An Introduction to Pairing-Based Cryptography

Alfred Menezes

Abstract. Bilinear pairings have been used to design ingenious protocols for such tasks as one-round three-party key agreement, identity-based encryption, and aggregate signatures. Suitable bilinear pairings can be constructed from the Tate pairing for specially chosen elliptic curves. This article gives an introduction to the protocols, Tate pairing computation, and curve selection.

1. Introduction

The discrete logarithm problem (DLP) has been extensively studied since the discovery of public-key cryptography in 1975. Recall that the 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 a 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., see [**10, 38**]), that the DLP reduces in polynomial time to the DHP.

The assumed intractability of the DHP is the basis for the security of the Diffie-Hellman key agreement protocol [**20**] illustrated in Figure 1. The objective of this protocol is to allow Alice and Bob to establish a shared secret by communicating over a channel that is being monitored by an eavesdropper 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 randomly selects a secret integer $b \in [1, n-1]$ and sends bP to Alice. Both Alice and Bob can use their secret integers to calculate the shared secret $K = abP$. The eavesdropper is faced with the task of computing K given P, aP and bP, which is precisely an instance of the DHP.

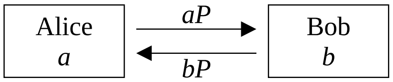


Figure 1. Two-party one-round key agreement protocol.

1991 *Mathematics Subject Classification.* Primary 94A60.

Key words and phrases. Public-key cryptography, elliptic curves, Tate pairing.

The Diffie-Hellman protocol can be viewed as a one-round protocol because the two exchanged messages are independent of each other. The protocol can easily be extended to three parties, as illustrated by the two-round protocol depicted in Figure 2; the secret shared by Alice, Bob and Chris is $K = abcP$. The protocol is secure against eavesdroppers if the problem of computing $K = abcP$ given P, aP, bP, cP, abP, bcP and caP is intractable. This problem is presumably no easier than the DHP.

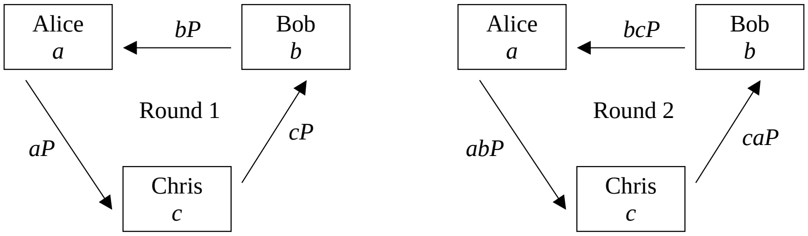


FIGURE 2. Three-party two-round key agreement protocol.

A natural question to ask is whether there exists a three-party one-round key agreement protocol that is secure against eavesdroppers. This question remained open until 2000 when Joux [**32**] devised a surprisingly simple protocol that used bilinear pairings. Joux's paper was of great interest to cryptographers, who started investigating further applications of pairings. The next two important applications of pairings were the identity-based encryption scheme of Boneh and Franklin [**14**] and the short signature scheme of Boneh, Lynn and Shacham [**16**]. 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.

The purpose of this paper is to provide an introduction to pairing-based cryptography. We will present some of the important developments in protocol design, Tate pairing computation, and elliptic curve selection. Our treatment will be neither exhaustive nor complete, but nonetheless we hope that it will be sufficiently detailed so that the reader will appreciate the crucial ideas. More in-depth studies of these topics can be found in the expository articles by Galbraith [**25**] and Paterson [**45**], and in the extensive research literature.

The remainder of this paper is organized as follows. Bilinear pairings are introduced in §2. In §3 we present Joux's key agreement protocol, the Boneh-Lynn-Shacham short signature scheme, and the Boneh-Franklin identity-based encryption scheme. Relevant properties of elliptic curves are reviewed in §4, and then in §5 we describe how the Tate pairing on elliptic curves can be used to construct bilinear pairings. In §6, we present methods for generating suitable elliptic curves. §7 makes some concluding remarks.

2. Bilinear pairings

Let n be a prime number. Let $G_1 = \langle P \rangle$ be an additively-written group of order n with identity ∞, and let G_T be a multiplicatively-written group of order n with identity 1.

Definition 2.1. A *bilinear pairing* on (G_1, G_T) is a map

$$\hat{e} : G_1 \times G_1 \to G_T$$

that satisfies the following conditions:

(1) (*bilinearity*) For all $R, S, T \in G_1$, $\hat{e}(R + S, T) = \hat{e}(R, T)\hat{e}(S, T)$ and $\hat{e}(R, S + T) = \hat{e}(R, S)\hat{e}(R, T)$.
(2) (*non-degeneracy*) $\hat{e}(P, P) \neq 1$.
(3) (*computability*) $\hat{e}$ can be efficiently computed.

The following properties of bilinear pairings can be easily verified. Property (5) is another way of defining non-degeneracy. For all $S, T \in G_1$:

(1) $\hat{e}(S, \infty) = 1$ and $\hat{e}(\infty, S) = 1$.
(2) $\hat{e}(S, -T) = \hat{e}(-S, T) = \hat{e}(S, T)^{-1}$.
(3) $\hat{e}(aS, bT) = \hat{e}(S, T)^{ab}$ for all $a, b \in \mathbb{Z}$.
(4) $\hat{e}(S, T) = \hat{e}(T, S)$.
(5) If $\hat{e}(S, R) = 1$ for all $R \in G_1$, then $S = \infty$.

One consequence of the bilinearity property is that the DLP in G_1 can be efficiently reduced to the DLP in G_T. For, if (P, Q) is an instance of the DLP in G_1 where $Q = xP$, then $\hat{e}(P, Q) = \hat{e}(P, xP) = \hat{e}(P, P)^x$. Thus $\log_P Q = \log_g h$, where $g = \hat{e}(P, P)$ and $h = \hat{e}(P, Q)$ are elements of G_T.

The security of many pairing-based protocols is dependent on the intractability of the following problem.

Definition 2.2. Let $\hat{e}$ be a bilinear pairing on (G_1, G_T). The *bilinear Diffie-Hellman problem (BDHP)* is the following: Given P, aP, bP, cP, compute $\hat{e}(P, P)^{abc}$.

Hardness of the BDHP implies the hardness of the DHP in both G_1 and G_T. First, if the DHP in G_1 can be efficiently solved, then one could solve an instance of the BDHP by computing abP and then $\hat{e}(abP, cP) = \hat{e}(P, P)^{abc}$. Also, if the DHP in G_T can be efficiently solved, then the BDHP instance could be solved by computing $g = \hat{e}(P, P)$, $g^{ab} = \hat{e}(aP, bP)$, $g^c = \hat{e}(P, cP)$ 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_T.

We note that the decisional Diffie-Hellman problem (DDHP) in G_1 can be efficiently solved. The DDHP is to decide whether a given quadruple (P, aP, bP, cP) of elements in G_1 is a valid Diffie-Hellman quadruple, i.e., whether $cP = abP$. This can be accomplished by computing $\gamma_1 = \hat{e}(P, cP) = \hat{e}(P, P)^c$ and $\gamma_2 = \hat{e}(aP, bP) = \hat{e}(P, P)^{ab}$; then $cP = abP$ if and only if $\gamma_1 = \gamma_2$.

3. Protocols

This section presents three fundamental pairing-based protocols. There are many other examples of innovative applications of pairings including short group signature schemes [**12**] and mechanisms for allowing selective searches on encrypted data [**13**].

3.1. Three-party one-round key agreement. Joux's key agreement protocol [**32**], as modified by Verheul [**53**], uses a bilinear pairing on (G_1, G_T) for which the BDHP is intractable. As depicted in Figure 3, Alice randomly selects a secret integer $a \in [1, n-1]$ and broadcasts the point aP to the other two parties. Similarly (and simultaneously), Bob and Chris broadcast the points bP and cP. After receiving bP and cP, Alice (and also Bob and Chris) can compute the shared secret $K = \hat{e}(bP, cP)^a = \hat{e}(P, P)^{abc}$. An eavesdropper who wishes to compute K is faced with the task of solving an instance of the BDHP.

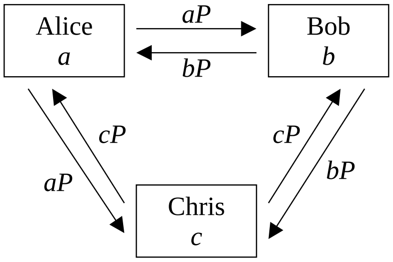


FIGURE 3. Three-party one-round key agreement protocol.

Joux's protocol can be generalized to an l-party one-round protocol by using an efficiently computable multilinear map $\hat{e}_n : G_1^{l-1} \to G_T$ for which the following analogue of the BDHP is intractable: given P, a_1P, $a_2P, \ldots, a_lP$, compute $\hat{e}_n(P, P, \ldots, P)^{a_1 a_2 \cdots a_l}$. The existence of such multilinear maps for any $l > 3$ remains an open question. In fact Boneh and Silverberg [**17**] have given some evidence that, unlike the case $l = 3$, it may not be possible to construct multilinear maps with $l > 3$ from natural maps that arise in algebraic geometry.

Joux's protocol is not interesting from a practical point of view because it is only resistant to passive attacks and needs at least one additional round of communications in order to resist active attacks. Nonetheless, it serves as an elegant example of the potential of pairings in protocol design.

3.2. Short signatures. Most discrete logarithm signature schemes such as the DSA [**22**] are variants of the ElGamal signature scheme [**21**]. In such schemes, signatures are generally comprised of a pair of integers modulo n, where n is the order of the underlying group $G_1 = \langle P \rangle$. Boneh, Lynn and Shacham (BLS) [**16**] proposed the first signature scheme in which signatures are comprised of a single group element (and where the group element can be represented using roughly the same number of bits as an integer modulo n).

The BLS short signature scheme utilizes a bilinear pairing $\hat{e}$ on (G_1, G_T) for which the DHP in G_1 is intractable. It also uses a cryptographic hash function $H : \{0,1\}^* \to G_1 \setminus \{\infty\}$. Alice's private key is a randomly selected integer $a \in [1, n-1]$, while her public key is the group element $A = aP$. Alice's signature on a message $m \in \{0,1\}^*$ is the single group element $S = aM$, where $M = H(m)$. Any party possessing Alice's public key can verify the signature by computing $M = H(m)$ and checking that (P, A, M, S) is a valid Diffie-Hellman quadruple. This is precisely an instance of the DDHP in G_1 (see §2) which the verifier can solve by checking that $\hat{e}(P, S) = \hat{e}(A, M)$.

An attacker who wishes to forge Alice's signature on a message m needs to compute $S = aM$ given P, A and $M = H(m)$. This is an instance of the DHP in G_1, which presumably is intractable.

The BLS signature scheme is very simple and has many interesting features. For example, signatures can be aggregated [**15**]. Suppose that for each i, $1 \leq i \leq t$, (m_i, S_i) is a signed message generated by party i with key pair (A_i, a_i). Suppose also that the messages are pairwise distinct. Then the aggregate signature is defined to be $S = \sum_{i=1}^{t} S_i$. A verifier who possesses the public keys A_i, the messages m_i and S, checks that $\hat{e}(P, S) = \prod_{i=1}^{t} \hat{e}(A_i, M_i)$, where $M_i = H(m_i)$, and thereby obtains the assurance that each m_i was signed by party i. The BLS signature scheme has also been used to design protocols for threshold, multisignature and blind signatures [**11**].

3.3. Identity-based encryption. When using public-key encryption to send a message securely to Alice, Bob encrypts the message using Alice's public key. Alice then uses her corresponding private key to decrypt. Bob should be certain that he possesses an authentic copy of Alice's public key because otherwise an attacker could induce Bob to use the attacker's public key, and would thereafter be able to decrypt Bob's messages that were intended only for Alice.

Large-scale deployments of public-key cryptography generally employ the services of a certifying authority (CA) who is responsible for generating *certificates* for public keys. Such a certificate for Alice would consist of Alice's identifying information and her public key, together with the CA's signature on this data. Any party who possesses an authentic copy of the CA's public key can verify the signature contained in the certificate, and thereby be assured of the authenticity of Alice's public key.

Although the notion of a certificate is very simple, there are many practical difficulties with managing certificates. For example, Bob may not know how to obtain Alice's certificate. Also, Bob should have the assurance that Alice's public key is still valid, i.e., her certificate has not been revoked by the CA on account of Alice having left her place of employment, or because her private key has somehow been compromised.

In 1984, Shamir [**51**] introduced the notion of identity-based cryptography to alleviate many of the problems inherent with managing certificates. Shamir proposed that Alice's public key consist of her identifying information ID_A (such as Alice's email address). A trusted third party (TTP) would use its private key to generate Alice's private key from ID_A and securely transmit it to Alice. Any other party Bob could encrypt messages for Alice using only ID_A and the TTP's public key. Notice that, unlike the case with traditional certificate-based encryption schemes, Bob can encrypt a message for Alice even before Alice has generated a key pair. In fact, Bob could include in ID_A any set of conditions that should be met before the TTP issues the private key. Such conditions could include a credit rating, employment status, or a minimum age requirement. In this way the TTP acts as a policy enforcer. The key revocation problem inherent with traditional certificates can be circumvented by including a date in ID_A; the TTP would only give Alice the corresponding private key if it has not been revoked by that date.

In 2001, Boneh and Franklin [**14**] proposed the first practical identity-based encryption scheme. Their scheme employs a bilinear pairing $\hat{e}$ on (G_1, G_T) for which the BDHP is intractable. It also uses two cryptographic hash functions

$H_1 : \{0,1\}^* \to G_1 \setminus \{\infty\}$ and $H_2 : G_T \to \{0,1\}^l$, where l is the bitlength of the plaintext. The TTP's private key is a randomly selected integer $t \in [1, n-1]$, and its public key is $T = tP$. It is assumed that all parties are able to obtain an authentic copy of T. When Alice requests her private key d_A, the TTP creates Alice's identity string ID_A, computes $d_A = tH_1(\mathrm{ID}_A)$, and securely delivers d_A to Alice. Notice that d_A can be considered as the TTP's BLS signature on the message ID_A.

To encrypt a message $m \in \{0,1\}^l$ for Alice using the basic Boneh-Franklin scheme, Bob computes $Q_A = H_1(\mathrm{ID}_A)$, selects a random integer $r \in [1, n-1]$, and computes $R = rP$ and $c = m \oplus H_2(\hat{e}(Q_A, T)^r)$. Bob then transmits the ciphertext (R, c) to Alice. To decrypt, Alice uses her private key d_A to compute $m = c \oplus H_2(\hat{e}(d_A, R))$. Decryption works because

$$\hat{e}(d_A, R) = \hat{e}(tQ_A, rP) = \hat{e}(Q_A, tP)^r = \hat{e}(Q_A, T)^r.$$

An eavesdropper who wishes to recover m from (R, c) must compute $\hat{e}(Q_A, T)^r$ given (P, Q_A, T, R); this is precisely an instance of the BDHP.

While secure against eavesdroppers, the basic encryption scheme is not resistant to chosen-ciphertext attacks where the attacker, who is trying to learn some information about the plaintext that corresponds to a target ciphertext, is able to obtain the decryption of any ciphertext of its choice (except for the target ciphertext). Given a target ciphertext (R, c), the attacker can simply flip the first bit of c to get c', and thereafter obtain the decryption m' of the modified ciphertext (R, c'). She then flips the first bit of m' to recover m.

Resistance to chosen-ciphertext attacks can be achieved by modifying the basic scheme as follows. In addition to H_1 and H_2, two hash function $H_3 : \{0,1\}^* \to [1, n-1]$ and $H_4 : \{0,1\}^l \to \{0,1\}^l$ are employed. To encrypt m, Bob randomly selects a bitstring $\sigma \in \{0,1\}^l$ and computes $g = \hat{e}(Q_A, T)$, $r = H_3(\sigma, m)$, $R = rP$, $c_1 = \sigma \oplus H_2(g^r)$, and $c_2 = m \oplus H_4(\sigma)$. The ciphertext is (R, c_1, c_2). To decrypt, Alice computes $g^r = \hat{e}(d_A, R)$, $\sigma = c_1 \oplus H_2(g^r)$, $m = c_2 \oplus H_4(\sigma)$, and $r = H_3(\sigma, m)$. Alice accepts the plaintext m provided that $R = rP$. Note that the attack described in the previous paragraph fails because of the integrity check on R.

As mentioned above, identity-based encryption schemes have several advantages over traditional certificate-based systems. However, there are some drawbacks such as the necessity of a secure channel for the transmission of private keys and the need for a TTP who has the ability to generate all private keys. A detailed comparison of the relative benefits and drawbacks of identity-based and certificate-based systems can be found in [**46**].

4. Elliptic curves

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{4.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$. The set $E(K)$ of K-rational points consists of the point at infinity ∞ and the points $(x, y) \in K \times K$ that satisfy (4.1). Suppose now that K is the finite field $\mathbb{F}_q$ of order q and characteristic p. Hasse's theorem gives tight bounds for the cardinality of $E(K)$:

$$(\sqrt{q} - 1)^2 \le \#E(K) \le (\sqrt{q} + 1)^2.$$

Hence we can write $\#E(K) = q + 1 - t$ where $|t| \leq 2\sqrt{q}$. If $p \mid t$ then E is said to be *supersingular*; otherwise E is *ordinary*. If $|t| \leq 2\sqrt{q}$ and $p \nmid t$, then there exists an elliptic curve E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$. In fact, if q is prime then for each t, $|t| < 2\sqrt{q}$, there exists an elliptic curve E defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = q + 1 - t$.

If $p > 3$, then a linear change of variables transforms equation (4.1) into the simpler form

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

where $a, b \in K$ and $4a^3 + 27b^2 \neq 0$. The following are two other simplified equations that will be considered later. If E is supersingular and $p = 3$, then (4.1) simplifies to

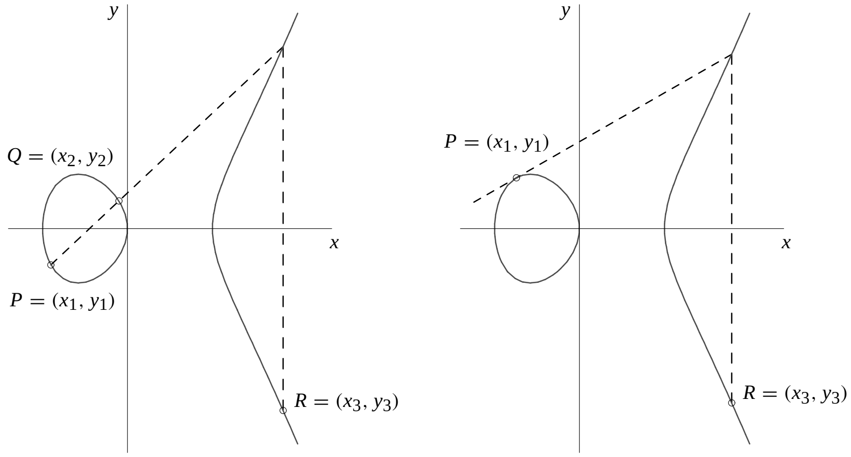
$$y^2 = x^3 + ax + b$$

where $a, b \in K$ and $b \neq 0$. If E is supersingular and $p = 2$, then (4.1) simplifies to

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

where $a, b, c \in K$ and $c \neq 0$.

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 as 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 $P, Q \in E(K) \setminus \{\infty\}$ with $P \neq \pm Q$, then $P + Q$ is defined to be R where $-R$ is the third point of intersection of the line through P and Q with the curve. The group law is depicted in Figure 4 for the elliptic curve $y^2 = x^3 - x$ over the real numbers.



(a) Addition: $P + Q = R$.

(b) Doubling: $P + P = R$.

FIGURE 4. Geometric addition and doubling of elliptic curve points.

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

Now, let $P \in E(K)$ be a point of prime order n, and suppose that $\gcd(n, q) = 1$. The elliptic curve discrete logarithm problem (ECDLP) in $\langle P \rangle$ is the following: given P and $Q \in \langle P \rangle$, find the integer l such that $Q = lP$. The best generic algorithm known for solving the ECDLP is Pollard's rho method [**47**] which has an expected running time of $O(\sqrt{n})$. If $n \approx q$, as should be the case if one wishes to maximize resistance to Pollard's rho method for a fixed field $\mathbb{F}_q$, then the running time is fully exponential in $\log q$. However, there may be other discrete log solvers that are faster for certain families of elliptic curves. In particular, it was shown in the early 1990s [**24, 39**] that the 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 defined as follows.

Definition 4.1. Let E be an elliptic curve defined over $\mathbb{F}_q$, and let $P \in E(\mathbb{F}_q)$ be a point of prime order n. Suppose that $\gcd(n, q) = 1$. Then the *embedding degree* of $\langle P \rangle$ is the smallest positive integer k such that $n \mid q^k - 1$.

If the embedding degree k is small, then there is the possibility that the known subexponential-time index-calculus algorithms (e.g., [**1, 18, 29**]) for solving the DLP in $\mathbb{F}_{q^k}$ are faster than Pollard's rho method for solving the ECDLP in $\langle P \rangle$. This is indeed the case for all supersingular curves since $k \in \{1, 2, 3, 4, 6\}$ for these curves. However, one can expect that $k \approx n$ for most elliptic curves (and this was proven to be the case for elliptic curves of prime order over prime fields [**5**]), and thus for most elliptic curves the ECDLP is not vulnerable to the Weil and Tate pairing attacks.

Following the discovery of these attacks in the early 1990s, the consensus was that elliptic curves with low embedding degrees should not be used in discrete log protocols. In fact many standards for elliptic curve cryptography such as ANSI X9.62 [**3**] explicitly forbid the use of such curves. However, low-embedding degree elliptic curves are now very much back in vogue since they are crucial for the efficient realization of the pairing-based protocols that were presented in §3. In §5 we define the Tate pairing for elliptic curves and show how it can be used to design bilinear pairings that meet the requirements of §2. Techniques for finding suitable elliptic curves of low embedding degree are presented in §6.

5. Tate pairing

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

A divisor on E is a formal sum of points $D = \sum_{P \in E} n_P(P)$, where the n_P are integers only a finite number of which are nonzero. The support of D is the set of points $P \in E$ for which $n_P \neq 0$. The divisor D is called a zero divisor if $\sum_{P \in E} n_P = 0$. D is said to be defined over K if $D^\sigma = \sum_P n_P(P^\sigma) = D$ for all automorphisms σ of $\overline{K}$ over K, where $P^\sigma = (\sigma(x), \sigma(y))$ if $P = (x, y)$, and $\infty^\sigma = \infty$. The set of all divisors that are defined over K is denoted by $\mathrm{Div}_K(E)$.

The function field of E over K is the field of fractions $K(E)$ of $K[x, y]/(r(x, y))$. The divisor of a function $f \in K(E)$ is $\mathrm{div}(f) = \sum_{P \in E} m_P(P)$, where m_P is the multiplicity of P as a root of f. Note that $\mathrm{div}(f)$ determines f up to multiplication by a nonzero field element. The divisors of functions are called principal divisors. The following result characterizes principal divisors.

Theorem 5.1. *A divisor $D = \sum_{P \in E} n_P(P)$ is principal if and only if*

$$\sum_{P \in E} n_P = 0 \quad \textit{and} \quad \sum_{P \in E} n_P P = \infty.$$

Two divisors $D_1, D_2 \in \mathrm{Div}_K(E)$ are said to be equivalent, written $D_1 \sim D_2$, if $D_1 = D_2 + \mathrm{div}(f)$ for some $f \in K(E)$. Let $f \in K(E)$ and $D = \sum n_P(P) \in \mathrm{Div}_K(E)$ be such that $\mathrm{div}(f)$ and D have disjoint support. Then $f(D)$ is defined to be $\prod_{P \in E} f(P)^{n_P}$; note that $f(D)$ is a nonzero element of K.

5.1. Tate pairing definition. Suppose that $\#E(\mathbb{F}_q) = hn$ where n is a prime such that $\gcd(n, q) = 1$. Let k be the smallest positive integer such that $n \mid q^k - 1$. The set of all points $P \in E(\overline{K})$ satisfying $nP = \infty$ is denoted by $E[n]$; it is known that $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$. By μ_n we denote the order-n subgroup of $\mathbb{F}_{q^k}^*$.

We make some further assumptions that will simplify our description of the Tate pairing. We first assume that $n \nmid q - 1$, and so $k > 1$. A result of Balasubramanian and Koblitz [**5**] tells us that $E[n] \subseteq E(\mathbb{F}_{q^k})$, and hence $n^2 \mid \#E(\mathbb{F}_{q^k})$. We further assume that $\gcd(n, h) = 1$ and that $n \nmid \#E(\mathbb{F}_{q^k})/n^2$.

The (modified) Tate pairing is a map

$$e : E[n] \times E[n] \to \mu_n$$

defined as follows. Let $P, Q \in E[n]$. Let f_P be a function with $\mathrm{div}(f_P) = n(P) - n(\infty)$, i.e., f_P has a zero of order n at P, a pole of order n at ∞, and no other zeros and poles. (The existence of f_P is guaranteed by Theorem 5.1.) Let $R \in E[n]$ such that $R \notin \{\infty, P, -Q, P - Q\}$, and let $D_Q = (Q + R) - (R)$. Note that the choice of R ensures that D_Q and $\mathrm{div}(f_P)$ have disjoint support. Then

$$e(P, Q) = f_P(D_Q)^{(q^k-1)/n} = \left(\frac{f_P(Q + R)}{f_P(R)}\right)^{(q^k-1)/n}. \tag{5.1}$$

The Tate pairing is well defined, i.e., the value $e(P, Q)$ does not depend on the choice of function f_P and point R. Moreover, it is bilinear and non-degenerate.

5.2. Miller's algorithm. We next describe Miller's algorithm [**40**] for computing the Tate pairing. The crucial ingredient of the algorithm is a procedure for determining, given $P \in E[n]$, a function f_P with divisor $n(P) - n(\infty)$.

For each $i \geq 1$, let f_i be a function whose divisor is

$$\mathrm{div}(f_i) = i(P) - (iP) - (i - 1)(\infty).$$

Note that $f_1 = 1$ and $f_n = f_P$. The following result enables the efficient computation of f_n.

LEMMA 5.2. *Let $P \in E[n]$, and let i and j be positive integers. Let l be the line through iP and jP, and let v be the vertical line through $iP + jP$. Then*

$$f_{i+j} = f_i f_j \frac{l}{v}. \tag{5.2}$$

PROOF. The divisors of the lines l and v encode the definition of the group law for E (cf. Figure 4). We have

$$\begin{aligned}
\mathrm{div}(f_i f_j \frac{l}{v}) &= \mathrm{div}(f_i) + \mathrm{div}(f_j) + \mathrm{div}(l) - \mathrm{div}(v) \\
&= \{i(P) - (iP) - (i-1)(\infty)\} + \{j(P) - (jP) - (j-1)(\infty)\} \\
&\quad + \{(iP) + (jP) + (-(i+j)P) - 3(\infty)\} \\
&\quad - \{((i+j)P) + (-(i+j)P) - 2(\infty)\} \\
&= (i+j)(P) - ((i+j)P) - (i+j-1)(\infty) \\
&= \mathrm{div}(f_{i+j}).
\end{aligned}$$

□

Let $n = (n_t, \ldots, n_1, n_0)_2$ be the binary representation of n. The function f_P can be efficiently computed by a left-to-right double-and-add method. Suppose that after the leftmost $t-u$ bits of n have been examined, one has computed f_m where $m = (n_t, n_{t-1}, \ldots, n_{u+1})_2$. One then computes f_{2m} using (5.2) with $i = j = m$. Furthermore, if $n_u = 1$, then one computes f_{2m+1} using (5.2) with $i = 2m$ and $j = 1$. After $t+1$ iterations, f_P will have been computed.

When evaluating the Tate pairing (5.1), one only needs the values of f_P at the points $Q+R$ and R. Thus, only the values of the intermediate functions f_i at these points are computed. Miller's algorithm for computing $e(P,Q)$ where $P, Q \in E[n]$ is the following.

```
(1) Let the binary representation of $n$ be $n = (n_t, \ldots, n_1, n_0)_2$.
(2) Select a point $R \in E[n] \setminus \{\infty, P, -Q, P-Q\}$.
(3) Set $f \leftarrow 1$, $T \leftarrow P$.
(4) For $i$ from $t$ down to 0 do:
    (a) Let $l$ be the tangent line through $T$, and let $v$ be the vertical line through $2T$.
    (b) $T \leftarrow 2T$.
    (c) $f \leftarrow f^2 \cdot \frac{l(Q+R)}{v(Q+R)} \cdot \frac{v(R)}{l(R)}$.
    (d) If $n_i = 1$ then
        (i) Let $l$ be the line through $T$ and $P$, and let $v$ be the vertical line through $T+P$.
        (ii) $T \leftarrow T + P$.
        (iii) $f \leftarrow f \cdot \frac{l(Q+R)}{v(Q+R)} \cdot \frac{v(R)}{l(R)}$.
(5) Return($f^{(q^k-1)/n}$).
```

Miller's algorithm may fail if one of the intermediate lines l or v has a zero at $Q+R$ or R. However, this is not a concern in pairing-based protocols because one generally has $P \in E(\mathbb{F}_q)$ and $Q \notin E(\mathbb{F}_q)$. In this case, the zeros of l and v are all in $\langle P \rangle \subseteq E(\mathbb{F}_q)$ and hence selecting $R \in E[n] \setminus E(\mathbb{F}_q)$ ensures that l and v do not have zeros at $Q+R$ or R.

Miller's algorithm has $O(\log n)$ iterations, each requiring a constant number of arithmetic operations in $\mathbb{F}_{q^k}$. Several improvements have been proposed that significantly reduce the operation count (e.g., see [**7, 26, 8**]), as a result of which pairing-based protocols can now be implemented to meet the performance demands of most applications.

5.3. Bilinear pairings from the Tate pairing. Although the Tate pairing is bilinear, non-degenerate and efficiently computable, it does not satisfy Definition 2.1 since $E[n]$ is not a (cyclic) group of order n. This deficiency can be remedied in two ways.

If E is supersingular and $k > 1$, then one selects a point $P \in E(\mathbb{F}_q)$ of order n and an endomorphism $\Psi : E \to E$ for which $\Psi(P) \notin \langle P \rangle$. Then $\hat{e} : \langle P \rangle \times \langle P \rangle \to \mu_n$ defined by $\hat{e}(Q,R) = e(Q, \Psi(R))$ satisfies $\hat{e}(P,P) \neq 1$ [**25**, Lemma IX.14]. Thus $\hat{e}$ is a bilinear pairing on $(\langle P \rangle, \mu_n)$ in the sense of Definition 2.1. Ψ is called a distortion map.

If E is ordinary and $k > 1$, then no such distortion map exists [**53**]. Instead one selects order-n points $P \in E(\mathbb{F}_q)$ and $Q \notin E(\mathbb{F}_q)$ and defines $\hat{e} : \langle P \rangle \times \langle Q \rangle \to \mu_n$

by $\hat{e}(R,S) = e(R,S)$. This restriction of the Tate pairing is a non-degenerate asymmetric bilinear pairing $\hat{e} : G_1 \times G_2 \to G_T$, where $G_1 = \langle P\rangle$, $G_2 = \langle Q\rangle$, $G_T = \mu_n$ are cyclic groups of order n. The protocols described in §3 can be modified to use these kinds of pairings instead of the symmetric pairings of Definition 2.1.

6. 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 $\mathbb{F}_q$, n is a prime divisor of $\#E(\mathbb{F}_q)$ such that $\gcd(n,q) = 1$, and k is the smallest positive integer such $n \mid q^k - 1$. The parameters q, n and k should satisfy the following conditions:

(1) n should be sufficiently large so that Pollard's rho method for computing discrete logarithms in an order-n subgroup of $E(\mathbb{F}_q)$ is infeasible.
(2) k should be sufficiently large so that the index-calculus methods for solving the DLP in $\mathbb{F}_{q^k}$ are infeasible.
(3) k should be small enough so that arithmetic in $\mathbb{F}_{q^k}$ can be efficiently performed.

For example, if an 80-bit security level is desired then one should select $n \approx 2^{160}$ and $q^k \approx 2^{1024}$. For an 128-bit security level, one should select $n \approx 2^{256}$ and $q^k \approx 2^{3072}$. Some other conditions may be imposed on the elliptic curve parameters in order to accelerate the computation of the Tate pairing, e.g., one might require that n have low Hamming weight so that most of the doubling operations (step 4(d)) in Miller's algorithm are eliminated.

As mentioned 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 elliptic curves that are suitable for pairing applications are described in §6.1. In §6.2 we present three methods for generating suitable ordinary curves.

6.1. Supersingular curves.

Recall that the embedding degree k for a supersingular elliptic curve E satisfies $k \in \{1,2,3,4,6\}$. If E is defined over a prime field $\mathbb{F}_q$ with $q > 3$, then $k = 1$ or $k = 2$. All supersingular 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 $k = 4$ and $k = 6$ supersingular curves are studied in this section. The next result is useful for determining group orders.

THEOREM 6.1 ([**52**, §V.2]). *Let E be an elliptic curve defined over $\mathbb{F}_q$, and let $t = q + 1 - \#E(\mathbb{F}_q)$. Let α, β be the complex roots of $T^2 - tT + q \in \mathbb{Z}[T]$. Then $\#E(\mathbb{F}_{q^m}) = q^m + 1 - \alpha^m - \beta^m$ for all $m \geq 1$.*

6.1.1. *Supersingular curves with $k = 4$.* Consider the supersingular elliptic curve

$$E_1 : y^2 + y = x^3 + x + 1$$

defined over $\mathbb{F}_2$. One can check that $\#E_1(\mathbb{F}_2) = 1$. Let $q = 2^m$ and $i = \sqrt{-1}$. Using Theorem 6.1 one can deduce that

$$\begin{aligned} \#E_1(\mathbb{F}_{2^m}) &= 2^m + 1 - (1+i)^m - (1-i)^m \text{ for all } m \geq 1 \\ &= \begin{cases} q+1-2\sqrt{q}, & \text{if } m \equiv 0 \pmod 8, \\ q+1-\sqrt{2q}, & \text{if } m \equiv \pm 1 \pmod 8, \\ q+1, & \text{if } m \equiv \pm 2 \pmod 8, \\ q+1+\sqrt{2q}, & \text{if } m \equiv \pm 3 \pmod 8, \\ q+1+2\sqrt{q}, & \text{if } m \equiv 4 \pmod 8). \end{cases} \end{aligned}$$

Suppose now that m is odd, and let n be a prime divisor of $\#E_1(\mathbb{F}_q) = q+1 \pm \sqrt{2q}$. Since

$$q^2 + 1 = (q+1-\sqrt{2q})(q+1+\sqrt{2q}),$$

we have $n \mid q^2+1$ and hence $n \mid q^4 - 1$. Furthermore, since $n \mid q^2+1$ and n is odd, we have $n \nmid q^2 - 1$ and hence $n \nmid q - 1$. Also, $n \nmid q^2 + q + 1$ and thus $n \nmid (q^3 - 1) = (q-1)(q^2+q+1)$. It follows that the embedding degree of any prime-order subgroup of $E_1(\mathbb{F}_q)$ is $k = 4$.

The map $\Psi : E_1 \to E_1$ defined by

$$\Psi : (x, y) \mapsto (x + s^2, y + sx + t),$$

where $s, t \in \mathbb{F}_{2^{4m}}$, $s^4 = s$, and $t^2 + t = s^6 + s^2$, is a distortion map. Hence, if $P \in E_1(\mathbb{F}_{2^m})$ is a point of order n, then the map $\hat{e} : \langle P \rangle \times \langle P \rangle \to \mu_n$ defined by $\hat{e}(Q, R) = e(Q, \Psi(R))$ is a bilinear pairing that is suitable for implementing the protocols described in §3. Some values of m for which $\#E_1(\mathbb{F}_{2^m})$ is prime are $m = 239$, 283, 367 and 457.

Similarly, one can show that the supersingular elliptic curve

$$E_2 : y^2 + y = x^3 + x$$

defined over $\mathbb{F}_2$ has the property that any prime-order subgroup of $E_2(\mathbb{F}_{2^m})$ with m odd has embedding degree $k = 4$, and the distortion map Ψ can be used to define a bilinear pairing as above.

6.1.2. *Supersingular curves with* $k = 6$. Consider the supersingular elliptic curve

$$E_3 : y^2 = x^3 - x - 1$$

defined over $\mathbb{F}_3$. One can verify using Theorem 6.1 that $\#E_3(\mathbb{F}_{3^m}) = 3^m + 1 + 3^{(m+1)/2}$ if $m \equiv \pm 5 \pmod{12}$, and $\#E_3(\mathbb{F}_{3^m}) = 3^m + 1 - 3^{(m+1)/2}$ if $m \equiv \pm 1 \pmod{12}$. Furthermore, the embedding degree of any prime-order subgroup of $E_3(\mathbb{F}_{3^m})$ is $k = 6$. The map $\Omega : E_3 \to E_3$ defined by

$$\Omega : (x, y) \mapsto (-x + r, iy),$$

where $r, i \in \mathbb{F}_{3^{6m}}$, $i^2 = -1$, and $r^3 - r = -1$, is a distortion map. Some values of m for which $\#E_3(\mathbb{F}_{3^m})$ is prime are $m = 163$, 193, 239, 317 and 353.

Similarly, one can show that the supersingular elliptic curve

$$E_4 : y^2 = x^3 - x + 1$$

defined over $\mathbb{F}_3$ has the property that any prime-order subgroup of $E_4(\mathbb{F}_{3^m})$ with $m \equiv \pm 1 \pmod 6$ has embedding degree $k = 6$, and Ω (with $r^3 - r = 1$) is a distortion map.

6.2. Ordinary curves. We begin by establishing a condition that the embedding degree must satisfy. Recall that if k is a positive integer and $\omega = e^{2\pi i/k} \in \mathbb{C}$, the kth cyclotomic polynomial is

$$\Phi_k(X) = \prod_{\substack{1 \le i \le k \\ \gcd(i,k)=1}} (X - \omega^i) \in \mathbb{Z}[X].$$

The first six cyclotomic polynomials are $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_3(X) = X^2 + X + 1$, $\Phi_4(X) = X^2 + 1$, $\Phi_5(X) = X^4 + X^3 + X^2 + X + 1$, and $\Phi_6(X) = X^2 - X + 1$. The factorization of $X^k - 1$ into irreducible polynomials over $\mathbb{Z}$ is

$$X^k - 1 = \prod_{d|k} \Phi_d(X).$$

LEMMA 6.2. *Let n and q be primes such that $n \mid \Phi_k(q)$ and $n \nmid k$. Then $n \nmid q^d - 1$ for each $1 \le d \le k - 1$.*

PROOF. Let $f(X) = X^k - 1$, and let $\mathbb{F}$ be the field of integers modulo n. Since $n \nmid k$, we have $\gcd(f(X), f'(X)) = 1$ in $\mathbb{F}[X]$, and hence $f(X)$ does not have any repeated roots in $\mathbb{F}$. Thus, since q is a root of $\Phi_k(X)$ over $\mathbb{F}$, $\Phi_d(q) \not\equiv 0 \pmod{n}$ for each proper divisor d of k, from which it follows that $n \nmid q^d - 1$ for each proper divisor d of k. Finally, if $d \in [1, k-1]$ is not a divisor of k, then $n \nmid q^d - 1$ because otherwise $n \mid q^e - 1$ where $e = \gcd(d, k)$ is a proper divisor of k. □

6.2.1. *Complex multiplication method.* All known techniques for generating ordinary elliptic curves with low embedding degree use the complex multiplication (CM) method.

Let q be a prime, and let t be a nonzero integer satisfying $|t| < 2\sqrt{q}$. The CM norm equation is

$$t^2 - 4q = -DV^2, \tag{6.1}$$

where the *discriminant* D is positive and squarefree if t is odd, and $D = 4d$ with d positive and squarefree if t is even. The *complex multiplication method* [**4, 43**] is an algorithm for finding an elliptic curve E over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = N = q + 1 - t$. (More precisely, the elliptic curve E has complex multiplication by an order in the imaginary quadratic number field $\mathbb{Q}(\sqrt{-D})$.) The running time of the CM method is exponential in $\log q$; however it is efficient in practice if D is relatively small (e.g., $D < 10^9$).

If $D = 3$ and N is prime, then the CM method is especially simple. Since $D = 3$, the equation for E takes the form $E_b : y^2 = x^3 + b$. All isomorphic curves are also of this form, and there are precisely 6 isomorphism classes of such curves. Thus E can be very quickly generated by selecting arbitrary $b \in \mathbb{F}_q$ until $E_b(\mathbb{F}_q)$ has a point $P \ne \infty$ that satisfies $NP = \infty$.

6.2.2. *MNT curves.* Miyaji, Nakabayashi and Takano (MNT) [**41**] were the first to describe a procedure for generating ordinary elliptic curves of low embedding degree. Their method is based on the following result.

THEOREM 6.3 ([**41**]). *Let $q > 64$ be a prime number. Let E be an ordinary elliptic curve defined over $\mathbb{F}_q$ such that $n = \#E(\mathbb{F}_q)$ is prime, and let $t = q + 1 - n$. Suppose that the embedding degree of $E(\mathbb{F}_q)$ is k.*

(i) *$k = 3$ if and only if $q = 12l^2 - 1$ and $t = -1 \pm 6l$ for some $l \in \mathbb{Z}$.*
(ii) *$k = 4$ if and only if $q = l^2 + l + 1$ and $t \in \{-l, l + 1\}$ for some $l \in \mathbb{Z}$.*

(iii) $k = 6$ *if and only if* $q = 4l^2 + 1$ *and* $t = 1 \pm 2l$ *for some* $l \in \mathbb{Z}$.

PROOF. We prove (iii) and leave the proofs of (i) and (ii) as exercises for the reader.

Suppose first that $q = 4l^2 + 1$ and $t = 1 \pm 2l$ for some integer l. Then $n = q + 1 - t = 4l^2 \mp 2l + 1$, and

$$\Phi_6(q) = q^2 - q + 1 = 16l^4 + 4l^2 + 1 = (4l^2 + 2l + 1)(4l^2 - 2l + 1).$$

Thus $n \mid \Phi_6(q)$. Since $q > 64$, it follows from Hasse's theorem that $n > 6$. Hence by Lemma 6.2 we have $k = 6$.

Suppose now that $k = 6$. Let $\Phi_6(q) = q^2 - q + 1 = \lambda n$ where $\lambda \in \mathbb{Z}$. Then

$$q^2 - q + 1 = (q + 1)^2 - t^2 + t^2 - 3q = \lambda(q + 1 - t)$$

and so

$$(q + 1 - t)(q + 1 + t - \lambda) = 3q - t^2. \tag{6.2}$$

Dividing both sides by q yields

$$\left(1 + \frac{1}{q} - \frac{t}{q}\right)(q + 1 + t - \lambda) = 3 - \frac{t^2}{q}.$$

Let $L = 1 + \frac{1}{q} - \frac{t}{q}$. The inequality $|t| < 2\sqrt{q}$ implies that $-1 < 3 - \frac{t^2}{q} < 3$. Hence

$$-1 < L(q + 1 + t - \lambda) < 3. \tag{6.3}$$

Now $L = (q + 1 - t)/q$ and so by Hasse's theorem we have

$$\frac{(\sqrt{q} - 1)^2}{q} < L < \frac{(\sqrt{q} + 1)^2}{q}.$$

Since $q > 64$, we have $\frac{49}{64} < L < \frac{81}{64}$ and it follows from (6.3) that $q + 1 + t - \lambda \in \{-1, 0, 1, 2, 3\}$. If $q+1+t-\lambda = 0$, then (6.2) simplifies to $t^2 = 3q$; this is impossible since $q > 3$ is prime. If $q + 1 + t - \lambda \in \{-1, 1, 3\}$, then reducing (6.2) modulo 2 gives $t^2 + t + 1 \equiv 0 \pmod 2$, which again is impossible. Therefore it must be the case that $q + 1 + t - \lambda = 2$, and (6.2) simplifies to $t^2 - 2t - q + 2 = 0$. The result now follows by solving for t and noting that q is odd. □

We now show how Theorem 6.3 can be used to generate ordinary elliptic curves with embedding degree $k = 6$. (The cases $k = 3$ and $k = 4$ are similar.)

The first algorithm suggested by Theorem 6.3 is to choose integers l of the appropriate size until both $q = 4l^2 + 1$ and $n = q + 1 - t = 4l^2 \mp 2l + 1$ are prime. One then writes $t^2 - 4q = -DV^2$, and uses the CM method to construct the desired elliptic curve. Unfortunately this algorithm will in general not be efficient because one expects that V is small and thus $D \approx q$. (Recall that the CM method is only efficient if D is small.) What is needed is a technique for selecting suitable t and q so that D is guaranteed to be small.

Miyaji, Nakabayashi and Takano [**41**] observed that the norm equation (6.1) with $t = 1 \pm 2l$ and $q = 4l^2 + 1$ can be written as

$$(6l \pm 1)^2 + 8 = 3DV^2.$$

Letting $U = 6l \pm 1$ yields a quadratic Diophantine equation

$$U^2 - 3DV^2 = -8. \tag{6.4}$$

Suppose that this equation has at least one integer solution. (This implies that -8 should be a quadratic residue modulo 3 and modulo D.) A solution (U, V) to an equation of the form $U^2 - 3DV^2 = c$ is associated with the real number $U + V\sqrt{3D}$. Suppose also that $3 \nmid D$. One first uses continued fractions to find the smallest integer solution (X, Y) with $X > 0$ and $Y > 0$ to the related Pell equation $X^2 - 3DY^2 = 1$; for example see [**44**, §7.8]. Then any solution (U_0, V_0) of (6.4) yields an infinite class of solutions $\{(U_j, V_j)\}$, $j \in \mathbb{Z}$, where

$$U_j + V_j\sqrt{3D} = (U_0 + V_0\sqrt{3D})(X + Y\sqrt{3D})^j.$$

The so-called fundamental solutions (U_0, V_0) can be used to describe all solutions to equation (6.4); these fundamental solutions can be found using the techniques described in [**37, 42**].

The MNT curve generation strategy is to repeatedly select small discriminants D and search for a solution (U, V) to (6.4) for which $U \equiv \pm 1 \pmod 6$ (in which case $l = (U \mp 1)/6$) and $q = 4l^2 + 1$ and $n = 4l^2 \mp 2l + 1$ are primes of the desired size. Then an elliptic curve E with $k = 6$ can be efficiently constructed with the CM method. Luca and Shparlinski [**36**] (see also [**33**]) showed that MNT curves are very rare. Nonetheless, it appears that the MNT curve generation method can be successful in practice.

6.2.3. *BN curves.* In 2005, Barreto and Naehrig (BN) [**9**] discovered the following elegant method for constructing elliptic curves E of prime order n over prime fields $\mathbb{F}_q$ with embedding degree $k = 12$.

Let $t = q + 1 - n$, so $q \equiv t - 1 \pmod n$. Since $k = 12$, we have $n \mid \Phi_{12}(q)$, and hence $\Phi_{12}(t - 1) \equiv 0 \pmod n$; here $\Phi_{12}(X) = X^4 - X^2 + 1$. Barreto and Naehrig observed that if $t(z) = 6z^2 + 1$, then

$$\Phi_{12}(t(z) - 1) = (36z^4 + 36z^3 + 18z^2 + 6z + 1)(36z^4 - 36z^3 + 18z^2 - 6z + 1).$$

Setting $n(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1$, we have

$$q(z) = n(z) + t(z) - 1 = 36z^4 + 36z^3 + 24z^2 + 6z + 1$$

and the CM norm equation (6.1) becomes

$$t(z)^2 - 4q(z) = -3(1 + 4z + 6z^2)^2. \tag{6.5}$$

Note that the square-free part of (6.5) is $D = 3$.

A BN curve can be constructed by selecting integers z of the appropriate size until both $q(z)$ and $n(z)$ are prime. Then the CM method with $D = 3$ (see §6.2.1) can be used to generate the desired elliptic curve.

EXAMPLE 6.4. $q(7) = 100003$ and $n(7) = 99709$ are both prime. The elliptic curve $E : y^2 = x^3 + 37$ satisfies $\#E(\mathbb{F}_q) = n$, and $P = (1, 11498)$ is a point of order n. One can check that $n \mid \Phi_{12}(q)$, and so the embedding degree of $E(\mathbb{F}_q)$ is $k = 12$.

6.2.4. *Cocks-Pinch method.* Cocks and Pinch (see §IX.15.2 of [**25**]) described a method for generating elliptic curves for any embedding degree. In their method, which is based on the following lemma, one first selects an embedding degree k, point order n, and discriminant D (subject to some mild conditions), and subsequently determines a prime q such that the existence of an elliptic curve over $\mathbb{F}_q$ having the chosen values for k, n and D is guaranteed. The desired elliptic curves can then be constructed using the CM method.

LEMMA 6.5. *Let k be a positive integer, and $n \equiv 1 \pmod{k}$ a prime. Let $D > 0$ be a squarefree integer such that $D \equiv 3 \pmod{4}$ and $-D$ is a square modulo n. Let g be a primitive kth root of unity modulo n, and let $a = 2^{-1}g \bmod n$ and $t = 2a + 1$. Let $V_0 = \pm(t-2)/\sqrt{-D} \bmod n$, and let $j \geq 0$ be an integer such that $q = (t^2 + D(V_0 + jn)^2)/4$ is prime. (To ensure that q is an integer, j should be even if V_0 is odd, and odd otherwise.) Then there exists an elliptic curve E defined over $\mathbb{F}_q$ satisfying:*

(i) *$n \mid \#E(\mathbb{F}_q)$;*
(ii) *the norm equation is $t^2 - 4q = -D(V_0 + jn)^2$; and*
(iii) *the order-n subgroup of $E(\mathbb{F}_q)$ has embedding degree k.*

PROOF. Let $N = q + 1 - t$. We first note that an elliptic curve E defined over $\mathbb{F}_q$ with $\#E(\mathbb{F}_q) = N$ exists by Hasse's theorem since

$$q \geq \frac{t^2 + DV_0^2}{4} \geq \frac{t^2}{4}.$$

Now, $n \mid \#E(\mathbb{F}_q)$ since

$$\begin{aligned} 4N &= 4(q+1-t) = t^2 + D(V_0 + jn)^2 + 4 - 4t \\ &\equiv t^2 + D\frac{(t-2)^2}{-D} + 4 - 4t \equiv 0 \pmod{n}. \end{aligned}$$

Statement (ii) about the norm equation is immediate. Finally, $t - 1 = 2a \equiv g \pmod{n}$, whence $\Phi_k(t-1) \equiv 0 \pmod{n}$. Since $q \equiv t - 1 \pmod{n}$, it follows that $\Phi_k(q) \equiv 0 \pmod{n}$ and therefore the embedding degree of the order-n subgroup of $E(\mathbb{F}_q)$ is k. □

By trying different values for n, D and g, one can expect to quickly find an elliptic curve with the desired embedding degree. Note that n can be selected to have low Hamming weight, which accelerates Tate pairing computations. Note also that since $V_0 \approx n$, one expects the bitlength of q to be at least twice that of n.

EXAMPLE 6.6. We select $n = 100003$, $k = 21$, $D = 3$ and $g = 96699$. Then $t = 196703$ and $V_0 = (t-2)/\sqrt{-D} \bmod n = 88367$. For $j = 2$,

$$q = (t^2 + D(V_0 + jn)^2)/4 = 72042257899$$

is prime. The elliptic curve $E : y^2 = x^3 + 6$ has order

$$N = q + 1 - t = 72042061197 = 3 \cdot 439 \cdot 547 \cdot 100003.$$

One can check that $P = (46359640528, 5962208999) \in E(\mathbb{F}_q)$ has order n. Finally, $n \mid \Phi_{21}(q)$, and so the embedding degree of $\langle P \rangle$ is $k = 21$.

7. Concluding remarks

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; see [**23**] for a comprehensive survey. The fastest algorithms [**6, 31, 35**] for computing the Tate pairing (and its variants) on these curves have fast implementations on software [**2, 19, 30, 50**] and hardware [**48**] platforms, and are competitive with the exponentiation algorithms that are used in traditional discrete logarithm cryptography. Two areas that deserve further investigation are the practicality of implementing various pairing-based protocols at high security levels (see [**34**]), and the hardness of the BDHP and related problems.

Researchers are also actively investigating the suitability of hyperelliptic curves and other abelian varieties (see [**49, 6, 28, 27**]). Research in pairing-based cryptography will continue to flourish in the coming years, and especially so if protocols such as identity-based encryption see widespread commercial deployment.

References

1. L. Adleman and M. Huang, "Function field sieve methods for discrete logarithms over finite fields", *Information and Computation*, 151 (1999), 5–16.
2. O. Ahmadi, D. Hankerson and A. Menezes, "Software implementation of arithmetic in $\mathbb{F}_{3^m}$", *International Workshop on Arithmetic of Finite Fields (WAIFI 2007)*, Lecture Notes in Computer Science 4547 (2007), 85–102.
3. ANSI X9.62, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, American National Standards Institute, 1999.
4. A. Atkin and F. Morain, "Elliptic curves and primality proving", *Mathematics of Computation*, 61 (1993), 29–68.
5. 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 (1998) 141–145.
6. P. Barreto, S. Galbraith, C. Ó hÉigeartaigh, and M. Scott, "Efficient pairing computation on supersingular abelian varieties", *Designs, Codes and Cryptography*, 42 (2007), 239–271.
7. P. Barreto, H. Kim, B. Lynn and M. Scott, "Efficient algorithms for pairing-based cryptosystems", *Advances in Cryptology – CRYPTO 2002*, Lecture Notes in Computer Science, 2442 (2002), 354–368.
8. P. Barreto, B. Lynn and M. Scott, "Efficient implementation of pairing-based cryptosystems", *Journal of Cryptology*, 17 (2004), 321–334.
9. P. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order", *Selected Areas in Cryptography – SAC 2005*, Lecture Notes in Computer Science, 3897 (2006), 319–331.
10. B. den Boer, "Diffie-Hellman is as strong as discrete log for certain primes", *Advances in Cryptology – CRYPTO '88*, Lecture Notes in Computer Science, 403 (1996), 530–539.
11. A. Boldyreva, "Efficient threshold signatures, multisignatures and blind signatures based on the gap-Diffie-Hellman-group signature scheme", *Public Key Cryptography – PKC 2003*, Lecture Notes in Computer Science, 2567 (2003), 31–46.
12. D. Boneh, X. Boyen and H. Shacham, "Short group signatures", *Advances in Cryptology – CRYPTO 2004*, Lecture Notes in Computer Science, 3152 (2004), 41–55.
13. D. Boneh, G. Di Crescenzo, R. Ostrovsky and G. Persiano, "Public key encryption with keyword search", *Advances in Cryptology – EUROCRYPT 2004*, Lecture Notes in Computer Science, 3027 (2004), 506–522.
14. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", *Advances in Cryptology – CRYPTO 2001*, Lecture Notes in Computer Science, 2139 (2001), 213–229. Full version: *SIAM Journal on Computing*, 32 (2003), 586–615.
15. D. Boneh, C. Gentry, H. Shacham and B. Lynn, "Aggregate and verifiably encrypted signatures from bilinear maps", *Advances in Cryptology – EUROCRYPT 2004*, Lecture Notes in Computer Science, 2656 (2003), 416–432.
16. D. Boneh, B. Lynn and H. Shacham, "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*, 17 (2004), 297–319.
17. D. Boneh and A. Silverberg, "Applications of multilinear forms to cryptography", *Contemporary Mathematics*, 324 (2003), 71–90.
18. D. Coppersmith, "Fast evaluation of logarithms in fields of characteristic two", *IEEE Transactions on Information Theory*, 30 (1984), 587–594.
19. A. Devegili, M. Scott and R. Dahab, "Implementing cryptographic pairings over Barreto-Naehrig curves", *Pairing-Based Cryptography – Pairing 2007*, Lecture Notes in Computer Science 4575 (2007), 197–207.
20. W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, 22 (1976), 644–654.
21. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, 31 (1985), 469–472.

22. FIPS 186, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186, National Institute of Standards and Technology, 1994.
23. D. Freeman, M. Scott and E. Teske, "A taxonomy of pairing-friendly elliptic curves", Cryptology ePrint Archive Report 2006/372, 2006. Available from http://eprint.iacr.org/2006/372.
24. G. Frey and H. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of Computation*, 62 (1994), 865–874.
25. S. Galbraith, "Pairings", Ch. IX of I. Blake, G. Seroussi and N. Smart, eds., *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005.
26. S. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate pairing", *Algorithmic Number Theory: 5th International Symposium, ANTS-V*, Lecture Notes in Computer Science, 2369 (2002), 324–337.
27. S. Galbraith, F. Hess and F. Vercauteren, "Hyperelliptic pairings", *Pairing-Based Cryptography – Pairing 2007*, Lecture Notes in Computer Science, 4575 (2007), 108–131.
28. S. Galbraith, J. McKee and P. Valença, "Ordinary abelian varieties having small embedding degree" *Finite Fields and Their Applications*, 13 (2007), 800–814.
29. D. Gordon, "Discrete logarithms in $GF(p)$ using the number field sieve", *SIAM Journal on Discrete Mathematics*, 6 (1993), 124–138.
30. D. Hankerson, A. Menezes and M. Scott, "Software implementation of pairings", in *Identity-Based Cryptography*, M. Joye and G. Neven, eds., IOS Press, to appear.
31. F. Hess, N. Smart and F. Vercauteren, "The eta pairing revisited", *IEEE Transactions on Information Theory*, 52 (2006), 4595–4602.
32. A. Joux, "A one round protocol for tripartite Diffie-Hellman", *Algorithmic Number Theory: 4th International Symposium, ANTS-IV*, Lecture Notes in Computer Science, 1838 (2000), 385–393. Full version: *Journal of Cryptology*, 17 (2004), 263–276.
33. K. Karabina and E. Teske, "On prime-order elliptic curves with embedding degrees k =3, 4 and 6" *Algorithmic Number Theory: 8th International Symposium, ANTS-VIII*, Lecture Notes in Computer Science, 5011 (2008), 102–117.
34. N. Koblitz and A. Menezes, "Pairing-based cryptography at high security levels", *Proceedings of the Tenth IMA International Conference on Cryptography and Coding*, Lecture Notes in Computer Science, 3796 (2005), 13–36.
35. E. Lee, H.-S. Lee and C.-M. Park, "Efficient and generalized pairing computation on abelian varieties", Cryptology ePrint Archive Report 2008/040, 2008. Available from http://eprint.iacr.org/2008/040.
36. F. Luca and I. Shparlinski, "Elliptic curves with low embedding degree", *Journal of Cryptology*, 19 (2006), 553–562.
37. K. Matthews, "The diophantine equation $x^2 - Dy^2 = N$, $D > 1$, in integers", *Expositiones Mathematicae*, 18 (2000), 323–331.
38. U. Maurer and S. Wolf, "The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms", *SIAM Journal on Computing*, 28 (1999), 1689–1731.
39. A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *IEEE Transactions on Information Theory*, 39 (1993), 1639–1646.
40. V. Miller, "The Weil pairing, and its efficient calculation", *Journal of Cryptology*, 17 (2004), 235–261.
41. A. Miyaji, M. Nakabayashi and S. Takano, "New explicit conditions of elliptic curve traces for FR-reduction", *IEICE – Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E84-A (2001), 1234–1243.
42. R. Mollin, "Simple continued fraction solutions for diophantine equations", *Expositiones Mathematicae*, 19 (2001), 55–73.
43. F. Morain, "Building cyclic elliptic curves modulo large primes", *Advances in Cryptology – EUROCRYPT '91*, Lecture Notes in Computer Science, 547 (1991), 328–336.
44. I. Niven, H. Zuckerman and H. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition, Wiley, 1991.
45. K. Paterson, "Cryptography from pairings", Ch. X of I. Blake, G. Seroussi and N. Smart, eds., *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005.
46. K. Paterson and G. Price, "A comparison between traditional public key infrastructures and identity-based cryptography", *Information Security Technical Report*, 8(3) (2003), 57–72.
47. J. Pollard, "Monte Carlo methods for index computation mod p", *Mathematics of Computation*, 32 (1978), 918–924.

48. R. Ronan, M. Keller, C. Murphy and W. Marnane, "Efficient hardware architectures for identity-based encryption", in *Identity-Based Cryptography*, M. Joye and G. Neven, eds., IOS Press, to appear.
49. K. Rubin and A. Silverberg, "Supersingular abelian varieties in cryptology", *Advances in Cryptology – CRYPTO 2002*, Lecture Notes in Computer Science, 2442 (2002), 336–353.
50. M. Scott, "Implementing cryptographic pairings", *Pairing-Based Cryptography – Pairing 2007*, Lecture Notes in Computer Science, 4575 (2007), 177–196.
51. A. Shamir, "Identity-based cryptosystems and signature schemes", *Advances in Cryptology – Proceedings of CRYPTO 84*, Lecture Notes in Computer Science, 196 (1985), 47–53.
52. J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.
53. E. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems", *Journal of Cryptology*, 17 (2004) 277–296.

Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: ajmeneze@uwaterloo.ca