, 4, 15, 16, 26]. Furthermore, very recent results on solving the DLP for finite fields of medium characteristics and composite degrees size have also significant consequences on the choice of primitives for pairing based cryptography [19, 21, 29]. The main technical part of pairing-based cryptography is the pairing functions including Weil, Tate and Ate pairing defined mostly on the product of certain subgroups of low dimensional abelian varieties over finite fields (in practice either on subgroups of elliptic curves or jacobians of genus two hyper-elliptic curves) [7]. Due to efficiency and reliability concerns of pairing based protocols many ad hoc and conceptual conversion methods from one type of pairing to another one has been proposed [9, 27, 31]. Abe *et al.* [1]. proposed a generic framework converting not only the protocols with the Type -I bilinear maps into the Type-II setting but also converting corresponding security proofs using black-box reduction methods in the random oracle model. Akinyele *et al.* [3]. have been very recently given some concerns about the practicability of the elegant theoretic solution of [2] and proposed an automated software tool transforming schemes using the Type-I bilinear maps into the Type-III setting. We note however that the proposed automated tool in [3] and generic frameworks in [1] suffer from being inefficient when compared to their manual counterparts like [9, 27, 31]. It is left as an open problem to generalize and systematize the manual advancement more efficiently for automated tools [3].

2. Elliptic Curve Cryptography

The use of elliptic curve cryptography was initially suggested by Koblitz [22] and Miller [25]. For $n \geq 1$ and a prime p let F_q be a finite field with $q = p^n$ elements. An elliptic curve E over F_q can be given by the Weierstrass equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \; a_i \in F_q \;, \; i = 1,2,...,6$$

Together with the condition that curve has no singular points.

If $q \neq 2,3$ then an easier representation of elliptic curve E is given by

$$y^2 = x^3 + ax + b \qquad (1)$$

where $qa = 0 \forall a \in F_q$ and the discriminant

$$\Delta = 4a^3 + 27b^2 \neq 0 (\mathrm{mod}\, q).$$

Thus an elliptic curve E is defined as the set of points (x, y) satisfying the equation (1) and including a point O called point at infinity.

The following properties hold on an elliptic curve E:

i). If $P(x, y)$ is a point on an elliptic curve E then inverse (reciprocal or opposite) point of P is $-P(x,-y)$.

ii). IF $P(x_1, y_1)$ and $Q(x_2, y_2)$ are two different points on the curve E, then their sum $R(x_3, y_3)$ is given by $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$, where $\lambda = (y_1 - y_2)/(x_1 - x_2)$.

iii). If $P = Q$ then $R(x_3, y_3) = 2P$ is given by $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = (3x_1^2 + a)/2y_1$.

3. Pairings Based Cryptography

As we know that every point on an elliptic curve E is one of two types (i) a point of finite order i.e. there exists a positive integer n such that $nP = O$ (ii) a point of infinite order i.e. there exist no such n. The points of first type are known as torsion points. Thus the set of torsion points P on an elliptic curve E denoted by $E[n]$ is defined as

$E[n] = \{P \in E : nP = O\}$.

It can be easily verified that $E[n]$ is a finite subgroup of E i.e. $(P_1 - P_2) \in E[n]$ for all $P_1, P_2 \in E[n]$.

For $n \in N$ (the set of natural numbers), let P and Q be two points of order n on an elliptic curve E defined over a finite field F_q. Let G_1 and G_2 be additive cyclic groups of prime order, generated by P and Q respectively i.e. $G_1 = < P >$ and $G_2 = < Q >$. Also let G_n be a multiplicative group of n[th] roots of unity in F_q^k i.e. $G_n = \{a \in F_q^k : a^n = 1\}$. Then a pairing on an elliptic curve E over finite field F_q, is a family of maps

$$e_n : G_1 \times G_2 \to G_n \quad (2)$$

Having the following properties:

1. $e_n(P_1 + P_2, Q) = e_n(P_1, Q).e_n(P_2, Q)$ and $e_n(P, Q_1 + Q_2) = e_n(P, Q_1).e_n(P, Q_2)$ for all $P, P_1, P_2 \in G_1$ and $Q, Q_1, Q_2 \in G_2$.
2. For some $0 \neq P \in G_1$ there exists $Q \in G_2$ such that $e_n(P, Q) \neq 1$ and for some $0 \neq Q \in G_2$ there exists $P \in G_1$ such that $e_n(P, Q) \neq 1$.
3. There exists an algorithm which computes the map e_n efficiently.

The value of the pairing belongs to finite field F_q^k and the embedding degree k is the least natural number such that $(q^k - 1)$ is divisible by n. The first property is known as bilinearity while second is called non-degeneracy. This bilinear property has enabled the construction of new cryptographic protocols using pairings. Although pairings exist for every elliptic curve but in practice there are curves whose pairings are not suitable for cryptographic applications. Associated to each elliptic curve, there is a parameter that can be calculated known as the embedding degree k. To implement pairings efficiently in cryptography, we required the value of k to be relatively small, definitely less than 100. However, it has been shown that almost all elliptic curves have very large k. Generally, k is of the same size as q, which is greater than or equal to 160 bits. There are mainly two common ways to find pairing-friendly elliptic curves. The first is to use what are known as super-singular elliptic curves, which always have embedding degree less than or equal to six. The second way is to use a technique called the complex multiplication method to construct certain families of elliptic curves with small embedding degree. There are advantages and drawbacks to each way. All known methods to determine such pairing-friendly curves can be found in [11]. In order to actually implement any pairing-based cryptographic protocol, it is necessary to choose a specific pairing map e_n. The two most commonly used pairings are the Weil and Tate pairings. With the goal of speeding up computation, researchers have discovered several new pairings. These include the Ate, Eta, reduced Tate, twisted Ate, and R-Ate pairings among others. It was observed by cryptographers that the various pairings are not interchangeable. For example, the Eta pairing can only be defined for super-singular curves. The Weil pairing satisfies $e_n(P, P) = 1$ for any point *P* in the domain, while the other pairings do not. The choice of pairing and elliptic curve is important.

Galbraith *et al.* [14]. were the first to identify that all of the potentially desirable properties in a protocol cannot be achieved simultaneously, and therefore classified pairings into certain three types. Although Galbraith *et al.* [14]. Originally presented three types of pairings but a fourth type was added soon after by Shacham [30]. There are now four types of pairings in literature (chapter 4, pp. 58-59 of [10]) discussed as under:

1. **Type-I:** The pairing (2) is said to be of type I if $G_1 = G_2$ and there exists no short representations for the elements of G_1.
2. **Type-II:** The pairing (2) is said to be of type II if $G_1 \neq G_2$ and there exists an efficiently computable homomorphism of G_2 into G_1 but not conversely. In this case no efficient secure hashing to the elements in G_2 is possible.

3. **Type-III:** The pairing (2) is said to be of type II if $G_1 \neq G_2$ and there exists no efficiently computable homomorphism between G_1 and G_2.
4. **Type-IV:** The pairing (2) is said to be of type II if $G_1 \neq G_2$ and there exists an efficiently computable homomorphism of G_2 into G_1 with an efficient secure hashing method to the group elements. This type of pairing is not generally used in protocol designs due to its insufficiency.

The pairing types essentially arise from observing the practical implications of choosing G_1 and G_2 in different subgroups of $E[n]$. The main factors affecting the classification are the ability to hash and/or randomly sample elements of G_2 i.e. the existence of an isomorphism of G_2 into G_1 which is often required to make security proofs work and issues concerning storage and efficiency. Pairings on super-singular curves come under type-I, while the other types of pairings are defined over ordinary elliptic curves. The pairing of type I is commonly known as symmetric pairing while other types of pairings are called asymmetric pairings. The drawback of type-I pairing comes when considering bandwidth and efficiency, as the condition that E be super-singular is highly restrictive when it comes to optimizing the speed of computing pairing.

4. Attacks on pairing based cryptography

As mentioned earlier, the security of pairing-based cryptography is based on the bilinear Diffie-Hellman problem. This is a relatively new problem in cryptography, and has not yet been as well-studied as other problems, such as the DLP. Several attacks on the DLP have recently been proposed improving the function field sieve algorithm in the multiplicative group of finite fields of small characteristics [2, 4, 15, 16, 26]. There are serious implications of these attacks on the security of pairing-based cryptography. More concretely, the use of symmetric pairing, and hence the use of pairing-friendly elliptic or hyper elliptic curves over finite fields of small characteristic are essentially useless [2, 16]. Concrete attacks are performed for certain super-singular elliptic or hyper elliptic curves [2, 16]. Difficulties of generalizing these attacks on the elliptic curve setting are pointed out in a recent work of Massierer [23]. However, it can be argued more generally that the use of elliptic curves over finite fields of small characteristics in group-based cryptography has severe potential security threads. There are mainly two new attacks on pairing based cryptography.

A. Quasi Polynomial Attack

It was a well-known fact that the DLP for the multiplicative subgroups of finite fields is not as difficult as in the generic groups. However, many researches have been done using these groups for cryptographic purposes by neglecting possible use of the algorithmic description of these groups to solve the discrete logarithm instances. The situation has been dramatically changed with the recent advancements of Joux *et al.* [4]. and Gologlu *et al.* [15]. Recently, Granger *et al.* [17]. Improved the result of Joux *et al.* [4]. by proposing a new expected quasi-polynomial algorithm for solving the DLP for finite fields F_q^k with roughly $q \approx k$. These attacks removed the DLP for multiplicative subgroups of small characteristic finite fields from the list of intractable problems.

B. Composite Degree Finite Fields Attack

Very recent results on a variant of the number field sieve algorithm for solving the discrete logarithm problem in medium characteristics finite fields of composite degrees have direct consequences on the choice of key sizes for pairing based algorithms [19, 21, 29]. The complexity analysis of these new techniques suggests that doubling the sizes of the underlying elliptic curves is a conservative choice of maintaining the desired security level.

Since, the algorithms for solving the DLP for finite fields are applicable on the discrete logarithm instances of pairing groups G_1 and G_2, therefore, these new attacks have direct consequences on the security of many pairing-based cryptographic applications if the characteristic of the field defining G_1 is small [20]. In order to understand the impact of these attacks on the design of pairing-based cryptographic protocols, we now briefly summarize the realization of bilinear maps using suitable elliptic curves for cryptographic purposes.

Over a finite field F_q with $q = p^m$, p a prime and m a positive integer, the candidate groups G_1 and G_2 of bilinear maps (2) are certain subgroups of a carefully chosen elliptic curve E over F_q. In particular, G_1 is the n^{th} torsion subgroup $E[n]$ and G_2 is a certain group related to the explicit realization of the bilinear map. A detail study can be found in [7].

4.1 Consequences of the above Attacks

As briefly discussed above, the new attacks for solving the DLP on the multiplicative subgroup of small characteristic finite fields have also dramatic consequences for the design of pairing-based protocols. In fact, these attacks showed either the insecurity of the use of super-singular elliptic curves or the inefficiency of their usage in the pairing-based settings [2, 4, 15, 16, 26]. Since the Type-I pairing can only be realized using super-singular elliptic or hyper-elliptic curves [14], therefore all Type-I bilinear maps and the related protocols are either useless or regarded completely as insecure.

The attack of Barbulescu and Kim [21] reduces the complexity of solving the DLP problem on F_p^n from $L_n\left(1/3, \sqrt[3]{96/9}\right)$ to $L_n\left(1/3, \sqrt[3]{48/9}\right)$ if $n = \lambda\mu$ with $\gcd(\lambda, \mu) = 1$ and $\lambda, \mu > 1$. Recently, Jeong

and Kim removed the condition $\gcd(\lambda, \mu) = 1$ implying that if n is composite, the previous key sizes could be doubled asymptotically to guarantee the same security level of the discrete logarithm problem. Since, most pairing friendly elliptic curves have composite embedding degree, one needs to be careful for the choice of elliptic curves, and to change their sizes according to these new attacks. Using a more conservative but less efficient elliptic curves of embedding degree one would also be an alternative to implement pairing-based protocols. For the choice and right notion of types of pairings of embedding degree one, we refer to the recent article of Chattarjee *et al*. [8].

4.2 Other Attacks on Pairing Based Cryptography

There are two more attacks on pairing based cryptography as described under.

A. Minimal Embedding Field Attack

Hitt [18] observed that the minimal embedding degree $F_p^{ord\ Np}$ is not necessarily equal to the field F_q^k, i.e. the extension can be defined over F_q^k instead of over F_q. Hence, in this case the group G_n can be realized as a subgroup of much smaller field yielding to solve the DLP more efficiently in G_1, G_2 and G_n. It is remarkable that this attack is only applicable for pairing-friendly curves defined over non-prime fields.

B. Subgroup Attack

Usually pairing functions are realized in such a way that two out of three groups G_1, G_2 and G_n are proper subgroups of larger composite order subgroups. This results in the so-called subgroup attacks if especially the underlying pairing implementation is not testing the group membership of the elements. Barreto *et al* [5]. introduced the notion of subgroup security and pointed out that most implementations of bilinear maps do not satisfy this notion [5]. They suggested new curve parameters using the known families of pairing-friendly elliptic curves achieving the subgroup security.

5. Conclusion

Pairings are being used to design elegant solutions to protocol problems, some of which have been open for many years. Many techniques [11] have been developed for generating suitable elliptic curves for a comprehensive survey. The fastest algorithms for computing the Tate pairing and its variants on these curves have fast implementations on software and hardware platforms, and are competitive with the exponentiation algorithms that are used in traditional discrete logarithm cryptography. Two areas that deserve further investigation are the practicality of implementing various pairing-based protocols at high security levels and the hardness of the BDHP and related problems. Researchers are also actively investigating the suitability of hyper-elliptic curves and other abelian varieties [6, 12, 13, 28].

6. References

1. Abe M, Groth J, Ohkubo Mk, Tango TT. Converting cryptographic schemes from symmetric to asymmetric bilinear groups, In Advances in Cryptology CRYPTO, volume 8616 of Lecture Notes in Computer Science, Springer Berlin Heidelberg. 2014, 241-260.
2. Adj G, Menezes A, Oliveira T, Rodriguez-Henriquez F. Computing discrete logarithms in $F_{3^{6.137}}$ using magma, IACR Cryptology e-Print Archive. 2014, 57.
3. Akinyele JA, Garman C, Hohenberger S. Automating fast and secure translations from type-I to type-III pairing schemes, In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, CCS '15. 2015; 1370-1381.
4. Barbulescu R, Gaudry P, Joux A, Thome E. Advances in Cryptology-EU ROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, Proceedings, chapter A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic, pages 1-16, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.
5. Barreto P, Costello C, Misoczki R, Naehrig M, Pereira G, Zanon G. Subgroup security in pairing-based cryptography, In Progress in Cryptology - LATIN- CRYPT of Lecture Notes in Computer Science, pages, Springer International Publishing. 2015, 245-265.
6. Barreto P, Galbraith S, ´O h´Eigeartaigh C, Scott M. Efficient pairing computation on super-singular abelian varieties, Designs, Codes and Cryptography. 2007; 42:239-271.
7. Blake I, Seroussi G, Smart N. Advances in Elliptic Curve Cryptography (London Mathematical Society Lecture Note Series), Cambridge University Press, New York, NY, USA, 2005.
8. Chatterjee S, Menezes A, Rodriguez-Henriquez F. On instantiating pairing-based protocols with elliptic curves of embedding degree one, 2016. http:// eprint.iacr.org/2016/403.
9. Chen J, Lim HW, Ling S, Wang H, Wee H. Pairing-Based Cryptography- Pairing 2012: 5th International Conference, Cologne, Germany, Revised Selected Papers, chapter Shorter IBE and Signatures via Asymmetric Pairings, pages, Springer Berlin Heidelberg, Berlin, Heidelberg. 2012-2013, 122-140.
10. Costello C. Pairings for beginners, http://www.craigcostello.com.au/pairings/PairingsForBeginners.pdf.
11. Freeman D, Scott M, Teske E. A taxonomy of pairing-friendly elliptic curves, Journal of Cryptology. 2010; 23(2):224-280.
12. Galbraith S, Hess F, Vercauteren F. Hyper-elliptic pairings, Pairing-Based Cryptography, Pairing 2007,

Lecture Notes in Computer Science. 2007; 4575:108-131.
13. Galbraith S, McKee J, Valenca P. Ordinary abelian varieties having small embedding degree, Finite Fields and Their Applications. 2007; 13:800-814.
14. Galbraith SD, Paterson KG, Smart NP. Pairings for cryptographers, Discrete Appl. Math. 2008; 156(16):3113-3121.
15. Gologlu F, Granger R, McGuire G, Zumbragel J. On the Function Field Sieve and the Impact of Higher Splitting Probabilities, Springer Berlin Heidelberg, Berlin, Heidelberg. 2013, 109-128.
16. Granger R, Kleinjung T, Zumbragel J. Breaking 128-bit Secure' Super-singular Binary Curves, Springer Berlin Heidelberg, Berlin, Heidelberg. 2014, 126-145.
17. Granger R, Kleinjung T, Zumbragel J. On the discrete logarithm problem in finite fields of fixed characteristic, 2015. http://arxiv.org/abs/1507.01495.
18. Hitt L. Pairing-Based Cryptography-Pairing: First International Conference, Tokyo, Japan, Proceedings, chapter On the Minimal Embedding Field, Springer Berlin Heidelberg, 2007, 294-301.
19. Jeong J, Kim T. Extended tower number field sieve with application to finite fields of arbitrary composite extension degree, IACR Cryptology e-Print Archive. 2016; 526:1-21.
20. Joux A, Pierrot C. Technical history of discrete logarithms in small characteristic finite fields, Designs, Codes and Cryptography. 2016; 78(1):73-85.
21. Kim T, Barbulescu R. Advances in Cryptology-CRYPTO 2016: 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, Proceedings, chapter Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case, Springer Berlin Heidelberg, Berlin, Heidelberg, 2012, 2016.
22. Koblitz N. Elliptic Curve Cryptosystem, Journal of Mathematics Computation. 1987; 48(177):203-209.
23. Massierer M. Some experiments investigating a possible L (1/4) algorithm for the discrete logarithm problem in algebraic curves. IACR Cryptology e-Print Archive. 2014; 996:1-16.
24. Menzes A. An introduction to Pairing based cryptography. https://www.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf.
25. Miller VS. Use of elliptic curves in cryptography, Advances in Cryptology-CRYPTO, 85 (LNCS 218). 1985, 417-426.
26. Odlyzko AM. Advances in Cryptology: Proceedings of EUROCRYPT 84 A Workshop on the Theory and Application of Cryptographic Techniques Paris, France, chapter Discrete logarithms in finite fields and their cryptographic significance, pages 224-314, Springer Berlin Heidelberg, Berlin, Heidelberg, 1984, 1985.
27. Ramanna SC, Chatterjee S, Sarkar P. Public Key Cryptography-PKC International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012, Proceedings, chapter Variants of Waters' Dual System Primitives Using Asymmetric Pairings, Springer Berlin Heidelberg, Berlin, Heidelberg. 2012, 298-315.
28. Rubin K, Silverberg A. Super-singular abelian varieties in cryptology, Advances in Cryptology-CRYPTO 2002, Lecture Notes in Computer Science. 2002; 2442:336-353.
29. Sarkar P, Singh S. A General Polynomial Selection Method and New Asymptotic Complexities for the Tower Number Field Sieve Algorithm, Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.
30. Shacham H. New Paradigms in Signature Schemes, Ph. D. thesis, Stanford University, 2005.
31. Waters B. Advances in Cryptology-CRYPTO: Annual International Cryptology Conference, Santa Barbara, CA, USA, Proceedings, chapter Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions, Springer Berlin Heidelberg. 2009, 619-636.