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. 194-200

A survey on pairing based schemes in elliptic curve cryptography

Manoj Kumar

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

Abstract
Recent years have been brought a host of cryptographic schemes that make use of pairings. 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. It has also recently become extremely useful in cryptologic constructions related to these objects. The present paper consists of brief survey on pairing based schemes in cryptography. The survey reviews the pairings mathematically and it includes the topics namely pairing-friendly elliptic curves. It also includes a brief introduction to existing identity-based encryption (IBE) schemes and other cryptographic schemes using pairing technology.

Keywords: RSA scheme, elliptic curve cryptography, bilinear paring maps, identity-based encryption, torsion points, finite fields

1. Introduction
In the recent years, pairing based cryptographic schemes on elliptic curve have been a very active field of research in cryptography. The concept of pairing in cryptography was first introduced by Weil [27]. Generally pairings map pairs of points on an elliptic curve into the multiplicative group of a finite field. The use of pairings in cryptography has developed at an extraordinary pace since the publication of the paper of Joux [11]. Joux's paper is of great interest to cryptographers, who want to start investigating further applications of pairings. The next two important applications of pairings are the identity-based encryption scheme of Boneh and Franklin [3] and the short signature scheme of Boneh, Lynn and Shacham [4]. Since then, there has been a flurry of activity in the design and analysis of cryptographic protocols using pairings. Pairings have been accepted as an indispensable tool for the protocol designer. There has also been a tremendous amount of work on the realization and efficient implementation of bilinear pairings using the Tate pairing on elliptic curves, hyperelliptic curves, and more general kinds of abelian varieties [10, 12, 13, 15, 16, 24, 25, 26]. In the world of elliptic curve cryptography, the pairing was initially considered as negative property. This is because it reduces the discrete logarithm problem on some elliptic curves (e.g. super singular curves) to the discrete logarithm problem in a finite field, thus diminishing the strength and practicability of super singular curves in cryptography. Until a tripartite key agreement protocol proposed by Joux in ANTS 2000 [11], the pairing for the first time became beneficial and favorable to cryptographic research and applications. Later Boneh and Franklin [3] proposed an identity based encryption scheme based on the modified weil-pairing and gave thorough analysis about its properties, security and performance. In next two sections we shall discuss a brief mathematical background of elliptic curve cryptography and pairings. A detail study can be found in [9, 26].

2. Elliptic Curve Cryptography
The use of elliptic curve cryptography was initially suggested by Koblitz [12] and Miller [16]. 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

$$y^2 = x^3 + ax + b \tag{1}$$

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:

1. If $P(x,y)$ is a point on an elliptic curve E then inverse (reciprocal or opposite) point of P is $-P(x,-y)$.
2. 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 $\lambda=(y_1-y_2)/(x_1-x_2)$.
3. 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 $\lambda=(3x_1^2+a)/2y_1$.

Following figure-1(a) and Figure-1(b) show the addition of two distinct points and doubling of a point on an elliptic curve.

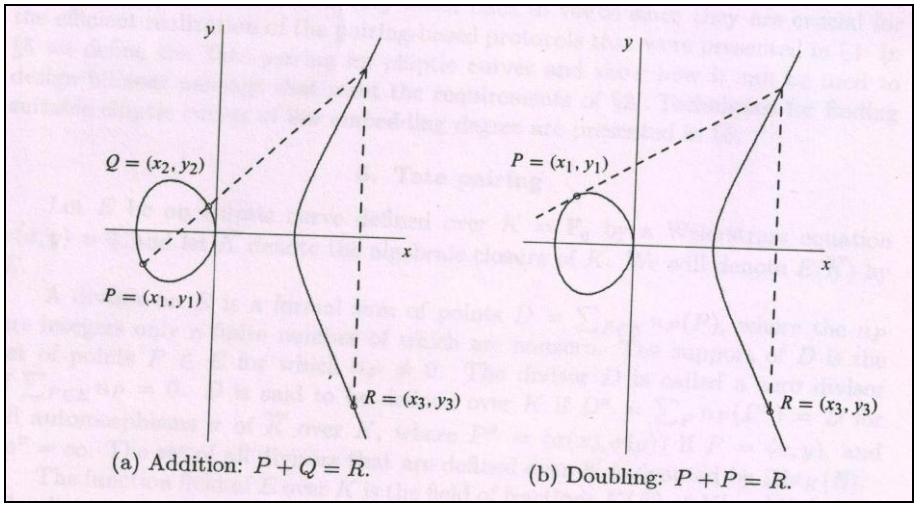

Fig 1: Addition and doubling of points on an elliptic curve

3. Mathematical background of pairings

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 $P_1, P_2\in E[n]$.

3.1 Pairing on Elliptic Curves

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 nth 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

$$e_n: G_1\times G_2\to G_n \tag{2}$$

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 [6]. 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.

3.2 Pairing Types

Galbraith *et al*. [8] 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*. [8] originally presented three types of pairings but a fourth type was added soon after by Shacham [22]. There are now four types of pairings in literature (chapter 4, pp. 58-59 of [5]) discussed as under:

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.

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.

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.

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. Selection of elliptic curves for pairings

In this section we discuss some well known methods for generating elliptic curves that are suitable for implementing pairing-based cryptographic protocols. The elliptic curves which are suitable for pairing based cryptography are known as pairing friendly curves. The first example of pairing friendly curve is super-singular curve. Following are the conditions for an elliptic curve to be pairing friendly:

1. n should divide $card\ E(F_q)$ and $n \geq \sqrt{q}$ for discrete logarithm problem to be hard.
2. For the least value of embedding degree k, we must have $k \leq \frac{\log n}{8}$.

If E is an elliptic curve defined over a finite field F_q, n is a natural number such that $\gcd(n,q)=1$ and k is a least natural number such that n divides (q^k-1) then the parameters n, q and k must satisfy the following conditions:

1. k must be sufficiently large so that the index-calculus methods for solving the discrete logarithm problem in F_{q^k} are infeasible.
2. k must be sufficiently small so that the arithmetic in F_{q^k} can be performed efficiently.
3. n must be sufficiently large so that Pollard's rho method for computing discrete logarithms in an order-n subgroup of $E(F_q)$ is infeasible.

If we assume $\rho = \frac{\log q}{\log n}$, then for efficient arithmetic it is required to have ρ as least as possible. It is also desired the least value of k for faster computation of pairing. To maintain the equivalent levels of security, we must have the constant value of ρk. Many cryptographers recommend choosing $\rho \approx 1$ but for some protocols $\rho \approx 2$ is also recommended. Following table-1 shows the selection of parameters on the elliptic curves for the different levels of security.

Table 1: Recommended Security levels for Pairing Groups

Security Levels(bits)	n **(bits)**	q^k	k **with** $\rho \approx 1$
80	160	960-1280	6-8
128	256	3000-5000	12-20
192	384	7000-9000	18-24
256	512	14000-18000	28-36

Some other conditions may be imposed on the elliptic curve parameters in order to accelerate the computation of the pairing, for example, one might require that n have low Hamming weight so that most of the doubling operations in Miller's algorithm are eliminated. As discussed earlier one can expect that $k \approx n$ for a randomly selected elliptic curve. Thus one cannot expect to generate suitable elliptic curves by random selection. Two classes of supersingular curves that are suitable for pairing applications are discussed in the next two subsections.

4.1 Super-singular Elliptic Curves

It is observed that for super-singular elliptic curves, the values of embedding degree k are in the set $\{1,2,3,4,5,6\}$. If E is defined over a prime field F_q with $q>3$, then we have $k=1$ or $k=2$. All super-singular elliptic curves with $k=4$ are defined over characteristic two finite fields, while those with $k=6$ are defined over characteristic three finite fields. The following result is helpful to determine the orders of group.

Proposition 4.1([24]): Let E be an elliptic curve defined over F_q, and let $t = q+1-card\ E(F_q)$. Also let α, β be the complex roots of $T^2 - tT + q \in Z[T]$. Then we have $card\ E(F_q) = q^m + 1 - \alpha^m - \beta^m$ for all $m \geq 1$.

4.2 Ordinary Elliptic Curves

In this section we discussed some well known techniques for generating ordinary elliptic curves for pairing based cryptography.

a. **Complex Multiplication method ([1, 19]):** Let q be a prime number and let t be a non-zero integer satisfying $|t| < 2\sqrt{q}$. Then complex multiplication norm equation is given by
$t^2 - 4q = -DV^2$
where D is the discriminant and square free if t is odd, and $D = 4d$ with d positive and square free if t is even.
The complex multiplication method is an algorithm for finding an elliptic curve E over F_q with $card\ E(F_q) = q+1-t$. The running time of complex multiplication method is exponential in $\log q$; however it is efficient in application if D is comparatively small i.e. $D < 10^9$. All known techniques for generating ordinary elliptic curves with low embedding degree use the complex multiplication method.

b. **MNT method ([18]):** Miyaji *et al.* [18] were the first to describe a method for constructing ordinary elliptic curves of low embedding degree. Their method is relying on the following result.

Proposition 4.2([18]): Let $q > 64$ be a prime number and let E be an ordinary elliptic curve defined over F_q such that $n = card\ E(F_q)$ is prime. Also let k be the embedding degree of $E(F_q)$ and $t = q+1-card\ E(F_q)$. Then we have the following results:

a) $k = 3$ if and only if $q = 12s^2 - 1$ and $t = -1 \pm 6s$ for some $s \in Z$.
b) $k = 4$ if and only if $q = s^2 + s + 1$ and $t \in (-s, s+1)$ for some $s \in Z$.
c) $k = 6$ if and only if $q = 4s^2 + 1$ and $t = 1 \pm 2s$ for some $s \in Z$.

c. **Cocks-Pinch method ([7]):** Cocks and Pinch introduced a new method for constructing elliptic curves for any embedding degree. Their method is based on the following result.

Proposition 4.3 ([7]): For a natural number k and a prime $n \equiv 1 (\bmod k)$, let $D > 0$ be a square free integer such that $D \equiv 3 (\bmod 4)$ and $-D$ is a square modulo n. Also for $t = 2a + 1$ and $a = 2^{-1} g \bmod n$, let g be a primitive k^{th} root of unity modulo n and $j \geq 0$ be an integer such that $q = \left(t^2 + D(V_0 + jn)^2\right)/4$ is a prime, where $V_0 = \pm(t-2)/\sqrt{-D} \bmod n$. Then there exists an elliptic curve E defined over F_q satisfying the following conditions:

1. n divides $card\ E(F_q)$.
2. the norm equation is $t^2 - 4q = -D(V_0 + jn)^2$ and
3. the order-n subgroup of $E(F_q)$ has embedding degree k.

5. Identity based encryption

Identity based encryption (IBE) is similar to classical public key cryptography in that each user has a public key for encryption anda private key for decryption. However, unlike classical public key encryption, where the public key is generated from the private key, IBE allows public keys to be set to the value of a pre-existing identifier, such as an email

address. Another difference is that for IBE the individual users cannot generate their own private keys, but must instead download them from a trusted third party known as the private key generator (PKG). Furthermore, in order to encrypt messages, the sender must obtain public system parameters from the PKG. These system parameters are used in combination with the intended recipient's identity string to generate an encrypted message. While the concept of IBE was first proposed by Shamir [23] in 1985, he was only able to provide a method for a conceptually similar, but not nearly as useful, identity-based signature scheme. It was not until 20 years later that a practical scheme for IBE was actually published. The tool that made the Boneh- Franklin [3] scheme possible was bilinear pairings. Another important IBE scheme is the Boneh-Boyen [2] scheme. The primary advantages are that the Boneh-Boyen scheme does not require the random oracle assumption in its security proof, and that the sender does not have to perform a bilinear pairing operation in order to encrypt a message. This reduced computation for the sender comes at the cost an extra pairing operation for the recipient, although the recipient can use a mathematical trick to compute the key (which is the ratio of the results of two different pairing operations) more efficiently than he or she could by computing the two pairing operations separately. Since this scheme is somewhat more complicated and non-intuitive than the Boneh-Franklin scheme, it will not be described here, even in simplified form. It works on similar principles, and aside from the random oracle assumption, makes similar security assumptions to the Boneh-Franklin scheme.

A third important IBE scheme is the Sakai *et al*. [21] scheme. This scheme has been proven secure in the random-oracle model and has better performance overall than either the Boneh-Franklin or the Boneh-Boyen schemes. It does not require a pairing operation for encryption, and only requires a single pairing computation for decryption.

A general advantage of IBE is that it simplifies key management procedures of certificate-based public key infrastructures. IBE also offers interesting features arising from the possibility of encoding additional information into a user's identity. IBE may be seen as an advantage or as a drawback, depending on the situation. There are two main drawbacks to IBE. First, the PKG has a master secret key, which if compromised would allow an attacker to decipher any message from any user. Second, the security of IBE relies on problems that have not been studied as extensively as the problems that underlie more traditional cryptosystems.

6. Conclusion

As we have seen, pairing-based cryptography has much to offer. Pairing-based schemes, such as IBE, provide special properties which cannot be provided through traditional PKI in a straightforward way. These schemes have received sufficient attention from the cryptographic community and no weakness has been identified. While pairing-based cryptography is still an emerging technology, with active research and development, it is being used in large and small scale applications. Bilinear pairings are also being considered for alternative implementations of available functionalities. These include various authentication schemes, privacy-preserving auctions, privacy-friendly aggregation for the smart grid, network communication resilient to traffic analysis, anonymous credentials, and many more.

References

1. Atkin A, Morain F. Elliptic curves and primality proving, Mathematics of Computation. 1993; 61:29-68.
2. Boneh D, Boyen X. Secure Identity-based Encryption without Random Oracles, in: Advances in Cryptology-Crypto 2004, Lect. Notes in Comput. Sci. 3152, Springer-Verlag. 2004, 443-459.
3. Boneh D, Franklin M. Identity-based encryption from the Weil pairing, Advances in Cryptology-CRYPTO 2001, Lecture Notes in Computer Science, 2139, 213-229. Full version: SIAM Journal on Computing. 2001-2003; 32:586-615.
4. Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing, Advances in Cryptology-ASIACRYPT 2001, Lecture Notes in Computer Science, 2248, (2001)514-532. Full version: Journal of Cryptology. 2004; 17:297-319.
5. Costello C., Pairings for beginners, http://www.craigcostello.com.au/pairings/PairingsForBeginners.pdf.
6. Freeman D, Scott M, Teske E. A Taxonomy of Pairing-Friendly Elliptic Curves, J. Cryptology. 2010; 23(2):224-280.
7. Galbraith SD. Pairings, Chapter IX of book Advances in elliptic curve cryptography edited by I. Blake, G. Seroussi and N. Smart, Cambridge University Press. 2005.
8. Galbraith SD, Paterson KG, Smart NP. Pairings for cryptographers, Discrete Applied Mathematics. 2008; 156(16):3113-3121.
9. Hankerson D, Menzes A, Vanstone S. Guide to Elliptic Curve Cryptography, Springer, New York. 2004.
10. Hardy GH, Wright EM. An introduction to the theory of numbers, oxford university press, United Kingdom. 1938.
11. Joux A. A one round protocol for tripartite Diffie-Hellman, Algorithmic Number Theory: 4th International Symposium, ANTS-IV, Lecture Notes in Computer Science, 2000; 1838: 385-393. Full version: Journal of Cryptology. 2004; 17:263-276.
12. Koblitz N. Elliptic Curve Cryptosystem, Journal of Mathematics Computation. 1987; 48(177):203-209.
13. Kumar M, Gupta P, Kumar A. A Novel and Secure Multi-party Key Exchange Scheme Using Trilinear Pairing Map Based on Elliptic Curve Cryptography, International Journal of Pure and Applied Mathematics. 2017, 116(1).
14. Massoud HD, Reza A. Zero-Knowledge Identification Scheme Based on Weil Pairing. ISSN 1995-0802, Lobachevskii Journal of Mathematics. 2007; 30(3):203-207.
15. Menzes A. An introduction to Pairing based cryptography, https://www.math.uwaterloo.ca/~ajmeneze/publications/pairings.pdf.

16. Miller VS. Use of elliptic curves in cryptography, Advances in Cryptology-CRYPTO, 85 (LNCS 218). 1985, 417-426.
17. Miller VS. The weil pairing and its efficient calculation, J. Cryptography. 2004; 17:235-261.
18. Miyaji A, Nakabayashi M, Takano S. New explicit conditions of elliptic curve traces for FR-reduction, EICE-Transactions on Fundamentals of Electronics, Communications and Computer Sciences. 2001; E84:1234-1243.
19. Morain F. Building cyclic elliptic curves modulo large primes, Advances in Cryptology, EUROCRYPT' 91, Lecture Notes in Computer Science. 1991; 547:328-336.
20. Paterson KG. ID based signature from pairings on elliptic curves, Electron Lett. 2002; 38(18):1025-1026.
21. Sakai R, Ohgishi K, Kasahara M. Cryptosystems based on pairing over elliptic curve, In Proceedings of the 2000 Symposium on Cryptography and Information Security, Okinawa, Japan. 2000.
22. Shacham H. New Paradigms in Signature Schemes, PhD thesis, Stanford University. 2005.
23. Shamir A. Identity-based cryptosystems and signature schemes, In Advances in Cryptology-CRYPTO 84, Lect. Notes in Comput. Sci. 196, Springer-Verlag. 1985, 47-53.
24. Silverman J. The Arithmetic of Elliptic Curves, Springer- Verlag, New York. 1986.
25. Stinson DR. Cryptography theory and practice, Chapman and Hall/CRC, United Kingdom. 2006.
26. Washington LC. Elliptic curves number theory and cryptography, Chapman and Hall/CRC, United Kingdom. 2008.
27. Weil A. André Sur les fonctions algébriques à corps de constantes fini. (French) C. R. Acad. Sci. Paris. 1940; 210:592-594.
28. Zhang F, Kim K. ID based blind signature and ring signature from pairings, In Advances in Cryptology-ASIACRYPT, springer-verlag. 2002, 533-547.