Math.Comput.Sci.
https://doi.org/10.1007/s11786-018-0347-3

Pairing-Based Cryptography on Elliptic Curves

Josep M. Miret · Daniel Sadornil · Juan G. Tena

Received: 31 May 2017 / Revised: 26 February 2018 / Accepted: 23 March 2018

Abstract We give a brief overview of a recent branch of Public Key Cryptography, the so called Pairing-based Cryptography or Identity-based Cryptography. We describe the Weil pairing and its applications to cryptosystems and cryptographic protocols based on pairings as well as the elliptic curves suitable for the implementation of this kind of cryptography, the so called pairing-friendly curves. Some recent results of the authors are included.

Keywords Elliptic curves · Pairings · Weil pairing · Identity-based cryptography · Embedding degree · Pairing-friendly elliptic curves

Mathematics Subject Classification Primary 94A60 · Secondary 14H52 · 14G50 · 14Q05

1 Introduction

In classical Public Key Cryptography a participant A sends her public key to another one B. With this key, B can either cipher a message addressed to A or verify a digital signature produced by A. The system works whenever the key received by B is really the public key of A and not that of an attacker C. This security condition poses an authentication problem of public keys problem (certificates and certification authorities).

This work has been partially supported by the Spanish Ministerio de Ciencia e Innovacion under Grants MTM2013-46949-P, MTM2014-55421-P and MTM2015-69138-REDT.

To the memory of Mirka Miller.

J. M. Miret (✉)
Dept. de Matemàtica, Escola Politècnica Superior, Universitat de Lleida, Jaume II, 69, 25001 Lleida, Spain
e-mail: miret@matematica.udl.cat

D. Sadornil
Dept. Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, Avda de los Castros s/n, 39005 Santander, Spain
e-mail: sadornild@unican.es

J. G. Tena
IMUVA y Dept. de Algebra, Análisis Matemático, Geometría y Topología, Facultad de Ciencias, Universidad de Valladolid, Paseo de Belén, 7, 47011 Valladolid, Spain
e-mail: juantenaayuso@gmail.com

Published online: 27 June 2018

The idea of a new system was proposed in 1984 by Shamir [22], whereby public keys would not need authentication and the public key of A could be any of A's identity pieces (name, E-mail, a digital picture, etc). This Identity-based Cryptography demands the existence of a *Trusted Authority* (TA), which selects the parameters common to all the participants and provides them with their private keys.

Nevertheless, to design specific cryptosystems and cryptographic protocols based on this proposal was another problem. Shamir was able to give an identity-based key distribution scheme, but the construction of an identity-based cryptosystem was only achieved by Boneh and Franklin [6], using pairings on elliptic curves defined over finite fields. Today there exist many identity-based cryptosystems, key distribution protocols and digital signature schemes using pairings (Weil, Tate, Ate, Eta, etc) as their main tool.

Section 2 is devoted to the description of the Weil pairing and the Miller's algorithm, which allows to compute that pairing efficiently. In Sect. 3 we present some of the most important cryptosystems and cryptographic protocols in the field of pairing-based cryptography: the cipher system of Boneh-Franklin, the Joux tripartite key exchange and some identity-based signature schemes.

Finally in Sect. 4 we make some remarks about the elliptic curves used in pairing cryptography, the so called pairing-friendly curves, and an algorithm to find such suitable curves in two families of elliptic curves.

2 Weil Pairing

Pairings on an elliptic curve E, defined over a finite field $\mathbb{F}_q$, are maps which to each pair of points of E assign an element of the multiplicative group of a certain extension field $\mathbb{F}_{q^k}$. They have been used in several different contexts. First, in a negative sense, because the MOV attack [16] using Weil pairing and FR attack [11] using Tate pairing reduce the discrete logarithm problem on some elliptic curves (ECDLP) to the discrete logarithm problem (DLP) in the finite field $\mathbb{F}_{q^k}$ (see [13,15]). On the other hand, the bilinear pairings have been used in a positive way in cryptography, because they are an important tool for the construction of identity-based schemes (see [14]).

We first discuss the basic facts used in pairing-based cryptosystems and then we focus on the elliptic curves. For a more detailed background see [5].

Definition 2.1 Let $(G_1, +)$ and $(G_2, +)$ be abelian additive groups of order n. Let $(G_3, \cdot)$ be a cyclic group of order n. A bilinear pairing is an efficient computable map

$$e : G_1 \times G_2 \to G_3$$

that satisfies the following additional conditions:

- (Bilinearity) $e(P + P', Q) = e(P, Q)e(P', Q)$ and $e(P, Q + Q') = e(P, Q)e(P, Q')$, for all $P, P' \in G_1$, $Q, Q' \in G_2$.
- (Non-degeneracy) For all $P \neq 0 \in G_1$, there exists $Q \in G_2$ with $e(P, Q) \neq 1$. Also, for all $Q \neq 0 \in G_2$, there exists $P \in G_1$ with $e(P, Q) \neq 1$.

From this definition, we also have that $e(P, 0) = e(0, Q) = 1$ and $e(aP, bQ) = e(P, Q)^{ab}$ for $P \in G_1,\ Q \in G_2$ and $a, b \in \mathbb{Z}$. Non-degeneracy can be rewritten as follows: if $e(P, Q) = 1$, for all $Q \in G_2$, then $P = 0$ and the same holds for the second component.

In the following, G_1 and G_2 will be groups related to an elliptic curve E defined over some finite field $\mathbb{F}_q$ ($q = p^r$, p prime) and G_3 will be a group of roots of unity. For simplicity, we always consider $p \geq 5$. A reference for an introduction on elliptic curves is [4]. An elliptic curve E over $\mathbb{F}_q$ is an algebraic curve given by an equation of the form

$$E/\mathbb{F}_q : \ y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q,$$

satisfying $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$. An extra point at infinity $\mathcal{O}$ is added. The set $E(\mathbb{F}_q)$ of points on E with coordinates in $\mathbb{F}_q$ (including $\mathcal{O}$) can be turned into a finite abelian group via the tangent-and-chord law, with $\mathcal{O}$ the neutral element.

Hasse's theorem gives bounds for the cardinality of an elliptic curve, that is $\#E(\mathbb{F}_q) = q+1-t$, with $|t| \leq 2\sqrt{q}$. If $p \mid t$, then E is said to be supersingular; otherwise E is ordinary. Moreover,

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z},$$

where $n_2 \mid n_1$ and $n_2 \mid (q-1)$. For an integer ℓ, $E[\ell]$ denotes the set of ℓ-torsion points of E (over $\overline{\mathbb{F}_q}$).

To define and compute the Weil pairing, we need the algebraic geometry language of divisors (for a more detailed treatment see [23]). A divisor on E is a formal sum of points $D = \sum n_P(P)$ where the sum is over all points of E and n_P are integers only a finite number of which are nonzero. The support of D is the set of points P for which $n_P \neq 0$. The divisor D is called a zero divisor if $\sum n_P = 0$. The set of all divisors that are defined over $\mathbb{F}_q$ is denoted by $Div_{\mathbb{F}_q}(E)$.

The function field of E over $\mathbb{F}_q$ is the field of fractions $\mathbb{F}_q(E)$ of the quotient ring $\mathbb{F}_q[x, y]/(y^2 - x^3 - ax - b)$. The divisor of a function $f \in \mathbb{F}_q(E)$ is $div(f) = \sum m_P(P)$, where m_P is the multiplicity of P as a root of f. Note that $div(f)$ determines f up to multiplication by a nonzero field element. The divisors of functions are called principal divisors (a divisor $D = \sum n_P(P)$ is principal if and only if $\sum n_P = 0$ and $\sum n_P(P) = \mathcal{O}$). Two divisors $D_1, D_2 \in Div_{\mathbb{F}_q}(E)$ are said to be equivalent, $D_1 \sim D_2$, if $D_1 = D_2 + div(f)$ for some $f \in \mathbb{F}_q(E)$. Let $f \in \mathbb{F}_q(E)$ and $D = \sum n_P(P) \in Div_{\mathbb{F}_q}(E)$ be such that $div(f)$ and D have disjoint support. Then $f(D)$ is defined as

$$f(D) = \prod f(P)^{n_P}.$$

Note that $f(D)$ is a nonzero element of $\mathbb{F}_q$.

Suppose $\#E(\mathbb{F}_q) = h\ell$, ℓ prime such that $\gcd(\ell, q) = 1$. The Weil pairing (and also the others pairings on E) is a bilinear map with values on $\mathbb{F}_{q^k}$ where k is the smallest positive integer such that $\ell \mid (q^k - 1)$. The integer k is called the embedding degree of $E/\mathbb{F}_q$. Then k is the minimum such that $\mathbb{F}^*_{q^k}$ contains an order-ℓ subgroup μ_ℓ. It is also worth noting (see [2]) that if $k > 1$, $\ell \mid (q^k - 1)$ if and only if $E(\mathbb{F}_{q^k})$ contains the full ℓ-torsion group $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

Definition 2.2 Let E an elliptic curve over $\mathbb{F}_q$ with cardinal $h\ell$ and embedding degree k. The Weil pairing is a bilinear map $e_\ell : E[\ell] \times E[\ell] \to \mu_\ell$ defined as follows:

For any pair $P, Q \in E[\ell]$, let A, B zero divisors such that $A \sim (P) - \mathcal{O}$, $B \sim (Q) - \mathcal{O}$ and A, B with disjoint support. Let $f_A, f_B \in \overline{\mathbb{F}_q}(E)$ such that $div(f_A) = \ell P$ and $div(f_B) = \ell B$. Then:

$$e_\ell(P, Q) = f_A(B)/f_B(A).$$

The value $e_\ell(P, Q)$ is independent of the choice of A, B, f_A and f_B. Weil pairing has the alternating property, that is $e_\ell(P, Q) = e_\ell(Q, P)^{-1}$ and so $e_\ell(P, P) = 1$. To avoid this, a modified pairing $\hat{e}_\ell$ can be used, employing a distortion map (see [5]).

Definition 2.3 A distortion map for a point $P \in E(\mathbb{F}_q)$ of prime order ℓ, coprime with p, is an endomorphism σ of E defined over $\mathbb{F}_{q^k}$ such that

$$\sigma(P) \notin \langle P \rangle.$$

Therefore a modified Weil pairing can be defined as

$$\hat{e}_\ell(P, Q) = e_\ell(P, \sigma(Q))$$

satisfying $\hat{e}_\ell(P, P) \neq 1$.

Since cryptographic schemes on pairings on elliptic curves work on a cyclic subgroup $\langle P \rangle \subseteq E(\mathbb{F}_q)$ of order ℓ, distortion maps avoid that the Weil pairing e_ℓ be trivial for every couple of points $Q, R \in \langle P \rangle$.

2.1 Miller's Algorithm

In 1986, Miller [17] described an algorithm for evaluating the Weil pairing on an algebraic curve. The original paper has never been published, but in 2004 the author presented an updated and extended version [18]. The crucial ingredient of the algorithm is a procedure for determining a function with a particular divisor. The Weil pairing can be computed more easily using two auxiliary points R, S as follows

$$e_\ell(P,Q) = \frac{f_{\ell,P}(Q+R)f_{\ell,Q}(S)}{f_{\ell,P}(R)f_{\ell,Q}(P+S)},$$

where $f_{\ell,P}$, $f_{\ell,Q}$ are rational functions in two variables computed recursively using

$$f_{0,T} = f_{1,T} = 1,$$
$$f_{m+n,T} = f_{m,T}\, f_{n,T}\, g_{mT,nT}.$$

where $g_{U,V} = \frac{L_{U,V}}{L_{(U+V),-(U+V)}}$ and $L_{U,V} = 0$ is the line through U, V or the tangent line if $U = V$. This function $f_{\ell,X}$ can be efficiently computed by a left-to-right double-and-add method.

Algorithm 2.4

```
Require: $T \in E(\mathbb{F}_{q^k})[\ell]$,
  $\ell = (\ell_{b-1}, \ell_{b-2}, \ldots, \ell_0)_2$ (binary representation)
Ensure: $f_{\ell,T}$
  $f \leftarrow 1$, $W \leftarrow P$.
  for $i$ from $b-2$ to 0 do
    $f \leftarrow f^2 \frac{L}{L'}$ ($L$ tangent line through $W$, $L'$ vertical line through $2W$)
    $W \leftarrow 2W$
    if $\ell_i = 1$ then
      $f \leftarrow f \frac{L}{L'}$ ($L$ be the line through $T$ and $W$, $L'$ vertical line through $T + W$)
      $W \leftarrow T + W$
    end if
  end for
  RETURN $f$
```

Miller's algorithm has $O(\log \ell)$ iterations, each requiring a constant number of arithmetic operations in $\mathbb{F}_{q^k}$. Several improvements have been proposed that significantly reduce the computational cost. In [19] the authors have presented a modified version of Miller's algorithm which exploits the non-adjacent form (NAF) of the integer ℓ, reducing the number of iterations. NAF is a unique binary signed-digit representation (i.e. in a NAF representation a value of -1 is allowed), where non-zero values cannot be adjacent. The main benefit is that the Hamming weight of the value will be minimal. For regular binary representations of values, half of all bits will be non-zero, on average, but with NAF this drops to only one-third of all digits.

From the previous recurrences taking into account that $f_{0,T} = f_{1,T} f_{-1,T} g_{T,-T}$, the following must be added to the algorithm if a NAF representation is used:

```
if $\ell_i = -1$ then
  $f \leftarrow f \frac{L}{L_1 L'}$ ($L_1$ vertical line through $T$, $L$ line through $-T$ and $W$, $L'$ vertical line through $W - T$)
  $W \leftarrow W - T$
end if
```

However, there is another way to get the function $f_{\ell,T}$ from the NAF representation of ℓ. To this end, we change above instructions to:

```
if $\ell_i = -1$ then
  $f \leftarrow f \frac{L'}{L}$ ($L'$ vertical line through $W$ and $L$ line through $T$ y $-W$)
  $W \leftarrow W - T$
```

end if

Note that the obtained function is different depending on the algorithm used (Miller's or the modified versions). However, the Weil pairing value $e_\ell(P, Q)$ is always the same (see [5]).

3 Identity-Based Cryptography

In this Section we will assume that the Trusted Authority (TA) has selected and published an elliptic curve E over a finite field $\mathbb{F}_q$, a point $P \in E$ of prime order ℓ, a cyclic group $\mu_\ell \subset \mathbb{F}^*_{q^k}$ with order ℓ, his own secret key s, $1 < s < \ell$, and the corresponding public key $P_{TA} = sP$. The TA has also chosen a distortion map σ and a modified, non trivial, Weil pairing $\hat{e}_\ell$, see [5] (and additional data for any particular algorithm).

We begin schematizing the cipher system of Boneh and Franklin [6]. The messages M to be ciphered will be binary blocks of preset length n (elements of $\{0, 1\}^n$).

- **Parameters** The TA:
  1. Sends P_{TA} to the participants.
  2. Chooses a hash function H_1 which allows to assign to each user's identity Id_A the public key $P_A = H_1(Id_A) \in \langle P \rangle$ and calculates A's private key $S_A = sP_A$.
  3. Chooses a hash function $H_2 : \mu_\ell \to \{0, 1\}^n$.
  4. Chooses a hash function $H_3 : \{0, 1\}^{2n} \to \{r;\ 1 < r < \ell\}$.
  5. Chooses a hash function $H_4 : \{0, 1\}^n \to \{0, 1\}^n$.
- **Ciphering**: If the participant B wants to send the message M to A:
  1. B computes $P_A = H_1(Id_A)$.
  2. B randomly takes $S \in \{0, 1\}^n$.
  3. B computes $r = H_3(S, M)$.
  4. B computes $C = (C_1, C_2, C_3)$ where,

     $$C_1 = rP, \quad C_2 = S \oplus H_2(\hat{e}_\ell(P_A, P_{TA})^r), \quad C_3 = M \oplus H_4(S).$$
- **Deciphering**: When A receives $C = (C_1, C_2, C_3)$:
  1. A computes $S' = C_2 \oplus H_2(\hat{e}_\ell(S_A, C_1))$.
  2. A computes $M' = C_3 \oplus H_4(S')$.
  3. A computes $r' = H_3(S', M')$.
  4. If $C_1 = r'P$ then A accepts $M'(= M)$ as valid. Otherwise, A rejects the received message.

3.1 Identity-Based Key Distribution Schemes

In their seminal paper, Diffie and Hellman [9] proposed a bipartite key exchange, based on the discrete logarithm problem, allowing two participants A, B to agree on a secret key, for use in a symmetric cipher, through an insecure channel (see [24]). It is easy to give a similar scheme in Identity-based Cryptography (see [5]). However, the use of pairings also allows the extension to a tripartite key agreement scheme, in which three participants A, B, C can simultaneously agree on a common key K_{ABC}. We describe below this tripartite key distribution scheme, proposed by Joux [12].

- **Choices and Messages**
  1. A randomly chooses an integer n_A; $1 < n_A < \ell$ and compute $P_A = n_A P$;
  2. B randomly chooses an integer n_B; $1 < n_B < \ell$ and compute $P_B = n_B P$;

3. C randomly chooses an integer n_C; $1 < n_C < \ell$ and compute $P_C = n_C P$;
4. A, B, C exchange the values P_A, P_B, P_C.

- **Key agreement**: Now A, B, C compute the common key K_{ABC}:

1. $\hat{e}_\ell(P_B, P_C)^{n_A} = \hat{e}_\ell(P, P)^{n_A n_B n_C} = K_{ABC}$;
2. $\hat{e}_\ell(P_A, P_C)^{n_B} = \hat{e}_\ell(P, P)^{n_A n_B n_C} = K_{ABC}$;
3. $\hat{e}_\ell(P_A, P_B)^{n_C} = \hat{e}_\ell(P, P)^{n_A n_B n_C} = K_{ABC}$.

Remark 3.1 While the security of the classical Diffie-Hellman key exchange rests on the (supposed) intractability of the Computational Diffie–Hellman Problem (see [24]), the security of the tripartite Joux scheme is based on the difficulty of the similar Bilinear Diffie-Hellman Problem: Known the values $n_A P, n_B P, n_C P$ compute $\hat{e}_\ell(P, P)^{n_A n_B n_C}$.

3.2 Identity-Based Digital Signatures

In classical Public Key Cryptography the idea of a cipher system (RSA, ElGamal) can be adapted to a digital signature scheme. The same happens with the Boneh-Franklin'algorithm. We detail one such signature scheme, which looks similar to ElGamal's signature (the signature is applied to a hashing of the message and it depends on a random value r).

- **Parameters**: The TA,

1. Sends the public key $P_{TA} = sP$ to the participants.
2. Chooses a hash function H_1 allowing a participant's identity Id_A to assign a public key $P_A = H_1(Id_A) \in \langle P \rangle$.
3. Chooses a hash function $H_2 : \{0, 1\}^n \times \langle P \rangle \to \{h;\ 1 < h < \ell\}$.
4. Computes the private key of any participant A: $S_A = sP_A$.

- **Signature Algorithm**: To sign a message M, participant A:

1. Chooses r, $1 < r < \ell$.
2. Computes:

$$F_1 = rP_A;\ \ h = H_2(M, F_1);\ \ F_2 = (r + h)S_A. \tag{3.1}$$

3. The couple $F = (F_1, F_2)$ is the signature of M.

- **Verification Algorithm**: When B receives (M, F):

1. B verifies if

$$\hat{e}_\ell(P_{AC}, F_1 + hP_A) = \hat{e}_l(P, F_2). \tag{3.2}$$

2. If the equality is true B accepts F as a valid signature of M.

Boneh et al. [7] proposed an identity-based digital signature scheme, simple, efficient and using very short keys.

- **Parameters**: Here the messages $M \in \mathcal{M}$ are binary sequences of arbitrary length. The TA chooses

1. A hash function $H : \mathcal{M} \to \langle P \rangle$.
2. The privates keys n_A; $1 < n_A < \ell$ and public keys $P_A = n_A P$.

- **Signature Algorithm**: To sign M, A computes $F(M) = n_A H(M)$.

Table 1 Equivalencies for curve parameters and embedding degree according to security level

Sec. level (bits)	ℓ (bits)	q^k (bits)	k ($\rho \equiv 1$)	k ($\rho \equiv 2$)
80	160	960–1280	6–8	3–4
112	224	2200–3600	10–16	5–8
128	256	3000–5000	12–20	6–10
192	384	8000–10000	20–26	10–13
256	512	14000–18000	28–36	14–18

- **Verification Algorithm**: The verifier receives (M, F) and computes if the following equality is true, $\hat{e}_\ell(F(M), P) = \hat{e}_\ell(H(M), P_A)$.

Boneh et al. used a modified Weil pairing $\hat{e}_\ell$ on a family of supersingular elliptic curves with immersion degree $k = 6$, achieving signatures of half the length of the ECDSA (with the same security level). They also point out that using curves with greater immersion degree will reduce the signature length even more (but it would require the use of ordinary elliptic curves, for which distortion maps do not exist).

4 Pairing-Friendly Elliptic Curves

Elliptic curves over $\mathbb{F}_q$ with near-prime order $n = h\ell$ and whose embedding degree k is neither too small nor too large are suitable to be used in pairing-based cryptography. They are the so-called pairing-friendly curves. It is advisable that the ECDLP over their subgroup of points of order ℓ as well as the DLP over the multiplicative group $\mathbb{F}^*_{q^k}$ have the same computational difficulty. Indeed, if k is the embedding degree, the Weil pairing and the reduced Tate pairing allow us to transform points on the curve to elements of the extension field $\mathbb{F}_{q^k}$. Thus, if k is very small the MOV and the FR attacks could solve the ECDLP from the DLP over the group $\mathbb{F}^*_{q^k}$. Besides, we need k not too large in order to compute the pairing.

In order to determine an appropriate relationship between k and ℓ, we can compare the complexity of the algorithms which solve the DLP and the ECDLP. Since one of the best algorithms to solve the ECDLP over a cyclic subgroup of order ℓ of $E(\mathbb{F}_q)$ is Pollard's rho algorithm which has complexity $O(\sqrt[4]{\ell})$, whereas the DLP over the group $\mathbb{F}^*_{q^k}$ can be solved by the index-calculus with subexponential complexity, it can be derived that $k \geq \log_2(\ell)/8$.

Then, it is said that a curve $E/\mathbb{F}_q$ is pairing-friendly if it satisfies the following properties:

- $E(\mathbb{F}_q)$ has a subgroup of order $\ell \geq \sqrt{q}$;
- $E/\mathbb{F}_q$ has embedding degree $k \geq \log_2(\ell)/8$.

Freeman et al. in [10] show a table comparing different sizes of ℓ, q and q^k. They also consider the parameter $\rho = \log q / \log \ell$ which measures the size of the base field with respect to the subgroup of prime-order ℓ. These equivalent security levels are given in Table 1.

For supersingular curves, their embedding degrees can take few values. For them, $k \leq 6$, and if the curve is defined over a prime finite field, $k = 2$ (see for instance [16]). However, it is not easy to construct ordinary curves with small embedding degree.

4.1 Some Families

A general method that can be used for constructing pairing-friendly curves is the complex multiplication method, proposed by Atkin and Morain [1], which builds a curve over a given finite field $\mathbb{F}_q$ with a fixed number of points $q + 1 - t$.

More recently, new strategies have appeared which allow us to obtain families of ordinary pairing-friendly curves, for which the parameters of the curve $E/\mathbb{F}_q$ (trace t and prime order ℓ of the subgroup) are given by means of three polynomials $q(x)$, $t(x)$ and $\ell(x)$ in terms of a new parameter x.

Thus, MNT curves proposed by Miyaji et al. [21] have prime order and possible embedding degrees 3, 4 or 6. More precisely, they are curves defined over a prime finite field $\mathbb{F}_q$ with $\ell = q+1-t$ and whose embedding degree is:

- $k = 3$ if and only if there exists $x \in \mathbb{Z}$ such that $q = 12x^2 - 1$ and $t = -1 \pm 6x$;
- $k = 4$ if and only if there exists $x \in \mathbb{Z}$ such that $q = x^2 + x + 1$ and either $t = -x$ or $t = x + 1$;
- $k = 6$ if and only if there exists $x \in \mathbb{Z}$ such that $q = 4x^2 + 1$ and $t = 1 \pm 2x$.

Other families of curves called cyclotomic are based on the properties:

- ℓ divides $q + 1 - t$ implies $q \equiv t - 1 \pmod{\ell}$;
- ℓ divides $q^k - 1$, k embedding degree, implies ℓ divides $\Phi_k(q)$, where $\Phi_k(x)$ is the k-th cyclotomic polynomial.

One of these cyclotomic families was constructed by Barreto and Naehrig [3]. Their curves are given by:

$$q(x) = 36x^4 + 36x^3 + 24x^2 + 6x + 1, \quad t(x) = 6x^2 + 1, \quad \ell(x) = 36x^4 + 36x^3 + 18x^2 + 6x + 1.$$

All of them have embedding degree $k = 12$ and $\rho = 1$.

4.2 Curves with j-Invariant 0 and 1728

In [20], families of curves with j-invariant 0 and 1728, that is, of equation $y^2 = x^3 + b$ and $y^2 = x^3 + ax$, respectively, which have small embedding degree, are studied. The number of isomorphim classes of ordinary elliptic curves with j-invariant 0 and 1728 over $\mathbb{F}_q$, $q = p^r$, is given by:

- If $p \equiv 1 \pmod 4$ there exist four isomorphism classes with j-invariant 1728, whose representatives are

  $$E_i : y^2 = x^3 + \omega^i x, \quad 0 \le i \le 3,$$

  where ω is a generator of $\mathbb{F}_q^*$. If $p \equiv 3 \pmod 4$ all classes are supersingular.
- If $p \equiv 1 \pmod 3$ there exist six isomorphism classes with j-invariant 0, whose representatives are

  $$E_i : y^2 = x^3 + \omega^i, \quad 0 \le i \le 5,$$

  where ω is a generator of $\mathbb{F}_q^*$. If $p \equiv 2 \pmod 3$ all classes are supersingular.

To characterize when these elliptic curves have low embedding degree, one can take advantage of the following result [8], given by Cocks and Pinch:

Lemma 4.1 *An elliptic curve $E/\mathbb{F}_q$ with cardinality $h\ell$ has embedding degree k with respect to ℓ if and only if the trace t of its Frobenius endomorphism π satisfies $t \equiv 1 + \zeta_k \pmod{\ell}$, for ζ_k a kth root of unity modulo ℓ.*

Since elliptic curves with j-invariant 1728 or 0 are exactly those whose endomorphism ring is $\mathbb{Z}[i]$ or $\mathbb{Z}[\zeta_3]$, we have to search for elements π in this ring with norm q and right trace. Then we have to decide which of the four curves E_i (respectively six curves E_i') corresponds to such π.

Using this approach, for $k = 3$, in [20] we have obtained the following result.

Proposition 4.2 *Let $\ell > 3$ be an odd prime and ζ_3 a cubic root of the unity modulo ℓ.*

i) One of the four curves $E_i : y^2 = x^3 + \omega^i x$ has embedding degree 3 with respect to ℓ if and only if

$$q = \left(\frac{1+\zeta_3}{2} \pmod{\ell} + m\ell\right)^2 + \left(\frac{3\zeta_3}{4} \pmod{\ell}\right) + n\ell$$

for some integers m, n, being $(3\zeta_3/4 \pmod{\ell}) + n\ell$ a square in $\mathbb{Z}$.

ii) One of the six curves $E'_i\,:\,y^2 = x^3 + \omega^i$ has embedding degree 3 with respect to ℓ if and only if

$$q = a^2 + ab + b^2, \quad a = m\ell, \quad b = 1 + \zeta_3 + \ell(n - 2m),$$

for some integers m, n.

The group structure for the corresponding curves can also be computed for specific values ℓ, m, n and the correct ζ_3.

Concerning distortion maps, there always exist on supersingular elliptic curves. For instance, for curves with equations $y^2 = x^3 + x$ and $y^2 = x^3 - x$ over $\mathbb{F}_q$, $q \equiv 3 \pmod 4$, which have cardinality $q + 1$, a distortion map is given by

$$\sigma(x, y) = (-x, iy).$$

For curves with equations $y^2 = x^3 + 1$ and $y^2 = x^3 + B$, $B \in \mathbb{F}_q^* - (\mathbb{F}_q^*)^2$, over $\mathbb{F}_q$, $q \equiv 2 \pmod 3$, which have cardinality $q + 1$, a distortion map is given by

$$\sigma(x, y) = (\zeta_3 x, y).$$

Nevertheless, they do not exist for ordinary elliptic curves with embedding degree greater than 1 (see [25]).

All these methods and techniques for constructing pairing-friendly curves as well as for searching distorsion maps can provide improvements in the design of efficient cryptographic schemes on pairings on elliptic curves. However, open problems remain to be solved and new questions emerge. Advances in this field of research will contribute to guarantee the security of these cryptographic protocols.

References

1. Atkin, A.O.L., Morain, F.: Elliptic curves and primality proving. Math. Comput. **61**, 29–68 (1993)
2. Balasubramanian, R., Koblitz, N.: The improbability that an elliptic curve has subexponential log problem under the Menezes–Okamoto–Vanstone algorithm. J. Cryptol. **11**(2), 141–145 (1998)
3. Barreto, P., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: SAC 2005, LNCS 3897, pp. 319–331 (2006)
4. Blake, I., Seroussi, G., Smart, N.: Elliptic Curves in Cryptography, London Mathematical Society LNS, vol. 265. University Press, Cambridge (1999)
5. Blake, I., Seroussi, G., Smart, N.: Advances in Elliptic curve Cryptography. London Mathematical Society, LNS 317. University Press, Cambridge (2005)
6. Boneh, D., Franklin, M.: Identity-Based Encryption from the Weil Pairing. In: Advances in Cryptology—CRYPTO 2001. LNCS 2139, pp. 213–229. Springer (2001)
7. Boneh, D., Lynn, B., Shacham, H.: Short Signatures from the Weil Pairing. In: Advances in Cryptology—ASIACRYPT 2001, LNCS 2248. Springer (2001)
8. Brezing, F., Weng, A.: Elliptic curves suitable for pairings based cryptography. Des Codes Cryptogr. **37**, 133–141 (2005)
9. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory IT **22**(6), 644–654 (1976)
10. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptol. **23**(2), 224–280 (2010)
11. Frey, G., Rück, H.G.: A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comput. **62**(206), 865–874 (1994)
12. Joux, A.: A one round protocol for tripartite Diffie–Hellman. In: Algorithmic Number Theory Symposium 2000, LNCS 1838, pp. 385–394. Springer (2000)
13. Hankerson, D., Menezes, A., Vanstone, S.: Guide to Elliptic Curve Cryptography. Springer, Berlin (2004)
14. Martin, L.: Identity-Based Encryption. Information Security and Privacy series. Artec House, Washington (2008)
15. Menezes, A.: Elliptic Curves Public Key Cryptography. Kluwer, Alphen aan den Rijn (1993)
16. Menezes, A., Okamoto, T., Vanstone, S.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans. Inf. Theory **39**, 1639–1646 (1993)
17. Miller, V.: Short Programs for Functions on Curves. IBM Thomas J. Watson Research Center (available at https://crypto.stanford.edu/miller/miller.pdf), (1986)
18. Miller, V.: The Weil pairing, and its efficient calculation. J. Cryptol. **17**, 235–261 (2004)
19. Miret, J., Sadornil , D., Tena, J.: Familias de curvas elípticas adecuadas para Criptografía Basada en la Identidad. In Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información (RECSI2014), Publicaciones Universidad de Alicante, pp. 35–38 (2014)

20. Miret, J., Sadornil, D., Tena, J.: Computing elliptic curves with $j = 0, 1728$ and low embedding degree. Int. J. Comput. Math. **93**(12), 2042–2053 (2016)
21. Miyaji, A., Nakabayashi, M., Takano, S.: New explicit conditions of elliptic curve traces for FR-reduction. IEICE Trans. Fundam. **E84–A**(5), 1234–1243 (2001)
22. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Advances in Cryptology—CRYPTO'84, LNCS 196, pp. 47–53. Springer (1985)
23. Silvervam, J.: The Arithmetic of Elliptic Curves. Springer, GTM 106 (1986)
24. Stinson, D.: Cryptography. Theory and Practice. Chapman & Hall/CRC, Boca Raton (2006)
25. Verheul, E.R.: Evidence that XTR is more secure than supersingular elliptic curves cryptosystems. J. Cryptol. **17**(4), 277–296 (2004)