MATHEMATICS AND COMPUTATIONAL SCIENCES

Vol 2(2), 2021, pp:50-59

DOI:10.30511/mcs.2021.525072.1017

ISSN:2717-2708

http://mcs.qut.ac.ir/

Qom University of Technology

The review on elliptic curves as cryptographic pairing groups

Elaheh Khamseh [1]

Abstract: Elliptic curve is a set of two variable points on polynomials of degree 3 over a field acted by an addition operation that forms a group structure. The motivation of this study is that the mathematics behind that elliptic curve to the applicability within a cryptosystem. Nowadays, pairings bilinear maps on elliptic curves are popular to construct cryptographic protocol pairings to help to transform a discrete logarithm problem on an elliptic curve to the discrete logarithm problem in finite fields. The purpose of this paper is to introduce elliptic curve, bilinear pairings on elliptic curves as based on pairing cryptography. Also this investigation serves as a basis in guiding anyone interested to understand one of the applications group theory in cryptosystem.

Keywords: Elliptic curve; Bilinear map; Pairing-based cryptography
2020 Mathematics Subject Classification: 11Gxx, 11G05.
Receive: 13 February 2021, **Accepted:** 11 May 2021

1 Introduction

Cryptography is an evolving field that studies discrete mathematical equations which are representable by computer algorithms to provide message confidentiality. Modern mathematical cryptography involves many areas of mathematics, including especially number theory, abstract algebra (groups, rings, fields, etc.), probability and statistics. In this paper the researcher focuses on elliptic curves groups, that are used extensively as a based cryptography. Elliptic curve is a study of points on two-variable polynomials of degree 3 over a field. With a curve defined over a finite field, this set of points acted by an addition operation forms a finite group structure.

The discrete logarithm problem (DLP) has been studied since the discovery of public-key cryptography in 1975. Recall that DLP in an additively written group $G = \langle P \rangle$ of order n is the problem, given P and Q, of finding the integer $x \in [0, n-1]$ such that $Q = xP$. The DLP is believed to be intractable for certain (carefully chosen) groups including the multiplicative group of finite field, and the group of points on an elliptic curve defined over a finite field. The closely related Diffie-Hellman problem (DHP) is the problem, given P, aP and bP, of finding abP. It is easy to see that the DHP reduces in polynomial time to the DLP. It is generally assumed and has been proven in some cases (e.g. [4, 6]) that the DLP reduces in polynomial time to the DHP. The assumed intractability of DHP is the basis for the security of the Diffie-Hellman key agreement protocol [9]. The objective of this protocol is to allow Alice and Bob to

[1]Department of Mathematics, shahr-e-Qods Branch, Islamic Azad university, Tehran, Iran, elahehkhamseh@gmail.com

establish a shared secret by communicating over a channel that is being monitored by an eavasdropper Eve.

The group parameters n and P are public knowledge. Alice randomly selects a secret integer $a \in [1, n-1]$ and sends aP to Bob. Similarly Bob selects a secret integer $b \in [1, n-1]$ and sends bP to Alice. The eavesdropper is faced with the task of computing K given P, aP and bP, which is precisely an instance of the DHP. The Diffie-Hellman protocol can be viewed as a one-round protocol because the two exchange messages are independent of each other.The protocol can easily be extended to three parties, as illustrated by the two-round protocol depicted in the following that Joux[21] devised:

Let $(G_1, +)$ and $(G_2, .)$ be cyclic groups of prime order n, $G = \langle P \rangle$ and $\widehat{e} : G_1 \times G_1 \to G_2$ be a bilinear map, consider three parties A, B, C with secret keys $a, b, c \in \mathbb{Z}_n$.
. A broadcasts aP to both B, C
. B broadcasts bP to both A, C
. C broadcasts cP to both A, B
. A computes $\widehat{e}(bP, cP)^a$
. B computes $\widehat{e}(aP, cP)^b$
. C computes $\widehat{e}(aP, bP)^c$
. Common agreed key is $\widehat{e}(P, P)^{abc}$.

The protocol is secure against eavesdroppers if the problem of computing $\widehat{e}(P, P)^{abc}$ given P, aP,bP, cP and pairing $\widehat{e}$ is intractable. This problem is presumably no easier than DHP. Pairings have been accepted as an indispensable tool for the protocol designers. There has also been a tremendous amount of work on the realization and efficient implementation of bilinear pairings using elliptic curves[27]. 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.

The purpose of this paper is to provide an introduction to elliptic curve groups and pairing-based cryptography such as Tate and Weil pairing on elliptic curves. Elliptic curves are explained in section 2. In section 3 the researcher describes the bilinear map. In section 4 the researcher recalls how the Tate and Weil pairing on elliptic curves can be used to construct bilinear pairings. The suitable elliptic curves given for pairing-based cryptography are explained in section 5.

2 Elliptic Curves

An elliptic curve E over a field K is defined by a non-singular Weirestrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

where $a_1, a_2, a_3, ..., a_6 \in K$. The set $E(K)$ consists of the points $(x, y) \in K \times K$ that satisfy (2.1) and the point at infinity, which is denoted by ∞.

The chord-and-tangent rule for adding two points in $E(K)$ endows $E(K)$ with the structure of an abelian group. The point at infinity ∞ serves the identity element. The negative of a point $p = (x_1, y_1)$ is $-P = (x_1, y_2)$ where y_1, y_2 are the two roots of the defining equation for E with $x = x_1$. If $P, Q \in E(K) - \{\infty\}$ with $p \neq \pm Q$, then $P + Q$ is defined to be R where $-R$ is the third point of intersection of line through P and Q with the curve. If $P = Q$, then the tangent line through P that intersect curve is defined $-R$.

Figures 1 illustrate the group law for the elliptic curve over real numbers.

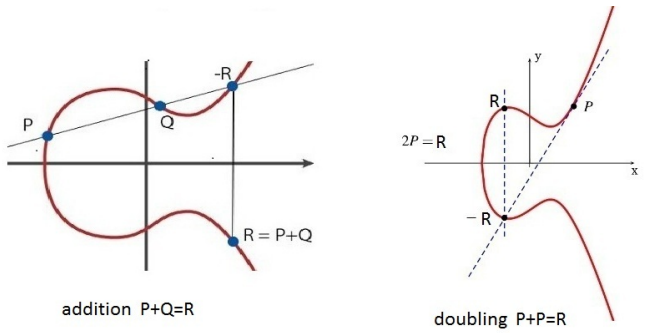

Figure 1:

In cryptography the researcher only ever instantiates elliptic curves, defined over finite fields. Suppose now that K is a finite field $\mathbb{F}_q$ of order q and characteristic p. Hasse's theorem [27] gives tight bounds for the cardinality of $E(\mathbb{F}_q)$:

$$(\sqrt{q}-1)^2 \leq |E(\mathbb{F}_q)| \leq (\sqrt{q}+1)^2.$$

Hence we can write $|E(\mathbb{F}_q)| = q+1-t$ where $|t| \leq 2\sqrt{q}$.

If $p|t$ then E is said to be supersingular; otherwise E is ordinary. There are some equivalent relations for this definition that you can see in [27].

If $p > 3$, then a linear change of variables transforms equation (2.1) into the simpler form:

$$y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$. We will always be working over large prime fields where the short Weierstrass equation covers all possible isomorphism classes of elliptic curves.

If E is supersingular and $p = 3$, then (2.1) simplifies to

$$y^2 = x^3 + ax + b$$

where $a, b \in \mathbb{F}_q$ and $b \neq 0$. If E is supersingular and $p = 2$, then (2.1) simplifies to

$$y^2 + cy = x^3 + ax + b$$

where $a, b, c \in \mathbb{F}_q$ and $c \neq 0$.

The rank of $E(\mathbb{F}_q)$, is at most two. More precisely, we have $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$ where $n_2|n_1$ and $n_2|q-1$.

Now let E be an elliptic curve over $\mathbb{F}_q$ and let P and Q be points in $E(\mathbb{F}_q)$. The elliptic curve discrete logarithm problem (ECDLP) is the problem of finding an integer n such that $Q = nP$. The best genetic algorithm known for solving the ECDLP is Pollard's rho method [25]. However, there may be other discrete log solvers that are faster for certain families of elliptic curves. In particular, it was shown in [15, 22] that Weil and Tate pairings can be used to transfer the ECDLP instance to an instance of the discrete logarithm problem in an extension field $\mathbb{F}_{q^k}$, where the embedding degree k is definied as follows:

Definition 2.1. *[27] Let E be an elliptic curve defined over $\mathbb{F}_q$, and $P \in E(\mathbb{F}_q)$ be a point of prime order r. Suppose that $gcd(r, q) = 1$. Then the embedding degree of $\langle P \rangle$ is the smallest positive integer k such that $r|q^k - 1$.*

Elliptic curves with small embedding degrees and large prime order subgroups are key ingredients for implementing pairing-based cryptographic systems, which are called pairing-friendly curves.

Definition 2.2. *[27] A curve is pairing friendly if the following two conditions holds:*
1) there is a prime $r \geq \sqrt{q}$ dividing $|E(\mathbb{F}_q)|$ (i.e. $\rho = \frac{logq}{logr} \approx 2$) and
2) the embedding degree k with respect to r less than $\frac{log_2(r)}{8}$

3 Pairing-based Cryptography

Let G_1, G_2 be a cyclic additive group generated by P_1, P_2 respectively, whose order is a prime p, and G_T be a cyclic multiplicative group of order p. A bilinear pairing is a map $\widehat{e} : G_1 \times G_2 \to G_T$ with the following properties:
1) bilinearity: $\widehat{e}(aP_1, bP_2) = \widehat{e}(P_1, P_2)^{ab}$ for all $a, b \in \mathbb{Z}_p^*$,
2) non-degeneracy: $\widehat{e}(P_1, P_2) \neq 1$,
3) computability: There is an efficient algorithm to compute $\widehat{e}(g_1, g_2)$ for all $g_1 \in G_1$, $P_2 \in G_2$

There are essentially types of bilinear maps [16, 26] used in the design of pairing-based protocols depending on the special requirements such as short representation, hashing to a group element, efficient homomorphism.
- Type-1: $G_1 = G_2$, in this case there exist no short representations for the elements of G_1.
- Type-2:$G_1 \neq G_2$ and there is an efficiently computable homomorphism $\psi : G_2 \to G_1$.
- Type-3: $G_1 \neq G_2$ and there exists no efficiently computable $\psi : G_2 \to G_1$.
- Type-4: $G_1 \neq G_2$ and there exists an efficiently computable homomorphism $\psi : G_2 \to G_1$ as in the case of Type-2 setting but with an efficient secure hashing method to a group element [26]. Security proofs can be quite cumbersome in this setting as discussed in [7]. We note that this Type is not generally used in protocol designs due to its inefficiency [28].

For instance, choosing $G_1 = E(\mathbb{F}_q)$, $G_2 = E(\mathbb{F}_{q^k})$ and $G_T \subset \mathbb{F}_{q^k}^*$ with k an embedding degree, defines bilinear pairings. In practice, elliptic curves are the only groups used to implement pairings. The Weil and Tate pairings for elliptic curves that can be used for design bilinear pairings, see [27], that are recalled in the next section. There are other pairings such as Ate pairing, Twisted ate pairing [20], and generalizations of Ate and Twisted Ate pairing, Optimal pairing have been given in [18, 29]. The implementation of the various pairings for different curves analysed in [12], in order to give recommendations on which curve and pairing to choose at each security level. The security of many pairing-based protocols are dependent on the intractability of the following problem:

Definition 3.1. *Let $\widehat{e}$ be a bilinear pairing on (G_1, G_2). The bilinear Diffie-Hellman problem (BDHP) is to compute the value of bilinear pairing $\widehat{e}(P, P)^{abc}$, whenever P, aP, bP, cP are given.*

Hardness of the BDHP implies the hardness of DHP in both G_1 and G_2. First, if the DHP in G_1 can be efficiently solved, then one could solve an instance of BDHP by computing abP and then $\widehat{e}(abP, cP) = \widehat{e}(P, P)^{abc}$. Also, if the DHP in G_2 can be efficiently solved, then the BDHP instance could be solved by computing $g = \widehat{e}(P, P)$, $g^{ab} = \widehat{e}(aP, bP)$, $g^c = \widehat{e}(P, cP)$ and then g^{abc}. Nothing else is known about the intractability of the BDHP, and the problem is generally assumed to be just as hard as the DHP in G_1 and G_2.

The Weil and Tate pairings are defined in the following for elliptic curves that can be used for design bilinear pairings. Both pairings make use of a special case of the following fact on the elliptic curve.

Let E be an elliptic curve over $K = \mathbb{F}_q$ by a Weierestrass equation $r(x, y) = 0$, and let $\bar{K}$ denote the algebraic closure of K. We will denote $E(\bar{K})$ by E.

The divisor group of a curve E, denoted by $Div(E)$, is the free abelian group generated by the point 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, is the set of point $P \in E$ for which $n_p \neq 0$. The divisors of degree zero form a subgroup of $Div(E)$, that is denoted by:

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

The function field of E over K is the field of fractions $K(E)$ of $\frac{k[x,y]}{r(x,y)}$. The divisor of a function $f \in K(E)$ is $div(f) = \sum_{p \in E} ord_p(f)(P)$, where $ord_p(f)$ is the multiplicity of P as a root of f, which is positive if f has a zero at P and negative if f has a pole at P. Note that $div(f)$ determines f up to multiplication by a non zero field element. It is a well-known fact that $deg(div(f)) = 0$. A divisor D is called principal if $D = div(f)$ for some $f \in K(E)$. This is denoted by:

$$Prin(E) = \{D \in Div^0(E) \mid D = div(f),\ f \in K(E)\},$$

$Prin(E)$ is a subgroup of $Div^0(E)$. The following result characterizes principal divisors:

Theorem 3.1. *[27] A divisor $D = \sum_{p \in E} n_p(P)$ is principal if and if*

$$deg(D) = \sum_{p \in E} n_p = 0 \quad and \quad \sum_{p \in E} n_p P = \infty$$

The divisor class group (or Picard group) $Pic(E)$ of E is the quotient of the group of degree zero divisors $Div^0(E)$ by the principal divisors, $Prin(E)$, i.e,

$$Pic(E) = \frac{Div^0(E)}{Prin(E)}.$$

It is known that for every divisor $D \in Div^0(E)$, 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 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 $S = P + Q$, corresponds to the divisor equality $div(\frac{l}{v}) = (P) + (Q) - (S) - (\infty)$.

If $D = \sum_{p \in E} n_p(P) \in Div(E)$ and $f \in K(E)$ such that $supp(D) \cap supp(div(f)) = \emptyset$, then the value of f at D is defined to be the following equation:

$$f(D) = \prod_{p \in E} f(p)^{n_p}.$$

4 Weil and Tate pairings definition

Suppose that $|E(F_q)| = hr$, where r is a prime such that $gcd(r, q) = 1$. Let k be the smallest positive integer such that $r|q^k - 1$. The group $E[r] = \{P \in E(\bar{\mathbb{F}_q}) \mid rP = \infty\}$ is a r-torsion points of E. It is known that $E[r] \cong \mathbb{Z}_r \oplus \mathbb{Z}_r$.

Theorem 4.1. *(Balasubramanian, Kobitz [3]).Let E be an elliptic curve defined over $\mathbb{F}_q$ and suppose E has a subgroup $\langle P\rangle$ of order r with $gcd(r, q-1) = 1$. Then $E[r] \subset E(\mathbb{F}_{q^k})$ if and only if $r|q^k - 1$.*

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 $D_p = (P + R) - (R)$ and $D_Q = (Q + S) - (S)$. Then, by theorem 3.1, there exist functions f, g such that $(f) = rD_p$ and $(g) = rD_Q$.

Definition 4.1. *(The Weil pairing)[23]. The bilinear map*

$$w_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})[r] \to \mu_r$$

defined by:

$$w_r(P, Q) = \frac{f(D_q)}{g(D_p)} = \frac{f(Q + S)/f(S)}{g(P + R)/g(R)}$$

is called Weil pairing, where μ_r be the group of r-th roots of unity in $\mathbb{F}^*_{q^k} = \mathbb{F}_{q^k} - \{0\}$.

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

$$f_1 = \frac{l_{P,R}}{v_{P+R}}, \quad f_{i+j} = f_i f_j \frac{l_{[i]P,[j]P}}{v_{[i]P+[j]P}}, \quad f_{[2]i} = f_i^2 \frac{l_{[i]P,[i]P}}{v_{[2i]P}}$$

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

Let P, $Q \in E[r]$ and $f \in \bar{\mathbb{F}}^*_q$ 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 R.

Definition 4.2. *(The Tate pairing)[27] Let $P \in E(\mathbb{F}_q)[r]$, from which it follows that there is a function f whose divisor is $(f) = r(P) - r(\infty)$. Let $Q \in E(\mathbb{F}_{q^k})$ be any representative in any equivalence class in $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$, and let D_Q be a degree zero divisor defined over $\mathbb{F}_{q^k}$, that is equivalent to $(Q) - (\infty)$, but whose support is disjoint to that of (f). The Tate pairing t_r is a map*

$$t_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r$$

defined as:

$$t_r(P, Q) = f_p(D_Q) = (\frac{f_p(Q + R)}{f_p(R)})^{\frac{q^k-1}{n}}$$

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:

$$f_1 = 1, \quad f_{i+1} = f_i \frac{l_{iP,P}}{v_{(i+1)P}}, \quad f_{[2i]} = f_i^2 \frac{l_{[i]P,[i]P}}{v_{[2i]P}}$$

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

One can see the details of Miller [23] algorithm for computing Weil and Tate pairings. 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.

5 Curve Selection

This section describes some of the known methods for generating elliptic curves that are suitable for implementing pairing-based protocols. Recall that E is an elliptic curve defined over $\mathbb{F}_q$, r is a prime divisor of $|E(\mathbb{F}_q)|$ such that $(r, q) = 1$ and k is the smallest positive integer such that $r|q^k - 1$. By Hasse's theorem [27], $|E(\mathbb{F}_q)| = q+1-t$ such that $|t| \leq 2\sqrt{q}$. The following theorem, where the proof can be found in [22], shows the classification of supersingular curves over any finite field for pairing-based cryptography.

Theorem 5.1. *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 $E(\mathbb{F}_q) \cong \mathbb{Z}_{q+1}$,
3) $k = 2$, $t = 0$ and $E(\mathbb{F}_q) \cong \mathbb{Z}_{\frac{q+1}{2}} \oplus \mathbb{Z}_2$ 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 a so-called distortion map $\psi : E(\mathbb{F}_q) \mapsto E(\mathbb{F}_{q^k})$, which is easily computable. This allows us to choose $G = \langle P \rangle$, $G = \psi(P)$ together with Weil/ Tate pairing to produce a non-degenerate bilinear map $\widehat{e} : G \times G \to G$ such that $\widehat{e}(P, Q) = f(P, \psi(Q))$. Distortion maps are all known for supersingular curves. Therefore, we have computable pairing associated with any supersingular curves. One can see the details of the equation and distortion map of essential supersingular curves [1, 17, 19].

It is a research problem to find suitable non-supersingular (ordinary) for pairing-based cryptography, [11, 14]. For this, one needs to find curves with large subgroups for 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 [3]:

Theorem 5.2. *[3] Let E be a randomly chosen elliptic curve over $\mathbb{F}_q$, where q is prime and $z \leq q \leq \frac{z}{2}$. 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 a complex multiplication method to construct suitable ordinary elliptic curves for pairing-based cryptography.

Some of the classification of pairing-friendly ordinary curves constructed by using the complex multiplication [24] are given as follows:
1) Miyagi, Nakabayashi and Takano (MNT) [24] give a complex characterization of ordinary elliptic curves of prime order with embedding degree $k = 3, 4, 6$.
2) Freeman [14] gives a construction for curves of prime order with $k = 10$.
3) Barreto and Naehrig [5] give a construction for curves of prime order with $k = 12$.

In other words, 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 $\rho = \frac{logq}{logr} \approx 2$, for arbitrary k, which leads to inefficient implementation. It should be noticed that ρ it should be as close as one for an efficient pairing-based cryptographic protocol.

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 $E(\mathbb{F}_q)$. It is easy to show that the map $\psi : E'(\mathbb{F}_{q^d}) \to E(\mathbb{F}_{q^k})$ given by $\psi(x, y) = (v^{-1}x, v^{\frac{-3}{2}}y)$ 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 and 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 use for these.

6 Conclusion

In this paper, a broad view of the elliptic curve has been discussed. Elliptic curve is an abelian group that is a suitable candidate for public key cryptosystems. Pairings are being used to design elegant solutions to protocol problems, some of which have been open for many years. Many techniques have been developed for generating suitable elliptic curves in pairing, see [2, 13] for a comprehensive survey and see [10], which explains elliptic curves and pairing from the beginning. Implementing ECC with applying the combination of software and hardware is advantageous as it provides flexibility and favourable performance. Its disadvantage is its lack of maturity, as mathematicians believe that not enough research has been done in ECDLP.

7 Acknowledgement

I would like to thank Islamic Azad university of Shahr-e-Qods for supporting this work.

References

[1] G. Adj , O. Ahmadi, A. Menezes, On isogeny graphs of supersingular elliptic curves over finite fields, Finite Fields and Their Applications, 55 2019, 268-283.

[2] S. Akleylek, B.B. Kirlar, O. Sever and Z. Yuce, Pairing-based cryptography: A Survey, 3rd information security and cryotology conference, 2008.

[3] R. Balasubramanian, N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Dkamoto-Vanstone algorithm, Journal of cryptology, 11(2) 1998, 141-145.

[4] P. Barreto, B. Lynn, M. Scott, Efficient implemention of pairing-based cryptosystem, Journal of Cryptology, 17(4) 2004, 321-334.

[5] P.S.L.M. Barreto, M. Naehrig, Pairing-friendly elliptic curves of prime order, International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2005.

[6] B. Den Boer, Diffie-Hellman is as strong as discrete log for certain primes, Lecture Notes in Computer Science, 403 1996, 530–539.

[7] L. Chen, Z. Cheng, N. P. Smart, Identity-based key agreement protocols from pairings, International Journal of Information Security, 6(4) 2007, 213-241.

[8] C. Cocks, R.G.E. Pinch, Identity-based cryptosystems based on the Weil pairing, unpublished manuscript, 2001.

[9] W. Diffie, M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 22(6) 1976.

[10] C. Costello , Pairing for beginners, A Note, 2013.

[11] P. Duan, S. Cui, C. Chan, Finding More Non-Supersingular Elliptic Curves for Pairing-Based Cryptosystems, Technology, 2(2) 2005, 157-163.

[12] A. Enge, J. Milan, Implementing cryptographic pairings at standard security levels, International Conference on Security, Privacy, and Applied Cryptography Engineering. Springer, Cham, 2014.

[13] D. Freeman, M. Scott, E. Teske, A taxonomy of pairing-friendly elliptic curves, Journal of cryptology, 23(2) 2010, 224-280.

[14] D. Freeman, Constructing pairing-friendly elliptic curves with embedding degree 10, International Algorithmic Number Theory Symposium, Springer, Berlin, Heidelberg, 2006.

[15] G. Frey, H. Ruck, A remark concerning m-advisibility and the discrete logarithm in the divisor class group of curves, Mathematics of computation, 62(206) 1994, 865-874.

[16] S.D. Galbraith, K. G. Paterson, P.N. Smart, Pairings for cryptographers, Discrete Applied Mathematics, 156(16) 2008, 3113-3121.

[17] S.D. Galbraith, F. Vercauteren, Computational problems in supersingular elliptic curve, Quantum Information Processing, 17(10) 2018, 1-22.

[18] S.D. Galbraith, K. Paterson, editors, Pairing Based Cryptography-Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008, Proceedings. Vol. 5209. Springer, 2008.

[19] F. Hess, Efficient Identity Based Signature Schemes Based on Pairings, Lecture Notes in Computer Science, 2595 2003, 310-324.

[20] F. Hess, N.P. Smart, F. Vercauteren, The eta pairing revisited, IEEE Transactions on Information Theory, 52(10) 2006, 4595-4602.

[21] A. Joux, A one round protocol for tripartite Diffie-Hellman, Journal of cryptology, 17(4) 2004, 263-276.

[22] A. Menezes, T. Okamoto, S. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, iEEE Transactions on information Theory, 39(5) 1993, 1639-1646.

[23] V. Miller, The Weil pairing, and its efficient calculation, Journal of cryptology, 17(4) 2004, 235-261.

[24] A. Miyaji, M. Nakabayashi, S. Takano , New explicit conditions of elliptic curves traces for FR-reduction, IEICE transactions on fundamentals of electronics, communications and computer sciences, 84(5) 2001, 1234-1243.

[25] J. Pollard, Monte Carlo methods for index computation mod p, Mathematics of computation, 32(143)1978, 918-924.

[26] H. Shacham, New Paradigms in Signature Schemes, PhD thesis, Stanford, 2006.

[27] H. Silverman Joseph, The arithmetic of elliptic curves, Graduate texts in Mathematics, Springer Verlag , 2008.

[28] O. Uzunkol, M.S. Kiraz, Still wrong use of pairing in cryptography, Applied Mathematics and Computation, 333(C) 2018, 467-479.

[29] F. Vercauteren, Optimal pairings, IEEE Transactions on Information Theory, 56(1) 2009, 455-461.