Pairing-Based Cryptography : A Survey

Sedat AKLEYLEK, Barış Bülent KIRLAR, Ömer SEVER, Zaliha YÜCE

***Abstract*—Pairings, bilinear maps, help to transform a discrete logarithm problem on an elliptic curve to the discrete logarithm problem in finite fields. They started to be used in cryptography during 1990's. At the beginning, they are used to build as attacks on elliptic curve digital signature algorithm. Nowadays, pairings are popular to construct cryptographic protocols. The purpose of this paper is to introduce bilinear pairings in cryptography and to show how to construct protocols in pairing-based cryptography.**

***Keywords* —bilinear map, pairing-based cryptographic protocols, Weil and Tate pairing.**

I. Introduction

Over the last years, there has been an increasing interest in pairing-based cryptography. The primitives of pairing based cryptosystems are three groups in which the discrete logarithm problem (DLP) is believed to be hard. Moreover, one requires the existence of an efficiently computable, so-called non-degenerate pairing map. This additional structure allows many interesting protocols for all kind of different applications [6], [8], [12]. Pairings in elliptic curve cryptography are functions which map a pair of elliptic curve points to an element of the multiplicative group of a finite field.

Earlier bilinear pairings, namely Weil pairing and Tate pairing were used in cryptography for the Menezes-Okamoto-Vanstone (MOV) [13] and Frey-Rueck (FR) [10] attacks, respectively. MOV and FR attack reduces elliptic curve discrete logarithm problem (ECDLP) to DLP in a finite field. They use bilinearity of the pairings. The basic idea of MOV and FR attack is to find an isomorphism between $r-$torsion point and r-th roots of unity of $\mathbb{F}_{q^k}$, where k is the embedding degree of r-torsion points. When k is small enough, i.e., $k \leq (logq)^2$, there is a sub-exponential time algorithm such as index calculus and function field sieve algorithms that can be used to solve DLP on a finite field. For supersingular curves, ECDLP is easy to solve since MOV or FR attack is applicable.

Most of the protocol researchers use the fascinating properties of the bilinear pairings to design new cryptographic protocols. They just focus on the efficiency of the pairing but skip the details of pairings. On the other side, the security of the protocol must be based on a hard problem which depends on the mathematical properties of the pairing. In this respect Galbraith, Paterson and Smart [11] give a good guidance to non-specialists who are interested in using pairings to design cryptographic schemes focusing on efficiency, bandwidth and security.

Pairing-based protocols primarily achieve two main objective; to construct methods which can not be constructed using other techniques (ID-based encryption, etc) and methods which can be done using other techniques, but for which pairings provide improved functionality (short signature, tri partite key exchange in one round, etc).

For pairing-based cryptography, it is a general problem of choosing elliptic curves together with bilinear mappings. To find a suitable elliptic curve one needs with a prime $r \geq \sqrt{q}$ dividing $\#E(\mathbb{F}_q)$ and the embedding degree of E, k, small enough so that arithmetic on $\mathbb{F}_{q^k}$ is feasible and large enough that DLP on $\mathbb{F}_{q^k}^*$ is as hard as the ECDLP on $E(\mathbb{F}_q)[r]$.

In this paper, a survey on pairing-based cryptography is given. Section II briefly explains the cryptographic bilinear map, Bilinear Diffie-Hellman Problem and describes the pairing-based cryptographic protocols. The Weil and Tate pairings, the basic elements in protocols, are discussed with their use in Section III. The suitable elliptic curves with the given embedding degree for pairing-based cryptography are explained in Section IV. Finally, we conclude in Section V.

II. Pairing-Based Cryptography

A. Bilinear Pairings

Definition 1. *Let $(G_1, +)$ and $(G_2, +)$ be abelian groups of order n. Let $(G_3, .)$ be a cyclic group of order n. A bilinear pairing is an efficiently computable map $e : G_1 \times G_2 \longrightarrow G_3$ which satisfies the following additional properties:*

1) *(bilinearity) For all $P, R \in G_1$ and all $Q, S \in G_2$, we have $e(P+R, Q) = e(P, Q)e(R, Q)$ and $e(P, Q+S) = e(P, Q)e(P, S)$.*
2) *(non-degeneracy) For all $P \in G_1$, with $P \neq Id_{G_1}$, there is some $Q \in G_2$ such that $e(P, Q) \neq 1$. For all $Q \in G_2$, with $Q \neq Id_{G_2}$, there is some $P \in G_1$ such that $e(P, Q) \neq 1$. When $G_1 = G_2$ and n is prime, $e(P, P)$ is a generator of G_3 for all $P \neq Id_{G_1}$*

Weil and Tate pairings on elliptic curves over finite fields can be given as an example of pairings. For the use in cryptography it is assumed that DLP on G_1, G_2 and G_3 are hard to solve. This bilinear property has many applications and it was first used for DLP in [13]. For instance, choosing $G_1 = G_2 = E(\mathbb{F}_q)$ and $G_3 \subset \mathbb{F}_{q^k}^*$ with k an embedding degree, defines bilinear pairing.

The following lemma which is related to the properties of bilinear pairings can be easily verified.

Lemma 2. *Let $e : G_1 \times G_2 \longrightarrow G_3$ be a bilinear pairing. Let $P \in G_1$ and $Q \in G_2$. Then*

Manuscript received November 10, 2008.

S. Akleylek, B. B. Kırlar, Ö. Sever, Z. Yüce are with the Institute of Applied Mathematics, METU, Ankara, Turkey, e-mail: {akleylek,kirlar}@metu.edu.tr, severomer@yahoo.com, zyuce@stm.com.tr

S. Akleylek is also with the Department of Computer Engineering, On-Dokuz Mayıs University, Samsun, Turkey

B. B. Kırlar is also with the Department of Mathematics, Süleyman Demirel University, Isparta, Turkey

Z. Yüce is a software engineer in STM A.Ş.

* This research is partially supported by ASELSAN A.Ş.

1) $e(P,0) = e(0,Q) = 1$
2) $e(-P,Q) = e(P,-Q) = e(P,Q)^{-1}$
3) $e(kP,Q) = e(P,kQ) = e(P,Q)^k$ *for all* $k \in \mathbb{Z}$.

We will now give the Bilinear Diffie Hellman Problem that has been widely studied in recent years.

B. The Bilinear Diffie-Hellman Problem (BDHP)

Security of the some of the applications of bilinear pairings in cryptography relies on the difficulty of bilinear Diffie-Hellman problem which was first stated in [7].

Definition 3. *Let G be a finite cyclic group of order n with a generator g, and let a, b, c be integers. The BDHP is to compute the value of the bilinear pairing $e(g^{abc}, g)$, whenever g^a, g^b and g^c are given.*

There is a close relation between BDHP and DHP which are defined on elliptic curve. The following fact is easy to prove.

Lemma 4. *BDHP is no harder than either the elliptic curve Diffie-Hellman problem or any finite field Diffie-Hellman problem.*

We presents three fundamental pairing-based protocols that the security of them depends upon the BDHP.

C. Pairing-Based Cryptographic Protocols

Protocols from pairings can be classified into two types :

1) Construction of primitives which can be constructed using other techniques, however by using pairings efficiency is gained.
2) Construction of primitives which cannot be constructed by using other cryptographic techniques.

Three party key agreement in one round and short signature protocols are the examples for the first class. Identity-Based encryption which eliminates the public key distribution is the example of the second class

1) Joux's One Round Three Party Key Agreement Protocol [12]: Key agreement, one of the fundamental cryptographic primitives, is required when two or more parties want to share a message securely.Three party key agreement in a single round proposed by Joux was the first application of bilinear pairings in cryptography.

Protocol:

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order n, $P \in G_1$, $G_1 =< P >$ and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map. Consider three parties A, B, C with secret keys $a, b, c \in Z_n$

- A broadcasts aP to both B, C
- B broadcasts bP to both A, C
- C broadcasts cP to both A, B
- A computes $e(bP, cP)^a$
- B computes $e(aP, cP)^b$
- C computes $e(aP, bP)^c$
- Common agreed key is $e(P,P)^{abc}$

2) Short Signatures [6]: Digital signatures are the most important cryptographic primitive for the daily life. Short signatures are needed in environments with space and bandwidth constraints. So far, the best known shortest signature is obtained by using the Digital Signature Algorithm (DSA) over a finite field $\mathbb{F}_q$. The length of the signature is approximately $2logq$. On the other hand, when the following pairing-based protocol is used the length of the signature is about $\rho logq$, where $\rho = logq/logr$ and r is the largest prime divisor of the number of the points in the elliptic curve. For example, if one uses RSA signature 1024 bit modulus, ECDSA signature is 320 bit long for the same security level. However, short signature provides the same security level only for 160 bits for the best choose. This case corresponds finding a suitable elliptic curve $E(\mathbb{F}_q)$, for which r is close to q and it is a general problem to find such suitable elliptic curves having this property [2].

Protocol:

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order n, $P \in G_1$, $G_1 =< P >$ and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map.

- **Public Key Generation :** Let $H : Z_2^\infty \rightarrow G_1$ be a map to point hash function. The secret key is $k \in \mathbb{Z}_n^*$ and public key is kP for a signer.
- **Sign :** Given a secret key k and a message $m \in \mathbb{Z}_2^\infty$, compute the signature $\sigma = kH(m) \in G_1$
- **Verify :** Given a public key kP, a message m and a signature σ, verify $e(P, \sigma) = e(kP, H(m))$.

3) Identity-Based (ID-B) Cryptosystems [7]: This was firstly suggested by [17] that a public key encryption scheme can be run with the identity of receiver. In other words, for ID-B encryption provides the simplification of certificate management in e-mail systems. By this way, management of keys and certificates gets more and more easier. The most used ID-B cryptosystem was proposed by [7] in 2001. The main advantage of ID-B crytosystems is to eliminate the need for certificates. Moreover, ID-B cryptosystems remove the certificate lookup, lifecycle management and certificate revocation lists.

Protocol:

Let $(G_1, +)$ and $(G_2, \cdot)$ be cyclic groups of prime order n, $P \in G_1$, $G_1 =< P >$ and $e : G_1 \times G_1 \rightarrow G_2$ be a bilinear map.

- **Public Key Generation :** Let $H_1 : \{0,1\}^* \rightarrow G_1^*$ and $H_2 : G_2 \rightarrow \{0,1\}^l$, where l is the length of the message m be the cryptographic hash functions. Let $s \in \mathbb{Z}_n^*$ and $S = sP$.
- **Encrypt :** Choose a random $r \in \mathbb{Z}_n^*$, then the ciphertext for the message $m : C = \langle rP, m \oplus H_2(e(H_1(ID), S)^r) \rangle$
- **Decrypt :** Compute $V \oplus H_2(e(sH_1(ID)), U)$ for given $C = \langle U, V \rangle$.

In practice, elliptic curves are the only groups used to implement pairings.

III. Weil and Tate Pairings

A. Elliptic Curves and Divisors

A cubic equation in Weierstrass form is given by the expression

$$y\ +a\ xy+a\ y=x\ +a\ x\ +a\ x+a\ , \qquad (1)$$

where the coefficients a_i are in the field $\mathbb{F}_q$. The projective non-singular curve defined by the affine equation (1) over the algebraic closure $\overline{\mathbb{F}_q}$ is called an elliptic curve over $\mathbb{F}_q$. This curve is denoted by E and it has an additive group structure determined by the fact that $P,Q,R \in E : P+Q+R =$ identity $\Leftrightarrow R$ lies in the line joining P to Q in the projective space. We denote the identity element of E by ∞, and it is well-known that the set of $\mathbb{F}_{q^k}$-rational points of E is a subgroup of E for any $k \geq 1$. This subgroup is denoted by $E(\mathbb{F}_{q^k})$. In fact, $E(\mathbb{F}_{q^k})$ consists of all solutions of (1) in $\mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$ together with ∞.

The divisor group of a curve E, denoted by $Div(E)$, is the free abelian group generated by the points of E. Therefore, a divisor $D \in Div(E)$ is a formal sum given by

$$D = \sum_{P \in E} n_P(P)$$

with $n_P \in \mathbb{Z}$ and $n_P = 0$ except for finitely many $P \in E$. The *degree* of a divisor D is defined by

$$deg(D) = \sum_{P \in E} n_P.$$

The *support* of a divisor D, $supp(D)$, is the set of points $P \in E$ for which $n_P \neq 0$.

The divisors of degree zero form a subgroup of $Div(E)$, that is denoted by

$$Div\ (E) = \{D \in Div(E) \mid deg(D) = 0\}.$$

Let $f \in \overline{\mathbb{F}_q^*} = \overline{\mathbb{F}_q} \backslash \{0\}$ be a rational function. Then, the divisor of a function f is $div(f) = \sum_{P \in E} ord_P(f)(P)$, where $ord_P(f)$ is the multiplicity of f at P. It is a well-known fact that $deg(div(f)) = 0$. A divisor D is called *principal* if $D = div(f)$ for some rational function $f \in \overline{\mathbb{F}_q^*}$. This is denoted by

$$Prin(E) = \{D \in Div(E) \mid D = div(f),\ f \in \overline{\mathbb{F}_q^*}\}.$$

$Prin(E)$ is a subgroup of $Div\ (E)$ since for all rational functions $f, g \in \overline{\mathbb{F}_q^*}$, $div(fg) = div(f) + div(g)$ and $div(f/g) = div(f) - div(g)$.

Theorem 5. *A divisor $D = \sum_{P \in E} n_P(P)$ is principal if and only if $deg(D) = 0$ and $\sum_{P \in E} n_P P = \infty$.*

The *divisor class group* (or *Picard group*) $Pic\ (E)$ of E is the quotient of the group of degree zero divisors $Div\ (E)$ by the principal divisors $Prin(E)$, i.e,

$$Pic\ (E) = Div\ (E)/Prin(E).$$

It is known that for every divisor $D \in Div\ (E)$, there is a unique point $Q \in E$ such that $D \sim (Q) - (\infty)$. This gives a one-to-one correspondence between $Pic\ (E)$ and the group of points of E.

Let $P, Q \in E$. Suppose the line between P and Q (tangent line if $P = Q$) has an equation $l(x,y) = 0$. By Bezout's theorem, this line l intersects E at a third point $R = (x_R, y_R)$. Then, the divisor of l is $div(l) = (P) + (Q) + (R) - 3(\infty)$. The vertical line $v(x) = (x - x_R)$ passes through the points R and $S = P+Q$. Then, $div(v) = (R)+(S)-2(\infty)$. Therefore, the equation $S = P + Q$ corresponds to the divisor equality $div(l/v) = (P) + (Q) - (S) - (\infty)$.

If $D = \sum_{P \in E} n_P(P) \in Div\ (E)$ and $f \in \overline{\mathbb{F}_q^*}$ is a rational function such that $supp(D) \cap supp(div(f)) = \emptyset$, then the value of f at D is defined to be the following equation:

$$f(D) = \prod_{P \in E} f(P)^{n_P}.$$

B. Weil and Tate Pairings [5]

Let E be an elliptic curve over $\mathbb{F}_q$ and E be the corresponding elliptic curve over the algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$. For a positive integer r, $E[r]$ denotes the group of r-torsion points of E, namely $E[r] = \{P \in E \mid rP = \infty\}$.

Definition 6. *The embedding degree of $E[r]$ is the smallest k such that $E[r] \subset E(\mathbb{F}_{q^k})$.*

Theorem 7. (Balasubramanian, Koblitz [2]) *Let E be an elliptic curve defined over $\mathbb{F}_q$ and suppose that E has a subgroup $< P >$ of order r with $gcd(r, q-1) = 1$. Then, $E[r] \subset E(\mathbb{F}_{q^k})$ if and only if $r \mid q^k - 1$.*

Let $P, Q \in E[r]$ and let $R, S \in E(\mathbb{F}_{q^k})$ such that $S \notin \{R, P+R, P+R-Q, R-Q\}$. Let $D = (P+R) - (R)$ and $D' = (Q+S) - (S)$. Then, by theorem (5) the divisors rD, rD' are in the form $rD = div(f)$ and $rD' = div(g)$ for some rational functions $f \neq 0, g \neq 0$. Let μ_r be the group of r-th roots of unity in $\mathbb{F}_{q^k}^*$.

Definition 8. *The bilinear map*

$$e_r : E[r] \times E[r] \rightarrow \mu_r \subset \mathbb{F}_{q^k}^*$$

defined by

$$e_r(P,Q) = (-1)^r \frac{f\ D'}{g\ D} = (-1)^r \frac{f\ Q\ \ S\ /f\ S}{g\ P\ \ R\ /g\ R}.$$

is called Weil pairing. This map is well-defined, i.e., $e_r(S,T)$ is independent of the choice of D, D', f and g for all $S, T \in E[r]$.

Theorem 9. (Properties of Weil Pairing) *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then, the Weil pairing e_r satisfies the following properties :*

1) *(identity) $e_r(S,S) = 1$ for all $S \in E[r]$*
2) *(alternation) $e_r(S,T) = e_r(T,S)^-$ for all $S, T \in E[r]$*
3) *(bilinearity) e_r is bilinear in each variable; $e_r(S+T, P) = e_r(S,P)e_r(T,P)$ and $e_r(S, T+P) = e_r(S,T)e_r(S,P)$ for all $S, T, P \in E[r]$*
4) *(non-degeneracy) If $e_r(S,T) = 1$ for all $S \in E[r] - \infty$, then $T = \infty$ and if $e_r(S,T) = 1$ for all $T \in E[r] - \infty$, then $S = \infty$*
5) *(compatibility) For all $S, T \in E[r]$, $e_r(\alpha(S), \alpha(T)) = e_r(S,T)^{deg\alpha}$, for any endomorphism $\alpha : E \rightarrow E$*

6) *If* $E[r] =< P > \oplus < R >$, *then* $e_r(P,R) = \xi$ *is a primitive* r*-th root of unity.*

The following algorithm developed by Miller computes $e_r(P,Q)$ in a polynomial time, efficiently. This algorithm for Weil pairing aims to construct rational functions f and g associated to the point P and Q and evaluate at divisors $D' = (Q+S) - (S)$ and $D = (P+R) - (R)$, respectively. The functions f and g can be efficiently computed by double and add procedure. This idea is to define functions f_i, g_i, where $1 \leq i \leq r$ and $f_r = f$, $g_r = g$, recursively. These functions are computed by the following way :

$$f_{} = \frac{v_P \ _R}{l_{P,R}},\ f_{i\ \ j} = f_i f_j \frac{l_{iP,jP}}{v_{iP\ \ jP}},\ f_{\ i} = f_i \frac{t_{iP}}{v_{\ iP}}$$

where v_P is the vertical line at P, t_R is the tangent line at R and $l_{P,Q}$ is the line passing through the points P and Q.

Let $P, Q \in E[r]$ and let $f \in \overline{\mathbb{F}_q^*}$ be a function with $div(f) = r(P) - r(\infty)$. Let $R \in E(\mathbb{F}_{q^k})$ such that $R \notin \{\infty, P, -Q, P-Q\}$, and let $D_Q = (Q+R) - (R)$. Let k be the embedding degree and let $E(\mathbb{F}_{q^k})[r] = E(\mathbb{F}_{q^k}) \cap E[r]$. Note that $supp(D_Q) \cap supp(div(f)) = \emptyset$ due to the choice of R.

Definition 10. *The bilinear map*

$$\langle \cdot, \cdot \rangle : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \rightarrow \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \rightarrow \mu_r$$

defined by

$$\langle P, Q \rangle = f_P(D_Q)^{\ q^k - \ \ /r} = (f_P(Q+R)/f_P(R))^{\ q^k - \ \ /r}$$

is called Tate pairing. This map is well-defined, i.e., $\langle \infty, Q \rangle = 1$ *for all* $Q \in E(\mathbb{F}_{q^k})$ *and* $\langle P, Q \rangle \in (\mathbb{F}_{q^k}^*)^r$ *for all* $P \in E(\mathbb{F}_{q^k})[r]$ *and all* $Q \in rE(\mathbb{F}_{q^k})$.

Theorem 11. (Properties of Tate Pairing) *Let* E *be an elliptic curve defined over* $\mathbb{F}_q$. *Let* $r > 0$ *and* $gcd(r, q-1) = 1$, *and let* k *be the embedding degree of* $E[r]$. *Then, the Tate pairing satisfies the following properties :*

1) *(bilinearity) For all* $P, P\ , P \in E(\mathbb{F}_{q^k})[r]$, *and* $Q, Q\ , Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$, $\langle P + P\ , Q \rangle = \langle P\ , Q \rangle \langle P\ , Q \rangle$ *and* $\langle P, Q\ + Q\ \rangle = \langle P, Q\ \rangle \langle P, Q\ \rangle$
2) *(non-degeneracy) For all* $P \in E(\mathbb{F}_{q^k})[r] - \infty$, *there is some* $Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ *such that* $\langle P, Q \rangle \neq 1$. *Similarly, for all* $Q \in E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ *with* $Q \notin rE(\mathbb{F}_{q^k})$ *there is some* $P \in E(\mathbb{F}_{q^k})[r]$ *such that* $\langle P, Q \rangle \neq 1$.

The Tate pairing $\langle P, Q \rangle$ is computed by a function $f_P = f_r$ at the divisor $D_Q = (Q+R) - (R)$ using double and add method in the following way:

$$f_{} = 1,\ f_{i\ \ } = f_i \frac{l_{iP,P}}{v_{\ i\ \ \ P}},\ f_{\ i} = f_i \frac{t_{iP}}{v_{\ iP}}$$

By raising $f_P(D_Q)$ to the power $(q^k - 1)/r$, one obtains an r-th roots of unity μ_r in $\mathbb{F}_{q^k}^*$.

The main differences between the Weil and Tate pairings are the symmetric property and exponentiation. The Weil pairing also requires more computation time than the Tate pairing.

IV. Curve Selection

This section describes the elliptic curves that are suitable for implementing pairing-based protocols. It is well-known that the number of points of the elliptic curve E over $\mathbb{F}_q$ is defined by $\#E(\mathbb{F}_q) = q+1-t$ and by Hasse's Theorem [18] that $|t| \leq 2\sqrt{q}$. if p divides t, E is said to be *supersingular* . Otherwise, it is called *ordinary*. The following theorem, where the proof can be found in [13] shows the classification of supersingular curves over any finite field for pairing-based cryptography.

Theorem 12. *Let* E *be a supersingular elliptic curve over* $\mathbb{F}_q$ *of order* $q+1-t$, *where* $q = p^m$. *Then, there are six families of supersingular curves with embedding degree* $k \leq 6$.

1) $k = 1$: $t^2 = 4q$ *and* m *is even*
2) $k = 2$: $t = 0$ *and* $E(\mathbb{F}_q) \cong Z_{q+1}$.
3) $k = 2$: $t = 0$ *and* $E(\mathbb{F}_q) \cong Z_{(q+1)/2} \oplus Z_2$ *and* $q = 3 \ (mod\ 4)$.
4) $k = 3$: $t^2 = q$ *and* m *is even.*
5) $k = 4$: $t^2 = 2q$ *and* $p = 2$ *and* m *is odd.*
6) $k = 6$: $t^2 = 3q$ *and* $p = 3$ *and* m *is odd.*

For supersingular curves, there is always so-called a distortion map, $\Psi : E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_{q^k})$, which is easily computable. This allows us to choose $G\ =< P >$, $G\ = \Psi(P)$ together with Weil/Tate pairing to produce a non-degenerate bilinear map $e : G\ \times G\ \rightarrow G\ $ such that $e(P,Q) = f(P, \Psi(Q))$. Distortion maps are all known for supersingular curves. Therefore, we have computable pairing associated to any supersingular curves.

Example 13.
If $q = 3 \pmod 4$ *and* $E : y\ = x\ + ax$ *for any* $a \in \mathbb{F}_q^*$, *then a distortion map is of the form* $\Psi : E(\mathbb{F}_q) \rightarrow E(\mathbb{F}_{q^2})$, $\Psi(x,y) = (-x, iy)$, *where* i *is a square root of -1.*

It is a research problem to find suitable non-supersingular (ordinary) curves for pairing-based cryptography [3], [19]. For this, one needs to find curves with large subgroups of size r for which embedding degree k of $E[r]$ is sufficiently small. It is known that the choice of these curves are very special due to the following theorem [2].

Theorem 14. *[2] Let* E *be a randomly chosen elliptic curve over* $\mathbb{F}_q$, *where* q *is prime and* $z/2 \geq q \geq z$. *Let* G *be a subgroup of order* r. *Then the probability that* $r|q^k - 1$ *for some* $k \geq (logq)\ $ *is less than* $c(logz)\ (loglogz)\ /z$ *for an efficiently computable constant* c.

New special techniques are needed to construct such pairing-friendly curves. The only known method so far is Complex Multiplication method to construct suitable ordinary elliptic curves for pairing-based cryptography. This method is used to construct curves with endomorphism ring isomorphic to a given order in a quadratic imaginary field $Q(\sqrt{-D})$ with specified number of points, where D is discriminant of the characteristic polynomial [1].

Some of the classification of pairing-friendly ordinary curves constructed by using the Complex Multiplication [16] are given as follows:

1) Miyaji, Nakabayashi, and Takano (MNT) [15] give a complete characterization of ordinary elliptic curves of prime order with embedding degree $k = 3, 4, 6$.

2) Freeman [9] gives a construction for curves of prime order with $k = 10$.
3) Barreto and Naehrig [4] give a construction for curves of prime order with $k = 12$.

We would like to note that there is a general construction, originally due to Cocks and Pinch [8], for curves of arbitrary embedding degree k, but in this construction $\rho = logq/logr \approx 2$ for arbitrary k, which leads to inefficient implementation. It should be noticed that ρ should be as close as one for an efficient pairing-based cryptographic protocols.

There is no distortion map on ordinary curves. One overcomes this difficulty by going into so-called its twist $E^{'}$ over $\mathbb{F}_q$. For an efficient computation as above, this can be done as follows : Let E be an elliptic curve given by the equation

$$E : y^2 = x^3 + a_4x + a_6$$

over $\mathbb{F}_q$, where $q = p^m$ and $p > 3$. Let v be a quadratic non-residue in $\mathbb{F}_q$. Then, the twist of the curve is defined by the equation

$$E^{'} : y^2 = x^3 + v^2a_4x + v^3a_6$$

over $\mathbb{F}_q$.

Even embedding degree $k = 2d$ for $E[r] \subset E(\mathbb{F}_q)$, we consider the twist $E^{'}(\mathbb{F}_{q^d})$ of $E(\mathbb{F}_{q^d})$. It is easy to show that the map $\Psi : E^{'}(\mathbb{F}_{q^d}) \rightarrow E(\mathbb{F}_{q^k})$ given by $\Psi(x, y) = (v^{-1}x, v^{-3/2}y)$ is well-defined and easily computable. As in the supersingular case we can use this map Ψ to produce computable bilinear map $e(P, Q^{'}) = f(P, \Psi(Q^{'}))$, where $Q^{'} \in E^{'}(\mathbb{F}_{q^d})$ of order a multiple of r and for the choice of Weil or Tate pairing. So, if we have a suitable ordinary elliptic curve for pairing-based cryptography, this method gives us a computable bilinear map e to used for these.

V. Conclusions

In this paper, we give an introduction to pairing-based cryptography. New cryptographic protocols and applications whose security is based on pairings are still growing very fastly. To implement these protocols new pairing methods based on Tate pairing are also being proposed.

Acknowledgment

We would like to thank Professor Ersan Akyıldız for his valuable comments.

References

[1] A. Atkin and F. Morain, "Elliptic Curves and Primality Proving", *Math. Comp. Vol. 61, no.203*, pp. 29-68, 1993.
[2] R. Balasubramanian and N. Koblitz, "The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm", Journal of Cryptology, 11(2), 141145, 1998.
[3] P. Duan, S. Cui and C. Chan, "Finding More Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems", *Proceedings of 2nd In- ternational Conference on Information Security (ICIS2005), Vol. 2*, pp.157-163, 2005.
[4] P.S.L.M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order" *in SAC 2005, ed. B. Preneel, S. Tavares, Springer LNCS 3897*, pp. 319-331, 2006.
[5] I.F. Blake, G. Seroussi and N.P. Smart, 'Advances in Elliptic Curve Cryptography", *London Mathematical Society Lecture Note Series. 317, Cambridge University*, 2005.
[6] D. Boneh, B. Lynn and H. Shacham, "Short Signature from the Weil Pairing", *Advances in Cryptology - ASIACRYPT01, LNCS 2248*, pp. 514-532, 2001.
[7] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", *Advances in cryptology CRYPTO01, LNCS 2139*, pp. 213229, 2001.
[8] C. Cocks and R.G.E. Pinch, "Identity-based cryptosystems based on the Weil pairing", *unpublished manuscript*, 2001.
[9] D. Freeman, "Constructing pairing-friendly elliptic curves with embedding degree 10", *In Algorithmic Number Theory Symposium ANTS-VII, volume 4076 of Lecture Notes in Computer Science, Springer*, pp. 452-465, 2006.
[10] G. Frey, M. Muller and H. Ruck, "The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems", *IEEE Transactions on Information Theory 45(5)*, pp. 1717-1719, 1999.
[11] S. Galbraith, K. Paterson and N. Smart, "Pairings for Cryptographers", avaliable at `http://eprint.iacr.org/2006/165.ps.gz`, 2006
[12] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman", *Proceedings of ANTS 4, LNCS 1838*, pp. 385-394, 2000.
[13] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *The Annual ACM Symposium on Theory of Computing (STOC)*, ACM Press, pp. 8089, 1991.
[14] V.S. Miller, "The Weil Pairing, and Its Efficient Calculation", *Journal of Cryptology*, 17, pp. 235-261, 2004.
[15] A. Miyaji, M. Nakabayashi and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction", *IEICE Transactions on Fundamentals E84- A(5)*, pp. 1234-1243, 2001.
[16] F. Morain, "Building cyclic elliptic curves modulo large primes", *in EUROCRYPT 91, ed. D. W. Davies, Springer LNCS 547*, 328-336, 1991.
[17] A. Shamir, "Identity based cryptosystems and signature schemes", *Advances in Cryptology CRYPTO 84, LNCS 196*, pp. 47-53, 1985.
[18] J.H. Silverman, "The Arithmetic of Elliptic Curves", *Springer-Verlag*, 1986.
[19] E. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems", *Journal of Cryptology*, 17, 277-296, 2004.