Elliptic curve cryptographic systems

Andreas Enge

Elliptic curve cryptographic systems

Andreas Enge*

13 December 2012

The following text is published as Section 16.4 of [54] and reproduced here without the cross-references to other chapters of the book.

[7], [8], [16] give comprehensive accounts of elliptic curve cryptography.

1 Cryptosystems based on elliptic curve discrete logarithms

Remark 1 The $\mathbb{F}_q$-rational points on an elliptic curve E defined over a finite field $\mathbb{F}_q$ form a finite abelian group; its group order is close to q by Hasse's theorem. This group can be used to implement discrete logarithm based cryptosystems as first observed in [46, 53].

Remark 2 For reasons of efficiency, elliptic curve cryptosystems are usually implemented over prime fields $\mathbb{F}_p$ or fields $\mathbb{F}_{2^m}$ of characteristic two. Supersingular curves over fields $\mathbb{F}_{3^m}$ of characteristic three have attracted some attention in the context of pairing based cryptography, see Section 2.

1.1 Key sizes

Remark 3 To resist generic attacks on the discrete logarithm problem, elliptic curve cryptosystems are implemented in the prime order cyclic subgroup of maximal cardinality n inside $E(\mathbb{F}_q)$. For representing group elements with the minimum number of bits, it is desirable that the curve order itself be prime. Except for special cases (see Section 1.3 and [59, 61, 65]), only generic attacks are known on the elliptic curve discrete logarithm problem (ECDLP), with a running time on the order of $\sqrt{n}$. A security level of m bits, corresponding to a symmetric-key cryptosystem with 2^m keys, thus requires an order n of $2m$ bits. Extrapolating the theoretical subexponential complexity for factoring or the DLP in finite fields allows to derive heuristic security estimates for the corresponding public key cryptosystems. Several studies have been carried out in the literature, taking added heuristics on technological progress into account, see [36]. They are summarized in the following table; the figures for the factorization based RSA system essentially

*INRIA, LFANT, F-33400 Talence, France
CNRS, IMB, UMR 5251, F-33400 Talence, France
Univ. Bordeaux, IMB, UMR 5251, F-33400 Talence, France

carry over to systems based on discrete logarithms in finite fields. The 80 bit security level is a historic figure.

security (bits)	symmetric	ECC	RSA [36, 47]	RSA [56, §7.2.2.3]	RSA [67, Table 7.2]
80	—	160	1513	1536	1248
112	Triple DES	224	4509	4096	2432
128	AES-128	256	6669	6000	3248
192	AES-192	384	22089	—	7936
256	AES-256	512	49562	—	15424

1.2 Cryptographic primitives

Remark 4 Some cryptographic primitives (encryption, signatures, etc.) have been adapted and standardised specifically for elliptic curves. As other discrete logarithm based systems, they require a setup of public *domain parameters*, a cyclic subgroup G of prime order n of some curve $E(\mathbb{F}_q)$, with a fixed base point P such that $G = \langle P \rangle$. Moreover, the bit patterns representing elements of $\mathbb{F}_q$ and $E(\mathbb{F}_q)$ need to be agreed upon.

Example 5 (Elliptic Curve Integrated Encryption Scheme, ECIES) This cryptosystem is essentially the same as ElGamal's; but the encryption of elements of G is replaced by symmetric key encryption of arbitrary bit strings with a derived secret key. So the scheme is *hybrid*, using symmetric key and public key elements. An additional *message authentication code (MAC)* prevents alterations of the encrypted message during transmission and authenticates its sender. (A MAC is essentially a hash function, depending additionally on a symmetric key, and can indeed be constructed from hash functions; for more details, see [50, Subsection 9.5.2].)

Besides the domain parameters for the elliptic curve group, the setup comprises a symmetric key scheme with an encryption function E_{k_1} and inverse decryption function D_{k_1}, using keys k_1 of length ℓ_1 bits; and a message authentication code M_{k_2} using keys k_2 of length ℓ_2. Party A has the private key $a \in [0, n-1]$ and the related public key $Q = aP$.

To encrypt a message $m \in \{0,1\}^*$, party B selects a random integer $r \in [0, n-1]$, computes $R = kP$, $S = kQ$ and $(k_1, k_2) = f(S)$, where $f : G \to \{0,1\}^{\ell_1} \times \{0,1\}^{\ell_2}$ is a *key derivation function* (for instance, a cryptographic hash function). He computes $c_1 = E_{k_1}(m)$ and $c_2 = M_{k_2}(c_1)$; the ciphertext is (R, c_1, c_2).

To decrypt such a ciphertext, party A recovers $S = aR$ and $(k_1, k_2) = f(S)$. If $M_{k_1}(c_1) \neq c_2$, she rejects the ciphertext as invalid; otherwise, she obtains the clear text as $m = D_{k_1}(c_1)$.

Remark 6 The scheme has been first described in a generic discrete logarithm setting (and in a slightly different form) in [6], and standardised under the name *Elliptic Curve Augmented Encryption Scheme* in [2]. For arguments supporting its security under suitable assumptions on the underlying primitives, see [6, 66] and [8, Chapter III].

Example 7 (Elliptic Curve Digital Signature Algorithm, ECDSA) The algorithm is a simple transposition of the DSA to the elliptic curve setting.

Besides the domain parameters for the elliptic curve group, the setup comprises a hash function $H : \{0,1\}^* \to [0, n-1]$ and the reduction function $f : G \to [0, n-1]$, $(x, y) \mapsto x \pmod{n}$.

Party A has the private key $a \in [0, n-1]$ and the related public key $Q = aP$.

To sign a message m, party A randomly selects an integer $k \in [1, n-1]$, computes $R = kP$, $r = f(R)$, $h = H(m)$ and $s \equiv k^{-1}(h + ar) \pmod{n}$. The signature is the pair (r, s).

To verify such a signature, party B computes $h = H(m)$, $w \equiv s^{-1} \pmod{n}$, $u_1 \equiv wh \pmod{n}$, $u_2 \equiv wr \pmod{n}$ and $R = u_1P + u_2Q$. He accepts the signature as valid if and only if $r = f(R)$.

Remark 8 The scheme has been standardised in [1], see also [28], [42, Subsections 7.2.7–7.2.8], and [55, Section 6]. For arguments supporting its security under suitable assumptions on the underlying primitives, see [8, Chapter II] and [12]. The fact that the function f depends only on the x-coordinate of its argument has raised doubts about the security of the scheme [68]; in particular, it implies weak malleability: From a signature (r, s) on a given message, another signature $(r, -s)$ on the same message may be obtained.

1.3 Special curves

Remark 9 A necessary condition for the security of an elliptic curve cryptosystem is that the order of $E(\mathbb{F}_q)$ be prime, or a prime multiplied by a small cofactor. Some special curves for which this condition is easily tested have been suggested in the literature. These are more and more deprecated in favour of random curves (see Section 1.4) in conventional discrete logarithm settings, [13]. Supersingular and especially CM curves are still needed, however, in pairing based cryptography; see Section 2.

Example 10 (Supersingular curves) The orders of supersingular elliptic curves are known by [75]. Over $\mathbb{F}_p$, the only occurring order is $p+1$. Over $\mathbb{F}_{p^m}$ with $p \in \{2, 3\}$, the orders $p^m + 1 - t$ with $t \in \{0, \pm p^{m/2}, \pm p^{(m+1)/2}, \pm 2p^{m/2}\}$ may occur depending on the parity of m. The ECDLP on supersingular curves over $\mathbb{F}_{p^m}$ may be reduced to the DLP in the multiplicative group of $\mathbb{F}_{p^2}$ for curves over $\mathbb{F}_p$; of $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$ or $\mathbb{F}_{p^4}$ for curves over $\mathbb{F}_{2^m}$; and of $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$ or $\mathbb{F}_{p^6}$ for curves over $\mathbb{F}_{3^m}$. Thus, supersingular curves are deprecated except for low security pairing based cryptosystems.

Example 11 (Curves over extension fields) If E is defined over a finite field $\mathbb{F}_q$ with q small, then $|E(\mathbb{F}_q)|$ can be obtained by exhaustively enumerating all points; and $|E(\mathbb{F}_{q^m})|$ is easily computed. In particular, the case $q = 2$ has been suggested in the literature. However, since $E(\mathbb{F}_{q^m})$ contains the subgroup $E(\mathbb{F}_q)$ (and further subgroups if m is not prime), the group order cannot be prime any more.

Remark 12 The existence of the additional Frobenius automorphism of order m, together with the negation automorphism of order 2, may be used to speed up the generic algorithms by a factor of $\sqrt{2m}$ [32, 76], which reduces the effective security level.

Remark 13 (Weil descent) If E is defined over an extension field $\mathbb{F}_{q^m}$, then $E(\mathbb{F}_{q^m})$ can be embedded into $A(\mathbb{F}_q)$, where A is an abelian variety of dimension m, called the *Weil restriction* or *restriction of scalars* of E. There is reason to believe that the discrete logarithm problem in $A(\mathbb{F}_q)$ may be easier to solve than by a generic algorithm, relying on an approach of representing the group $A(\mathbb{F}_q)$ by a set of generators (called the *factor base*) and relations which are solved by linear algebra, leading to a potential attack described first in [27, Section 3.2]. Cases where A contains the Jacobian of a hyperelliptic curve of genus close to m have been worked out for curves over fields of characteristic 2 in [31, 33], and fields of odd characteristic in [19]. So far, the attack has been made effective for certain curves with prime $m \leqslant 7$.

Another algorithm for discrete logarithms, working directly with curves over $\mathbb{F}_{q^m}$ and specially adapted factor bases, is described in [35]; heuristically, it is faster than the generic algorithms for $m \geqslant 3$ fixed and $q \to \infty$. Since it involves expensive Gröbner basis computations, it has been made effective only for $m \leqslant 3$.

Combinations of these approaches are also possible and have led to an attack on curves of close to cryptographic size over $\mathbb{F}_{p^6}$ [43]. Moreover, isogenies may be used to transport the discrete logarithm problem from a seemingly secure curve to one that may be attacked by Weil descent [29].

It thus appears cautious to prefer for cryptographic applications curves over prime fields $\mathbb{F}_p$ or, if even characteristic leads to significant performance improvements, fields $\mathbb{F}_{2^m}$ of prime extension degree m.

Example 14 (Complex multiplication curves) All ordinary elliptic curves over a finite field $\mathbb{F}_q = \mathbb{F}_{p^m}$ have complex multiplication by some order $\mathcal{O}_D = \left[1, \frac{D+\sqrt{D}}{2}\right]_{\mathbb{Z}}$ of discriminant $D < 0$ in the imaginary-quadratic field $\mathbb{Q}(\sqrt{D})$;. For small $|D|$, this can be exploited to explicitly construct curves with a known number of points as follows.

1. Let $D < 0$, $D \equiv 0$ or $1 \pmod 4$, p prime and m minimal such that $4p^m = t^2 - v^2 D$ has a solution in integers t, v.
2. Compute the *class polynomial* $H_D \in \mathbb{Z}[X]$, the minimal polynomial of $j\left(\frac{D+\sqrt{D}}{2}\right)$, where j is the absolute elliptic modular invariant function.
3. H_D splits completely over $\mathbb{F}_{p^m}$ (and no subfield), and its roots are the j-invariants of the elliptic curves defined over $\mathbb{F}_{p^m}$ with complex multiplication by $\mathcal{O}_D$. For each such j-invariant, one easily writes down a curve with $p^m + 1 - t$ points by solving the expression of j for the curve coefficients (up to isomorphisms and twists, the solution is unique).

Remark 15 It is easy to see that a prime number of points is only possible for $D \equiv 5 \pmod 8$.

Remark 16 The degree of the class polynomial is the class number of $\mathcal{O}_D$, and its total bit size is of the order of $O(|D|^{1+\epsilon})$ under GRH. Several quasi-linear algorithms of complexity $O(|D|^{1+\epsilon})$ for computing class polynomials have been described in the literature, by floating point approximations of its roots [21], lifting to a local field [17] or Chinese remaindering [5]. Nevertheless, the algorithms are restricted to small values of $|D|$, while random curves correspond to $|D|$ of the order of q, so that only a negligible fraction of curves may be reached by the CM approach.

Remark 17 While no attack on this particular fraction of curves has been devised so far, random curves are generally preferred where possible; note, however, that pairing-based cryptosystems require the use of either supersingular curves or ordinary curves obtained with the CM approach; see Section 2.4.

Example 18 (NIST curves) The USA standard [55] suggests a prime field $\mathbb{F}_p$ and a pseudorandom curve (assuming that the hash function SHA-1 is secure) of prime order over $\mathbb{F}_p$ for p of 192, 224, 256, 384 and 521 bits. (The largest example is for the Mersenne prime $p = 2^{521} - 1$.) For the binary fields $\mathbb{F}_{2^{163}}$, $\mathbb{F}_{2^{233}}$, $\mathbb{F}_{2^{283}}$, $\mathbb{F}_{2^{409}}$ and $\mathbb{F}_{2^{571}}$, a pseudo-random curve (of order twice a prime) and a curve defined over $\mathbb{F}_2$ (of order twice or four times a prime) are given. As recommended in Remark 13, the extension degrees are prime for curves defined over $\mathbb{F}_2$.

Remark 19 We note that the generic discrete logarithm algorithms allow for a trade-off between precomputations and the breaking of a given discrete logarithm: In a group of size about 2^m, a precomputation of 2^k group elements yields additional logarithms in time 2^{m-k}. As a precaution, one may thus wish to avoid predetermined curves, especially at lower security levels.

1.4 Random curves: point counting

Remark 20 Algorithms for counting points on random elliptic curves currently come in two flavours. The first algorithm, SEA, is of polynomial complexity; for curves over extension fields $\mathbb{F}_{p^m}$, there are a variety of algorithms using p-adic numbers, with a much better polynomial exponent in m, but which are exponential in $\log p$.

Algorithm 21
(Schoof) In [60], Schoof describes the first algorithm of complexity polynomial in $\log q$ for counting the number of points on an arbitrary elliptic curve $E(\mathbb{F}_q)$. The algorithm is deterministic and computes the trace of Frobenius a_q and thus the zeta function. Given a prime ℓ not dividing q, the value of a_q modulo ℓ can be determined by checking for all possible values whether the numerator of the zeta function annihilates the ℓ-torsion points. Chinese remaindering for sufficiently many primes yields the exact value of a_q, which is bounded by Hasse's theorem. The algorithm has a complexity of $O\left((\log q)^{5+\epsilon)}\right)$, due in part to the fact that the ℓ-torsion points generate an $\mathbb{F}_q$-algebra of dimension $O(\ell^2)$.

Algorithm 22
(Schoof–Elkies–Atkin, SEA) Improvements are due to Atkin and Elkies [20]. When there is an $\mathbb{F}_q$-rational separable isogeny of degree ℓ from $E(\mathbb{F}_q)$ to another curve, then the ℓ-torsion points may be replaced by the kernel of the isogeny, generating an algebra of dimension $O(\ell)$ over $\mathbb{F}_q$. By the complex multiplication theory of Example 14, this happens when ℓ is coprime to the conductor of the ring of endomorphisms $\mathcal{O}_D$ of E and ℓ is not inert in the quadratic number field $\mathbb{Q}(\sqrt{D})$, which holds for about half of the primes. The complexity of the algorithm becomes $O\left((\log q)^{4+\epsilon)}\right)$ [7, Chapter VII], [16, Section 17.2].

Remark 23 The practical bottleneck of the algorithm used to be the computation of bivariate modular polynomials, of size $O(\ell^{3+\epsilon})$, needed to derive isogenies of degree ℓ. A quasi-linear algorithm is described in [22]; eventually limited by space, it has been used for ℓ up to around 10000. A more recent algorithm [69] computes the polynomial, reduced modulo the characteristic p of $\mathbb{F}_q$ and instantiated in one variable by an element of $\mathbb{F}_q$, also in time $O(\ell^{3+\epsilon})$, but in space $O(\ell(\ell + \log q))$; it has been used for ℓ up to about 100000. Further building blocks of the SEA algorithm have also been optimized [10, 34, 52]. The current record is for a prime field $\mathbb{F}_p$ with p having about 5000 decimal digits [70].

Remark 24 The SEA algorithm is implemented in several major computer algebra systems, and random elliptic curves of cryptographic size with a prime number of points are easily found, be it as domain parameters, be it in a setting where each user has his own elliptic curve as part of his public key.

Algorithm 25
(p-adic point counting) For an elliptic curve E over an extension field $\mathbb{F}_{p^m}$, Satoh [58] introduced an algorithm computing its *canonical lift* to a curve $\hat{E}$ over $\mathbb{Q}_{p^m}$, the unramified extension of degree m of the p-adic numbers $\mathbb{Q}_p$. The curve $\hat{E}$ has the same endomorphism ring $\mathcal{O}_D$ (Example 14) as E and reduces modulo the maximal ideal of $\mathbb{Q}_{p^m}$ to E. More precisely, an approximation to $\hat{E}$ may be computed by Newton iterations on a function derived from the modular polynomial of level p, Algorithm 21, at arbitrary p-adic precision. In a second step, the trace of the Frobenius map is computed in this characteristic 0 setting by the action of its dual isogeny (the reduction of which is separable) on a holomorphic differential; for this, the isogenies are computed explicitly. After a precomputation of $O(p^{3+\epsilon})$ for the p-th modular polynomial (see Algorithm 21), the complexity of the algorithm is $O(p^2 m^{3+\epsilon})$.

Remark 26 Satoh's algorithm is not immediately applicable in characteristic 2. Mestre suggests in [51] to use arithmetic-geometric mean (AGM) iterations, a sequence of isogenies of degree 2, to obtain the canonical lift and the trace of the Frobenius map, also in time $O(m^{3+\epsilon})$.

Remark 27 Later work concentrates on lowering the complexity in m: to quasi-quadratic for finite fields $\mathbb{F}_{q^m}$ with a Gaussian normal basis [48] or in the general case [37];

or on lowering the complexity in p: to quasi-linear [24] or even quasi-square root [38]. The record in [48] for a curve over $\mathbb{F}_{2^{100002}}$ goes beyond all practical cryptographic needs.

Remark 28 For a more thorough account, see [8, Chapter VI] or [16, Section 17.3].

2 Pairing based cryptosystems

Remark 29 While conventional elliptic curve cryptography relies on the map $x \mapsto xP$, which is a group homomorphism or, equivalently, a linear map of $\mathbb{Z}/n\mathbb{Z}$-modules, pairing based cryptography requires a bilinear map $e : G_1 \times G_2 \to G_3$. This introduces an additional degree of freedom and a wealth of new cryptographic primitives. Since 2007, a series of conferences, *Pairing-Based Cryptography — Pairing*, has been devoted to the topic [30, 44, 62, 71].

2.1 Cryptographic pairings

Definition 30 Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and let n be the largest prime divisor of the cardinality of $E(\mathbb{F}_q)$. Assume that n does not divide q. (This is required in a cryptographic setting due to anomalous curves.) Then the *embedding degree* of E is the smallest integer k such that $E(\mathbb{F}_{q^k})$ contains $E(\overline{\mathbb{F}}_q)[n]$, the n^2 points of n-torsion of $E(\overline{\mathbb{F}}_q)$; i.e., k is minimal such that $E(\mathbb{F}_{q^k})[n] = E(\overline{\mathbb{F}}_q)[n]$.

Theorem 31 *[3, Theorem 1] If n does not divide $q-1$, then the embedding degree is the smallest integer k such that n divides $q^k - 1$.*

Definition 32 A *cryptographic elliptic pairing* is a map $e : G_1 \times G_2 \to G_3$ that is bilinear, non-degenerate and efficiently computable, where E is an elliptic curve defined over $\mathbb{F}_q$, n is the largest prime factor of $|E(\mathbb{F}_q)|$, n divides neither $q-1$ nor q, k is the embedding degree of E, and $G_1 \subseteq E(\mathbb{F}_q)$ and $G_2 \subseteq E(\mathbb{F}_{q^k})$ (denoted additively) and $G_3 \subseteq \mathbb{F}_{q^k}^*$ (denoted multiplicatively) are subgroups of order n.

Remark 33 In this setting, $G_1 = E(\mathbb{F}_q)[n]$ and G_3 are in fact fixed, while there are $n+1$ possible choices for G_2; see Subsection 2.3. Diagonalising the matrix of the Frobenius endomorphism on $E(\overline{\mathbb{F}}_q)[n]$ yields a mathematically canonical choice also for G_2, which is given by the following theorems.

Theorem 34 *G_1 is the subgroup of $E(\mathbb{F}_{q^k})[n]$ generated by the points having eigenvalue 1 under the Frobenius endomorphism φ_q. There is a unique subgroup $\overline{G}_2 \subseteq E(\mathbb{F}_{q^k})$ of order n generated by the points having eigenvalue q under the Frobenius endomorphism.*

Theorem 35 *Let* $\mathrm{Tr} : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$, $P \mapsto \sum_{i=0}^{k-1} \varphi_q^i(P)$, *denote the* trace endomorphism *of level k on E. Then the endomorphisms* Tr *and $\pi_2 = \mathrm{id} - \varphi_q$, restricted to $E(\mathbb{F}_{q^k})[n]$, yield surjective group homomorphisms* $\mathrm{Tr} : E(\mathbb{F}_{q^k})[n] \to G_1$ *with kernel $\overline{G}_2$ and $\pi_2 : E(\mathbb{F}_{q^k})[n] \to \overline{G}_2$ with kernel G_1.*

Definition 36 For a point P on E defined over some extension field $\mathbb{F}_{q^m}$ and an integer r, let $f_{r,P}$ be the function with divisor $r(P) - (rP) - (r-1)(\mathcal{O})$ that is defined over $\mathbb{F}_{q^m}$ and has leading coefficient 1 in $\mathcal{O}$.

For finite points R and $S \neq -R$, denote by $v_R = x - x(R)$ the line with divisor $(R) + (-R) - 2(\mathcal{O})$ and by $\ell_{R,S} = (y - y(R)) - \lambda_{R,S}(x - x(R))$ the line with divisor $(R) + (S) + (-R - S) - 3(\mathcal{O})$, where

$$\lambda_{R,S} = \begin{cases} \frac{y(S)-y(R)}{x(S)-x(R)} & \text{if } R \neq S, \\ \frac{3x(R)^2+2a_2x(R)+a_4-a_1y(R)}{2y(R)+a_1x(R)+a_3} & \text{if } R = S; \end{cases}$$

additionally, $\ell_{R,-R} = v_R$ and $v_{\mathcal{O}} = 1$.

Definition 37 An *addition-negation chain* for an integer r is a sequence $r_1, \ldots, r_s$ such that $r_1 = 1$, $r_s = r$ and each element r_i is either

1. the negative of a previsously encountered one: there is $1 \leqslant j(i) < i$ such that $r_i = -r_{j(i)}$; or
2. the sum of two previously encountered ones: there are $1 \leqslant j(i) \leqslant k(i) < i$ such that $r_i = r_{j(i)} + r_{k(i)}$.

Algorithm 38
Require: A point P on E and an integer r
Ensure: $f_{r,P} = \frac{L}{V}$, where L and V are given as products of lines
  Compute an addition-negation chain $r_1, \ldots, r_s$ for r.
  $P_1 \leftarrow P$, $L_1 \leftarrow 1$, $V_1 \leftarrow 1$
  for $i = 2, \ldots, s$ **do**
    $j \leftarrow j(i), k \leftarrow k(i)$
    if $r_i = -r_j$ **then**
      $P_i \leftarrow -P_j$
      $L_i \leftarrow V_j$
      $V_i \leftarrow L_j v_{P_i}$
    else
      $P_i \leftarrow P_j + P_k$
      $L_i \leftarrow L_j L_k \ell_{P_{j(i)},P_{k(i)}}$
      $V_i \leftarrow V_j V_k v_{P_i}$
    end if
  end for
  return $L = L_s$, $V = V_s$

Example 39 The *Weil pairing* e_n is a cryptographic pairing as long as $G_2 \neq G_1$. If P, $Q \in E(\mathbb{F}_{q^k})[n]$, then $e_n(P, Q) = (-1)^n \frac{f_{n,P}(Q)}{f_{n,Q}(P)}$.

Example 40 Assume that $E(\mathbb{F}_{q^k})$ does not contain a point of order n^2, or, equivalently, that n^3 does not divide $|E(\mathbb{F}_{q^k})|$. Then the map $E(\mathbb{F}_{q^k})[n] \to E(\mathbb{F}_{q^k})/nE(\mathbb{F}_{q^k})$, $Q \mapsto$

$Q + nE(\mathbb{F}_{q^k})$, is a group isomorphism, and the *Tate pairing* T yields a non-degenerate pairing

$$e'_T : E(\mathbb{F}_{q^k})[n] \times E(\mathbb{F}_{q^k})[n] \to \mathbb{F}^*_{q^k}/(\mathbb{F}^*_{q^k})^n, \quad (P, Q) \mapsto \mathsf{T}(P, Q + nE(\mathbb{F}_{q^k})).$$

Since $e'_T|_{G_1 \times G_1}$ takes values in $\mathbb{F}^*_q/(\mathbb{F}^*_q)^n = \{1\}$, the restriction $e'_T|_{G_1 \times G_2}$ is non-degenerate for any $G_2 \neq G_1$.

The *reduced Tate pairing*

$$e_T : G_1 \times G_2 \to G_3, \quad (P, Q) \mapsto \big(\mathsf{T}(P, Q + nE(\mathbb{F}_{q^k}))\big)^{(q^k-1)/n},$$

is a cryptographic pairing for any $G_2 \neq G_1$. It is computed as

$$e_T(P, Q) = (f_{n,P}(Q))^{(q^k-1)/n}.$$

Remark 41 We observe that during the computation of the reduced Tate pairing by Algorithm 38, all factors lying in a subfield of $\mathbb{F}_{q^k}$ may be omitted due to the final exponentiation. In particular, if the x-coordinate of Q lies in a subfield, then all v_{P_i} may be dropped, a technique known as *denominator elimination*; see Remark 51.

Definition 42 A *distortion map* is an effectively computable endomorphism

$$\psi : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$$

that restricts to an isomorphism $\psi : G_1 \to G_2$ for some subgroup $G_2 \neq G_1$.

Remark 43 Since G_1 is invariant under the Frobenius φ_q, but G_2 is not, the endomorphisms ψ and φ_q cannot commute. So the existence of ψ implies that E is supersingular. Conversely, for supersingular curves, there are distortion maps $\psi : G_1 \to G_2$ for any $G_2 \neq G_1$ [74, Theorem 5].

Example 44 Let E be a supersingular curve with distortion map ψ and $G_2 = \psi(G_1)$. Let $e : G_1 \times G_2 \to G_3$ be a cryptographic pairing. Then

$$e' : G_1 \times G_1 \to G_3, \quad (P, Q) \mapsto e(P, \psi(Q)),$$

is a cryptographic pairing in which both arguments come from the same group G_1. This setting is sometimes called a *symmetric pairing* in the literature, although it does not in general satisfy $e(P, Q) = e(Q, P)$; see also Section 2.3.

Remark 45 Further work has produced a variety of pairings with a shorter loop in Algorithm 38, that is, defined by some function $f_{r,P}$ with $r < n$. In general, this is obtained by choosing special curves and restricting to the subgroups G_1 and $\overline{G}_2$ of Theorem 35. Since all involved groups are cyclic, such pairings are necessarily powers of the Tate pairing.

Example 46 (Eta pairing) Let E be a supersingular curve with even $k = 2a$ and distortion map ψ as in Definition 42. Let $T = t - 1$, where t is the trace of the Frobenius map. Then $T \equiv q \pmod{n}$ and $n \mid (T^a + 1)$. Assume that $n^2 \nmid (T^a + 1)$. Then the map

$$G_1 \times G_1 \to G_3, \quad (P, Q) \mapsto f_{T,P}(\psi(Q))^{aT^{a-1}\frac{q^k-1}{n}},$$

is a cryptographic pairing. For a proof, see [4, Section 4] and [40, Section III]. By Example 62, only curves over fields of characteristic two or three may satisfy the assumptions of the theorem. Notice that T is of order $\sqrt{q}$ by Hasse's theorem, so that in the best case $\rho \approx 1$ (see Definition 66) the loop length in Algorithm 38 is reduced by a factor of about 2, while the final exponentiation becomes more expensive.

Example 47 (Ate pairing) Let $T = t - 1$, where t is the trace of the Frobenius map, and assume that $n^2 \nmid (T^k - 1)$. Then the map

$$\overline{G}_2 \times G_1 \to G_3, \quad (Q, P) \mapsto f_{T,Q}(P)^{\frac{q^k-1}{n}},$$

is a cryptographic pairing [40]. Notice that the roles of G_1 and $\overline{G}_2$ are inverted compared to the reduced Tate pairing of Example 40. Thus, as a price to pay for the loop shortening in Algorithm 38, the number of operations in $\overline{G}_2$ and thus $\mathbb{F}_{q^k}$ increases.

Conjecture 48 *(Optimal ate pairing) A loop length of essentially $\frac{\log_2 n}{\varphi(k)}$, where φ is Euler's function, may be obtained for a pairing of the previous type, for instance via a product of functions $f_{c_i,Q}(P)^{q^i\frac{q^k-1}{n}}$ with $\sum \log_2 c_i$ of the desired magnitude; concrete instances have been obtained using lattice reduction [39, 73].*

2.2 Pairings and twists

Theorem 49 *Assume that E is defined over the field $\mathbb{F}_q$ of characteristic at least 5 and that $d \in \{2, 3, 4, 6\}$ is such that $d \mid \gcd(k, \#\operatorname{Aut}(E))$. There is, besides E itself and up to equivalence, precisely one twist E' of degree d such that $n \mid \#E'(\mathbb{F}_{q^{k/d}})$. There is an isomorphism $\varphi : E' \to E$ which is defined over $\mathbb{F}_{q^d}$. The subgroup G_2' of order n of $E'(\mathbb{F}_{q^{k/d}})$ satisfies $\varphi(G_2') = \overline{G}_2$.*

Remark 50 Theorem 49 implies that in the presence of twists, elements of $\overline{G}_2$ are more compactly represented by elements of G_2'; or otherwise said, any cryptographic pairing $e : G_1 \times \overline{G}_2 \to G_3$ yields an equivalent cryptographic pairing $e' : G_1 \times G_2' \to G_3$, $(P, Q') \mapsto e(P, \varphi(Q'))$.

Remark 51 Theorem 49 and the explicit form of φ show that the x-coordinates of elements in $\overline{G}_2$ lie in $\mathbb{F}_{q^{k/2}}$ for d even and that the y-coordinates lie in $\mathbb{F}_{q^{k/3}}$ where $3 \nmid d$. This may allow for simplifications of Algorithm 38 in conjunction with the final exponentiation; see Remark 41.

Example 52 (Twisted ate pairing) Under the hypotheses of Theorem 49, let $T = t - 1$, where t is the trace of the Frobenius map, and assume that $n^2 \nmid (T^k - 1)$. Then the map

$$G_1 \times \overline{G}_2 \to G_3, \quad (P, Q) \mapsto f_{T^{k/d},P}(Q)^{\frac{q^k-1}{n}},$$

is a cryptographic pairing [40]. Here, the roles of G_1 and $\overline{G}_2$ are again as in the reduced Tate pairing of Example 40. However, compared to the ate pairing of Example 47, the loop length in Algorithm 38 is increased by a factor of $\frac{k}{d}$. Unless t is smaller than generically expected, the twisted ate pairing is in fact less efficient to compute than the reduced Tate pairing.

2.3 Explicit isomorphisms

Remark 53 For the sake of giving security arguments for pairing based systems, the cryptologic literature has taken to distinguishing pairings according to the possibility of moving efficiently between the groups G_1 and G_2. For instance, if $G_1 = G_2$, then the decisional Diffie-Hellman problem is easy in G_1: Given P, aP, bP and $R \in G_1$, one has $R = abP$ if and only if $e(P, R) = e(aP, bP)$.

Definition 54 Let e be a cryptographic pairing in the sense of Definition 32. It is of

1. *Type 1* if $G_1 = G_2$;
2. *Type 2* if there is an efficiently computable isomorphism $\psi : G_2 \to G_1$, but no such isomorphism $G_1 \to G_2$ is known;
3. *Type 3* if no efficiently computable isomorphisms $G_1 \to G_2$ or $G_2 \to G_1$ are known.

Remark 55 We note that since G_1 and G_2 are cyclic of the same order n, they are trivially isomorphic; but exhibiting an effective isomorphism may require to compute discrete logarithms. In general, an efficiently computable isomorphism will be given by an endomorphism of the elliptic curve.

Example 56 The pairing of Example 44 on supersingular curves with distortion map is of type 1. Any pairing with $G_2 \neq G_1, \overline{G}_2$ is of type 2: The isomorphism is given by the trace map Tr of Theorem 35. To the best of our knowledge, pairings with $G_2 = \overline{G}_2$ are of type 3; at least the trace is trivial on $\overline{G}_2$.

Remark 57 The terminology *Type 4* has been used for pairings in which the second argument comes from the full n-torsion group; in this case, G_2 can be seen as the group generated by this argument, which may vary with each use of the cryptographic primitive. As it is then unlikely that $G_2 = G_1$ or $\overline{G}_2$, a Type 4 pairing essentially behaves as a Type 2 pairing.

Remark 58 Type 1 pairings, being restricted to supersingular curves, offer a very limited choice of embedding degrees, see Example 62. Type 2 pairings are sometimes preferred in the cryptographic literature since they appear to facilitate certain security arguments. On the other hand, the existence of ψ implies that the decisional Diffie-Hellman problem is easy in G_2, and it is apparently not possible to hash into any subgroup G_2 different from G_1 and $\overline{G}_2$; see Subsection 2.5. Recent work introduces a heuristic construction to transform a cryptographic primitive in the Type 2 setting, together with its security argument, into an equivalent Type 3 primitive [14].

Remark 59 Some cryptographic primitives have been formulated with a pairing on subgroups of composite order n. More precisely, n is the product of two primes that are unknown to the general public, but form part of the private key as in the RSA system. Such pairings can be realised either with supersingular curves [9, Section 2.1] or using Algorithm 64; the former leads to a ρ-value (Definition 66) at least 2, the latter to a ρ-value close to 2. There is a heuristic approach to transform such cryptosystems, together with their security proofs, into the setting of prime order subgroups [24].

2.4 Curve constructions

Remark 60 The existence of a cryptographic pairing $e : G_1 \times G_2 \to G_3$ reduces the discrete logarithm problem in G_1 or G_2 to that of G_3: For instance, given a point $P \in G_1$ and a multiple xP, choose a point $Q \in G_2$ such that $\zeta = e(P, Q) \neq 1$. Then $\xi = e(P, xQ) = e(P, Q)^x$, and x is the discrete logarithm of $\xi \in G_3$ to the base ζ [26, 49].

Remark 61 Thus to balance the difficulty of the discrete logarithm problems in the elliptic curve groups G_1 and G_2 over $\mathbb{F}_q$ and $G_3 \subseteq \mathbb{F}_{q^k}^*$, the embedding degree k should be chosen according to the security equivalences in Section 1.1. For instance, if one follows the recommendations of [67], for a system of 256 bit security one would choose $n \approx 2^{512}$ and thus $q \approx 2^{512}$, and $k \approx \frac{15425}{512} \approx 30$. Since by Theorem 31 the embedding degree k equals the order of n in $\mathbb{F}_q$, it will be close to q for random curves. Hence one needs special constructions to obtain *pairing-friendly curves*, curves with a prescribed, small value of k. For a comprehensive survey, see [25].

Example 62 (Supersingular curves) As first noticed in [49], the embedding degree is always exceptionally small for supersingular curves. The following table gives the possible cardinalities, the maximal size n of a cyclic subgroup by [57] and the embedding degree k with respect to n.

$\lvert E(\mathbb{F}_q)\rvert$	n	k
$q+1$	$q+1$	2
$q+1\pm\sqrt{q}$	$q+1\pm\sqrt{q}$	3
$q+1\pm\sqrt{2q}$	$q+1\pm\sqrt{2q}$	4
$q+1\pm\sqrt{3q}$	$q+1\pm\sqrt{3q}$	6
$q+1\pm 2\sqrt{q}$	$\sqrt{q}\pm 1$	1

Remark 63 All algorithms for finding ordinary pairing-friendly curves rely on complex multiplication constructions, cf. Example 14, and construct curves over prime fields only.

Algorithm 64
A very general method is due to Cocks and Pinch [25, Section 4.1]. It allows to fix the desired group order n beforehand; choosing a low Hamming weight in the binary decomposition of n or more generally a value of n with a short addition-subtraction chain speeds up Algorithm 38.

Require: An integer $k \geqslant 2$, a quadratic discriminant $D < 0$ and a prime n such that $k \mid (n-1)$ and the Legendre symbol $\left(\frac{D}{n}\right) = 1$

Ensure: A prime p and an elliptic curve $E(\mathbb{F}_p)$ (with complex multiplication by $\mathcal{O}_D$) having a subgroup of order n and embedding degree k

repeat
$\zeta \leftarrow$ an integer such that ζ modulo n is a primitive k-th root of unity in $\mathbb{F}_n^*$
$t \leftarrow \zeta + 1$
$v \leftarrow$ an integer such that $v \equiv \frac{t-2}{\sqrt{D}} \pmod{n}$
$p \leftarrow \frac{t^2 - v^2 D}{4}$
until p is an integer and prime
Then $p \equiv t - 1 \pmod{n}$
Construct the curve E over $\mathbb{F}_p$ with $p + 1 - t$ points as in Example 14

Remark 65 Generically, in this construction t and v will be close to n, so that p will be close to n^2. This motivates the following definition.

Definition 66 The *ρ-value* of a pairing-friendly curve is given by

$$\rho = \frac{\log p}{\log n}.$$

Remark 67 By Hasse's theorem, the superior limit of ρ is at least 1 for $p \to \infty$. Values of ρ larger than 1 result in a loss of bandwidth when transmitting elements of G_1, which is a $\log_2 n$-bit subgroup embedded into a $\rho \log_2 n$-bit group, and a less efficient arithmetic in the elliptic curve. The security equivalences of Section 1.1 do in fact not fix the value of k, but that of ρk; so different values of k may lead to comparable security levels.

Remark 68 Further research has concentrated on finding families of pairing-friendly curves, the parameters of which are given by values of polynomials.

Algorithm 69
[11] The following is a direct transcription of Algorithm 64 to polynomials.

Require: An integer $k \geqslant 2$ and a quadratic discriminant $D < 0$

Ensure: Polynomials p and $n \in \mathbb{Q}(x)$ such that if the values $p(x_0)$ and $n(x_0)$ are simultaneously prime integers, then there is an elliptic curve $E(\mathbb{F}_{p(x_0)})$ (with complex multiplication by $\mathcal{O}_D$) having a subgroup of order $n(x_0)$ and embedding degree k

$n \leftarrow$ an irreducible polynomial in $\mathbb{Q}[x]$ such that the number field $K = \mathbb{Q}[x]/(n)$ contains $\sqrt{D}$ and a primitive k-th root of unity
$z \leftarrow$ a polynomial in $\mathbb{Q}[x]$ that reduces to a primitive k-th root of unity ζ in K
$t \leftarrow z + 1$
$v \leftarrow$ a polynomial in $\mathbb{Q}[x]$ that reduces to the element $\frac{\zeta-1}{\sqrt{D}}$ in K
$s \leftarrow$ a polynomial in $\mathbb{Q}[x]$ that reduces to $\sqrt{D}$ in K
$v \leftarrow \frac{(z-1)s}{D} \bmod n$
$p \leftarrow \frac{t^2 - Dv^2}{4}$

Remark 70 The polynomials p and n need not represent primes or even integers; choosing small values of $|D|$, and n such that z, $s \in \mathbb{Z}[X]$ may help. Let $d = \deg(n)$ be the degree of K. While it is always possible to choose n such that either z or v is of low degree (as low as 1 if n is the minimal polynomial of the corresponding algebraic number), it is a priori not clear whether *both* can be chosen of low degree. Generically, p is of degree $2(d-1)$, and the asymptotic ρ-value of the family is $2 - \frac{2}{d}$, a small improvement over Algorithm 64. In many cases, however, actual ρ-values are much closer to 1, as demonstrated by the following example.

Example 71 [11, p. 137] Let k be odd, $D = -4$ and $K = \mathbb{Q}(\zeta, \sqrt{-1}) = \mathbb{Q}[x]/(\Phi_{4k}(x))$ where $\Phi_{4k}(x) = \Phi_k(-x^2)$ is the $4k$-th cyclotomic polynomial. Choose $\zeta(x) = -x^2$, $t(x) = -x^2 + 1$, $s(x) = 2x^k$, $v(x) = \frac{1}{2}(x^{k+2} + x^k)$, $p(x) = \frac{1}{4}(x^{2k+4} + 2x^{2k+2} + x^{2k} + x^4 - 2x^2 + 1)$. The polynomial p takes integral values in odd arguments and, conjecturally, represents primes if it is irreducible (since $p(1) = 1$, there is no local obstruction to representing primes). Asymptotically for $p \to \infty$, $\rho \to \frac{k+2}{\varphi(k)}$, and $\rho \to 1$ if furthermore $k \to \infty$ with a fixed number of prime factors.

Remark 72 Similar results hold for even k, and for $D = -3$ since $\sqrt{-3} \in \mathbb{Q}[x]/(\Phi_3(x))$.

Remark 73 Table 1, taken from [25], gives the current best values of $\overline{\rho} = \frac{\deg p}{\deg n}$ for polynomial families of pairing-friendly curves for $k \geqslant 4$. (Smaller values of k may be obtained for prime fields using supersingular curves; see Example 62.) For the constructions behind each family, see [25].

2.5 Hashing into elliptic curves

Remark 74 Hashing into elliptic curve groups is often required for pairing-based cryptosystems. Standard cryptographic hash functions $\{0,1\}^* \to \{0,1\}^\ell$ of sufficient length ℓ are easily modified to yield values in $\mathbb{Z}/nZ$ (by reduction modulo n) and to arbitrary finite fields (by hashing to coefficients with respect to a fixed basis). One would like to extend such constructions to elliptic curves.

Remark 75 In the setting of Definition 32, if $H : \{0,1\}^* \to \mathbb{Z}/n\mathbb{Z}$ is a collision-resistant hash function and G_1 is generated by a point P of order n, then the function

k	$\deg p$	$\deg n$	$\overline{\rho}$	$k\overline{\rho}$	k	$\deg p$	$\deg n$	$\overline{\rho}$	$k\overline{\rho}$
4	2	2	1.00	4.0	28	16	12	1.33	37.3
5	14	8	1.75	8.8	29	60	56	1.07	31.1
6	2	2	1.00	6.0	30	12	8	1.50	45.0
7	16	12	1.33	9.3	31	64	60	1.07	33.1
8	10	8	1.25	10.0	32	34	32	1.06	34.0
9	8	6	1.33	12.0	33	24	20	1.20	39.6
10	4	4	1.00	10.0	34	36	32	1.12	38.2
11	24	20	1.20	13.2	35	72	48	1.50	52.5
12	4	4	1.00	12.0	36	14	12	1.17	42.0
13	28	24	1.17	15.2	37	76	72	1.06	39.1
14	16	12	1.33	18.7	38	40	36	1.11	42.2
15	12	8	1.50	22.5	39	28	24	1.17	45.5
16	10	8	1.25	20.0	40	22	16	1.38	55.0
17	36	32	1.12	13.8	41	84	80	1.05	43.0
18	8	6	1.33	24.0	42	16	12	1.33	56.0
19	40	36	1.11	21.1	43	88	84	1.05	45.0
20	22	16	1.38	27.5	44	46	40	1.15	50.6
21	16	12	1.33	28.0	45	32	24	1.33	60.0
22	26	20	1.30	28.6	46	50	44	1.14	52.3
23	48	44	1.09	25.1	47	96	92	1.04	49.0
24	10	8	1.25	30.0	48	18	16	1.12	54.0
25	52	40	1.30	32.5	49	100	84	1.19	58.3
26	28	24	1.17	30.3	50	52	40	1.30	65.0
27	20	18	1.11	30.0					

Table 1: Pairing-friendly curve parameters

$\{0,1\}^* \to G_1$, $m \mapsto H(m)P$, is trivially collision-resistant. However, this simple construction reveals the discrete logarithm of the hash value, which in general renders the cryptosystem totally insecure.

Remark 76 In the following, let E be an elliptic curve defined over $\mathbb{F}_q$ as in Definition 32, and assume that $n^3 \nmid |E(\mathbb{F}_{q^k})|$. If one can hash into $E(\mathbb{F}_q)$, then one can also hash into $G_1 = E(\mathbb{F}_q)[n]$: It suffices for that to multiply the result by the cofactor $\frac{|E(\mathbb{F}_q)|}{n}$. The same argument holds for $E(\mathbb{F}_{q^k})[n]$. However, it is then in general not possible to project into an arbitrary group G_2. For $\overline{G}_2$ as in Theorem 35, that is, Type 3 pairings as in Definition 54, the trace $\mathrm{Tr} : E(\mathbb{F}_{q^k})[n] \to \overline{G}_2$ can be used to obtain a hash function with values in $\overline{G}_2$. Alternatively, in the presence of twists as described in Theorem 49, one may more efficiently hash into the subgroup G_2' on the twisted curve, for which the cofactor is smaller.

To hash into $E(k)$ where $k = \mathbb{F}_q$ or $k = \mathbb{F}_{q^k}$, one may use a hash function H :

$\{0,1\} \to k$ to obtain the x-coordinate of a point. As not all elements of k occur as x-ccordinates, one may need several trials. A possibility is to concatenate the message m with a counter i, denoted by $m||i$, and to increase the counter until $H(m||i)$ is the x-ccordinate of a point on E. An additional hash bit may be used to determine one of the generically two points with the given x-coordinate. The algorithm is deterministic and, if H is modelled as a random function, it needs an expected number of two trials averaged over all input values. However, for $|k| \to \infty$, there is a doubly exponentially small fraction of the input values that will take exponential time. Several recent results exhibit special cases in which polynomial time hashing is possible uniformly for all input values.

Example 77 [7, Section 4.1] If $q \equiv 2 \pmod 3$, then $E : y^2 = x^3 + 1$ is a supersingular curve over $\mathbb{F}_q$ with $q+1$ points and $k = 2$. Precisely, since third powering is a bijection on $\mathbb{F}_q$ with inverse $z \mapsto z^{1/3} = z^{(2q-1)/3}$, the map $\mathbb{F}_q \to E(\mathbb{F}_q)\backslash\{\mathcal{O}\}$, $y \mapsto \big((y^2-1)^{(2q-1)/3}, y\big)$, is a bijection.

Example 78 [63] Let $E : y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6$ over $\mathbb{F}_q$ of characteristic at least 3. There are explicit rational functions $u_1(t)$, $u_2(t)$, $u_3(t)$ and $v(t)$ such that $v(t)^2 = f(u_1(t^2))f(u_2(t^2))f(u_3(t^2))$ [64]. So for any t there is at least one $i(t)$ such that $u_{i(t)}(t^2)$ is a square in $\mathbb{F}_q$, which yields a map $\mathbb{F}_q \to E(\mathbb{F}_q)$, $t \mapsto \big(u_{i(t)}(t^2), f(u_{i(t)}(t^2))^{1/2}\big)$. In a cryptographic context, we may assume that a non-square in $\mathbb{F}_q^*$ is part of the input, and then Tonelli-Shanks's algorithm computes square roots in deterministic polynomial time; see [15, Section 1.5.1] and [72]. The argument is refined in [63] to give a deterministic procedure for computing points on the curve without knowing a non-square and to show that at least $\frac{q-4}{8}$ different points may be reached. The case of characteristic two is also handled.

Example 79 [41] Let $\mathbb{F}_q$ with $q \equiv 2 \pmod 3$ be of characteristic at least 5, and let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}_q$. Let $v(t) = \frac{3a-t^4}{6t}$ and $x(t) = \Big(v(t)^2 - b - \frac{t^6}{27}\Big)^{1/3} + \frac{t^2}{3}$. Then $0 \mapsto \mathcal{O}$, $0 \neq t \mapsto (x(t), tx(t) + v(t))$ is a map $\mathbb{F}_q \to E(\mathbb{F}_q)$ with image size at least $\frac{q}{4}$, and conjecturally close to $\frac{5q}{8}$. A similar result holds for curves over $\mathbb{F}_{2^m}$ with odd m.

Remark 80 Alternative encodings for elliptic curves in Hessian form over $\mathbb{F}_q$ with $q \equiv 2 \pmod 3$ and odd are given in [23, 45]; see also [18]. They have an image of proven size about $q/2$.

References

[1] ANSI. The elliptic curve digital signature algorithm (ECDSA). Working Draft American National Standard: Public Key Cryptography for the Financial Services Industry X9.62-1998, American National Standards Institute,

September 1998. Available at `http://grouper.ieee.org/groups/1363/private/x9-62-09-20-98.zip`.

[2] ANSI. Key agreement and key transport using elliptic curve cryptography. Working Draft American National Standard: Public Key Cryptography for the Financial Services Industry X9.63-199x, American National Standards Institute, January 1999. Available at `http://grouper.ieee.org/groups/1363/private/x9-63-01-08-99.zip`.

[3] R. Balasubramanian and Neal Koblitz. The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. *J. Cryptology*, 11(2):141–145, 1998.

[4] Paulo S. L. M. Barreto, Steven D. Galbraith, Colm Ó'hÉigeartaigh, and Michael Scott. Efficient pairing computation on supersingular abelian varieties. *Designs, Codes and Cryptography*, 42:239–271, 2007.

[5] Juliana Belding, Reinier Bröker, Andreas Enge, and Kristin Lauter. Computing Hilbert class polynomials. In Alf van der Poorten and Andreas Stein, editors, *Algorithmic Number Theory — ANTS-VIII*, volume 5011 of *Lecture Notes in Computer Science*, pages 282–295, Berlin, 2008. Springer-Verlag.

[6] Mihir Bellare and Phillip Rogaway. Minimizing the use of random oracles in authenticated encryption schemes. In Yongfei Han, Tatsuaki Okamoto, and Sihan Qing, editors, *Information and Communications Security*, volume 1334 of *Lecture Notes in Computer Science*, pages 1–16, Berlin, 1997. Springer-Verlag.

[7] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic curves in cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2000. Reprint of the 1999 original.

[8] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Advances in Elliptic Curve Cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2005.

[9] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In Joe Kilian, editor, *Theory of Cryptography — TCC 2005*, volume 3378 of *Lecture Notes in Computer Science*, pages 325–341, Berlin, 2005. Springer-Verlag.

[10] A. Bostan, F. Morain, B. Salvy, and É. Schost. Fast algorithms for computing isogenies between elliptic curves. *Mathematics of Computation*, 77(263):1755–1778, 2008.

[11] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptogr.*, 37(1):133–141, 2005.

[12] Daniel R. L. Brown. Generic groups, collision resistance, and ECDSA. *Designs, Codes and Cryptography*, 35:119–152, 2005.

[13] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen. Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen). *Bundesanzeiger*, 85, June 7:2034, 2011.

[14] Sanjit Chatterjee and Alfred Menezes. On cryptographic protocols employing asymmetric pairings—the role of Ψ revisited. *Discrete Appl. Math.*, 159(13):1311–1322, 2011.

[15] Henri Cohen. *A Course in Computational Algebraic Number Theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1993.

[16] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, editors. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Discrete Mathematics and Its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2006.

[17] Jean-Marc Couveignes and Thierry Henocq. Action of modular correspondences around CM points. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory — ANTS-V*, volume 2369 of *Lecture Notes in Computer Science*, pages 234–243, Berlin, 2002. Springer-Verlag.

[18] Jean-Marc Couveignes and Jean-Gabriel Kammerer. The geometry of flex tangents to a cubic curve and its parameterizations. *Journal of Symbolic Computation*, 47:266–281, 2012.

[19] Claus Diem. The GHS attack in odd characteristic. *Journal of the Ramanujan Mathematical Society*, 18(1):1–32, 2003.

[20] Noam D. Elkies. Elliptic and modular curves over finite fields and related computational issues. In *Computational perspectives on number theory (Chicago, IL, 1995)*, volume 7 of *AMS/IP Stud. Adv. Math.*, pages 21–76. Amer. Math. Soc., Providence, RI, 1998.

[21] Andreas Enge. The complexity of class polynomial computation via floating point approximations. *Mathematics of Computation*, 78(266):1089–1107, 2009.

[22] Andreas Enge. Computing modular polynomials in quasi-linear time. *Mathematics of Computation*, 78(267):1809–1824, 2009.

[23] Reza Rezaeian Farashahi. Hashing into Hessian curves. To appear in *Africacrypt*, 2011.

[24] David Mandell Freeman. Converting pairing-based cryptosystems from composite-order groups to prime-order groups. In Henri Gilbert, editor, *Advances in Cryptology — EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 44–61, Berlin, 2010. Springer-Verlag.

[25] David Freemann, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of Cryptology*, 23(2):224–280, 2010.

[26] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. *Math. Comp.*, 62:865–874, 1994.

[27] Gerhard Frey. Applications of arithmetical geometry to cryptographic constructions. In Dieter Jungnickel and Harald Niederreiter, editors, *Finite Fields and Applications — Proceedings of The Fifth International Conference on Finite Fields and Applications F_{q^5}, held at the University of Augsburg, Germany, August 2–6, 1999*, pages 128–161, Berlin, 2001. Springer-Verlag.

[28] D. Fu and J. Solinas. IKE and IKEv2 authentication using the elliptic curve digital signature algorithm (ECDSA). RFC 4754, Internet Engineering Task Force, 2007. `http://www.ietf.org/rfc/rfc4754.txt`.

[29] Steven D. Galbraith, Florian Hess, and Nigel P. Smart. Extending the GHS Weil descent attack. In Lars Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 29–44, Berlin, 2002. Springer-Verlag.

[30] Steven D. Galbraith and Kenneth G. Paterson, editors. *Pairing-Based Cryptography — Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, Berlin, 2008. Springer-Verlag.

[31] Steven D. Galbraith and Nigel P. Smart. A cryptographic application of Weil descent. In Michael Walker, editor, *Cryptography and Coding*, volume 1746 of *Lecture Notes in Computer Science*, pages 191–200, Berlin, 1999. Springer-Verlag.

[32] Robert Gallant, Robert Lambert, and Scott Vanstone. Improving the parallelized Pollard lambda search on binary anomalous curves. *Mathematics of Computation*, 69(232):1699–1705, 2000.

[33] P. Gaudry, F. Hess, and N. P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, 15(1):19–46, 2002.

[34] P. Gaudry and F. Morain. Fast algorithms for computing the eigenvalue in the Schoof–Elkies–Atkin algorithm. In Jean-Guillaume Dumas, editor, *Proceedings of the 2006 International Symposium on Symbolic and Algebraic Computations — ISSAC MMVI*, pages 109–115, New York, 2006. ACM Press.

[35] Pierrick Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *Journal of Symbolic Computation*, 44(12):1690–1702, 2009.

[36] Damien Giry and Jean-Jacques Quisquater. Bluekrypt cryptographic key length recommendation, 2011. v26.0, April 18, `http://www.keylength.com/`.

[37] Robert Harley. Asymptotically optimal p-adic point-counting, December 2002. Posting to the Number Theory List, available at `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0212&L=NMBRTHRY&P=R1277`.

[38] David Harvey. Kedlaya's algorithm in larger characteristic. *Int. Math. Res. Not. IMRN*, 2007(22):Art. ID rnm095, 29, 2007.

[39] Florian Hess. Pairing lattices. In S. D. Galbraith and K. Paterson, editors, *Pairing-Based Cryptography — Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 18–38, Berlin, 2008. Springer-Verlag.

[40] Florian Hess, Nigel P. Smart, and Frederik Vercauteren. The eta pairing revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006.

[41] Thomas Icart. How to hash into elliptic curves. In Shai Halevi, editor, *Advances in Cryptology — CRYPTO 2009*, volume 5677 of *Lecture Notes in Computer Science*, pages 303–316, Berlin, 2009. Springer-Verlag.

[42] IEEE. Standard specifications for public key cryptography. Standard P1363-2000, Institute of Electrical and Electronics Engineering, 2000. Draft D13 available at `http://grouper.ieee.org/groups/1363/P1363/draft.html`.

[43] Antoine Joux and Vanessa Vitse. Cover and decomposition index calculus on elliptic curves made practical — Application to a seemingly secure curve over $\mathbb{F}_{p^6}$. To appear in Eurocrypt 2012, `http://eprint.iacr.org/2011/020.pdf`, 2011.

[44] Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors. *Pairing-Based Cryptography — Pairing 2010*, volume 6487 of *Lecture Notes in Computer Science*, Berlin, 2010. Springer-Verlag.

[45] Jean-Gabriel Kammerer, Reynald Lercier, and Guénaël Renault. Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time. In Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors, *Pairing-Based Cryptography — Pairing 2010*, volume 6487 of *Lecture Notes in Computer Science*, pages 278–297, Berlin, 2010. Springer-Verlag.

[46] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177):203–209, 1987.

[47] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes (extended abstract). In Hideki Imai and Yuliang Zheng, editors, *Public Key Cryptography — 3rd International Workshop on Practice and Theory in Public Key Cryptosystems PKC 2000*, volume 1751 of *Lecture Notes in Computer Science*, pages 446–465, Berlin, 2000. Springer-Verlag.

[48] Reynald Lercier and David Lubicz. Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time. In Eli Biham, editor, *Advances*

in Cryptology — EUROCRYPT 2003, volume 2656 of *Lecture Notes in Computer Science*, pages 360–373, Berlin, 2003. Springer-Verlag.

[49] Alfred J. Menezes, Tatsuaki Okamoto, and Scott A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Trans. Inform. Theory*, 39(5):1639–1646, 1993.

[50] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of applied cryptography*. CRC Press Series on Discrete Mathematics and its Applications. CRC Press, Boca Raton, FL, 1997. With a foreword by Ronald L. Rivest.

[51] Jean-François Mestre. Lettre adressée à Gaudry et Harley. `http://www.math.jussieu.fr/~mestre/lettreGaudryHarley.ps`, December 2000.

[52] P. Mihăilescu, F. Morain, and É. Schost. Computing the eigenvalue in the Schoof–Elkies–Atkin algorithm using abelian lifts. In C. W. Brown, editor, *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation — ISSAC 2007*, pages 285–292, New York, 2007. Association for Computing Machinery.

[53] Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *Advances in Cryptology — CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426, Berlin, 1986. Springer-Verlag.

[54] Gary L. Mullen and Daniel Panario, editors. *Handbook of Finite Fields*. Discrete Mathematics and Its Applications. Chapman and Hall/CRC, Boca Raton, 2013.

[55] NIST. Digital signature standard (DSS). Federal Information Processing Standards Publication 186-3, National Institute of Standards and Technology, July 2009.

[56] Bart Preneel et al. NESSIE security report. Technical Report D20-v2, New European Schemes for Signatures, Integrity, and Encryption, 2003.

[57] Hans-Georg Rück. A note on elliptic curves over finite fields. *Mathematics of Computation*, 49(179):301–304, July 1987.

[58] Takakazu Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.

[59] Takakazu Satoh and Kiyomichi Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Comment. Math. Univ. St. Paul.*, 47(1):81–92, 1998.

[60] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170), April 1985.

[61] I. A. Semaev. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. *Math. Comp.*, 67(221):353–356, 1998.

[62] Hovav Shacham and Brent Waters, editors. *Pairing-Based Cryptography — Pairing 2009*, volume 5671 of *Lecture Notes in Computer Science*, Berlin, 2009. Springer-Verlag.

[63] Andrew Shallue and Christiaan E. van de Woestijne. Construction of rational points on elliptic curves over finite fields. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Algorithmic Number Theory — ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 510–524, Berlin, 2006. Springer-Verlag.

[64] M. Skałba. Points on elliptic curves over finite fields. *Acta arithmetica*, 117(3):293–301, 2005.

[65] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12(3):193–196, 1999.

[66] N. P. Smart. The exact security of ECIES in the generic group model. In Bahram Honary, editor, *Cryptography and Coding*, volume 2260 of *Lecture Notes in Computer Science*, pages 73–84, Berlin, 2001. Springer-Verlag.

[67] Nigel Smart et al. ECRYPT II yearly report on algorithms and keysizes (2009-2010). Technical Report D.SPA.13, European Network of Excellence in Cryptology II, 2010.

[68] Jacques Stern, David Pointcheval, John Malone-Lee, and Nigel Smart. Flaws in applying proof methodologies to signature schemes. In Moti Yung, editor, *Advances in Cryptology — CRYPTO 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 93–110, Berlin, 2002. Springer-Verlag.

[69] Andrew V. Sutherland. Genus 1 point counting in essentially quartic time and quadratic space, September 2010. Slides, `http://math.mit.edu/~drew/NYU0910.pdf`.

[70] Andrew V. Sutherland. Genus 1 point-counting record modulo a 5000+ digit prime, July 2010. Posting to the Number Theory List, `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1007&amp;L=nmbrthry&amp;T=0&amp;F=&amp;S=&amp;P=287`.

[71] Tsuyoshi Takagi, Tatsuaki Okamoto, Eiji Okamoto, and Takeshi Okamoto, editors. *Pairing-Based Cryptography — Pairing 2007*, volume 4575 of *Lecture Notes in Computer Science*, Berlin, 2007. Springer-Verlag.

[72] Alberto Tonelli. Bemerkung über die Auflösung quadratischer Congruenzen. *Nachrichten von der Königl. Gesellschaft der Wissenschaften und der Georg-Augusts-Universität zu Göttingen*, pages 344–346, 1891.

[73] Frederic Vercauteren. Optimal pairings. *IEEE Transactions on Information Theory*, 56(1):455–461, 2010.

[74] Eric R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *Journal of Cryptology*, 17(4):277–296, 2004.

[75] William C. Waterhouse. Abelian varieties over finite fields. *Annales Scientifiques de l'École Normale Supérieure,* 4^e *Série*, 2:521–560, 1969.

[76] Michael J. Wiener and Robert J. Zuccherato. Faster attacks on elliptic curve cryptosystems. In Stafford Tavares and Henk Meijer, editors, *Selected Areas in Cryptography — SAC '98*, volume 1556 of *Lecture Notes in Computer Science*, pages 190–100, Berlin, 1999. Springer-Verlag.