ALGEBRAIC CURVES AND CRYPTOGRAPHY

STEVEN GALBRAITH AND ALFRED MENEZES

Abstract. Algebraic curves over finite fields are being extensively used in the design of public-key cryptographic schemes. This paper surveys some topics in algebraic curve cryptography, with an emphasis on recent developments in algorithms for the elliptic and hyperelliptic curve discrete logarithm problems, and computational problems in pairing-based cryptography.

1. Introduction

In 1975, Diffie and Hellman [30] proposed an elegant solution to the problem of establishing a secret key by communicating over an unsecured channel. Let p be a prime, and let α be a generator of the multiplicative group $\mathbb{F}_p^*$. The parameters p and α are fixed and common knowledge. Suppose now that two users, A and B, wish to establish a shared secret key. User A randomly selects a secret integer a, $0 \leq a \leq p-2$, and sends $P_A = \alpha^a \bmod p$ to B. Similarly, B randomly selects a secret integer b, $0 \leq b \leq p-2$, and sends $P_B = \alpha^b \bmod p$ to A. Now both A and B can use their secret integers to compute the shared key $K = (P_A)^b = (P_B)^a = \alpha^{ab} \bmod p$.

An eavesdropper who monitors the communications channel is faced with the task of computing K given p, α, P_A and P_B. This problem has come to be known as the *Diffie-Hellman problem (DHP)*. If intractable, then K is indeed known only to A and B and the Diffie-Hellman key establishment mechanism can be considered secure against eavesdroppers. A necessary condition for intractability of the DHP is that the *discrete logarithm problem* (DLP) be hard. The latter problem is to determine a given p, α and P_A; the integer a is appropriately called the discrete logarithm of P_A to the base α and denoted $\log_\alpha P_A$.

ElGamal [35] later described protocols for public-key encryption and signatures whose security is based on the intractability of the discrete logarithm problem. It also became evident that such discrete logarithm (DL) protocols could be implemented using any finite cyclic group G instead of the multiplicative group $\mathbb{F}_p^*$ as long as (i) group elements can be compactly represented; (ii) the group operation can be performed efficiently; and (iii) the

Date: January 12, 2005; updated April 28, 2005.

1991 *Mathematics Subject Classification.* 94A60.

Key words and phrases. public-key cryptography, discrete logarithm problem, hyperelliptic curves, elliptic curves.

discrete logarithm problem (and Diffie-Hellman problem) in G is intractable. Schnorr [104] first proposed using a subgroup of prime order q of $\mathbb{F}_p^*$, where q can be substantially smaller than p. Schnorr's idea was combined with a modification of the ElGamal signature scheme to yield the Digital Signature Algorithm (DSA), the first digital signature scheme to be standardized [37].

In 1985, Koblitz [74] and Miller [88] showed that (subgroups of) the group of rational points on an elliptic curve over a finite field are viable candidates for implementing DL protocols. This was followed a few years later by a proposal to use the divisor class group of a hyperelliptic curve over a finite field [75]. Cryptographers thus became interested in computational problems related to the efficient implementation of the group law and to finding discrete logarithms in divisor class groups of algebraic curves. The results of some of this work have been commercialized. DLP protocols based on elliptic curves were standardized by several accredited standardization bodies including ANSI [3, 4], IEEE [65], ISO [66] and NIST [38], and have been included in numerous commercial products. Hyperelliptic curves of genus 2 are undergoing intensive study and there is some commercial interest in using them. Recently, innovative ideas of Joux [71] and Boneh and Franklin [19] have spurred tremendous interest in developing and deploying cryptographic protocols using the Weil and Tate pairings on elliptic curves over finite fields.

The purpose of this paper is to survey some recent developments in curve-based cryptography, with a particular emphasis on elliptic and hyperelliptic curve cryptography. We will be selective in our choice of topics, and instead refer the reader to recent books [8, 15, 16, 60] for more comprehensive treatments. We shall assume that the reader is familiar with the theory of finite fields [80], elliptic curves [112, 124], and algebraic curves [43, 112], but will not assume any prior knowledge of public-key cryptography.

The remainder of this paper is organized as follows. The properties of groups that are desirable for implementing DL protocols are further studied in §2. Index-calculus algorithms for solving special cases of the DLP are discussed in §3, with a particular emphasis on recent work of Semaev, Gaudry and Diem. In §4, we describe some interesting relationships between the elliptic and hyperelliptic curve discrete logarithm problems. In particular, we describe some families of curves whose DLP is easier than the general case. Protocols using bilinear pairings and some related computational problems are covered in §5. Finally, §6 discusses some avenues for future research.

2. Curves and Groups

Recall that a cyclic group G is suitable for implementing DL protocols if (i) group elements can be compactly represented; (ii) the group operation can be performed efficiently; and (iii) the discrete logarithm problem (and Diffie-Hellman problem) in G is intractable. We first consider groups arising

from algebraic curves that satisfy conditions (i) and (ii), and then discuss condition (iii).

Throughout the paper we denote by C a projective, non-singular algebraic curve over a finite field (see [112] for definitions). Often C is written as an affine curve, but we always work with the associated projective, non-singular curve. Let $K = \mathbb{F}_q$ denote the finite field of order q, and let C be defined over K. The (degree zero) divisor class group $\mathrm{Pic}^0_K(C)$ of C over K, also known as the Picard group of C, is the quotient group of degree zero divisors (defined over K) modulo the principal divisors (defined over K). Since $\mathrm{Pic}^0_K(C)$ is a finite abelian group, cyclic subgroups of it are candidates for implementing DL protocols. The algorithms known for performing the group addition in $\mathrm{Pic}^0_K(C)$ for general curves C (e.g., see [64, 123, 61]) are too inefficient for cryptographic applications, although they can be used for the index-calculus algorithms on general curves which we will sometimes require when discussing Weil descent attacks (cf. §4.4). Instead, one looks for special classes of curves which admit faster group addition.

Suppose now that C_a is a nonsingular affine curve over K and that C is the smooth projective curve associated with C_a. Suppose that C has exactly one point at infinity (i.e., there is exactly one point on C which does not lie on C_a), and suppose that this point is defined over K. We denote this point by ∞. Then $\mathrm{Pic}^0_K(C)$ is isomorphic to the ideal class group of the affine coordinate ring of C_a over K. Working with the ideal class group is more convenient as it enables a compact representation for elements of $\mathrm{Pic}^0_K(C)$ and fast algorithms for group addition. Families of such curves for which the group addition is fast enough for cryptographic applications include hyperelliptic curves [25], superelliptic curves [51], C_{ab} curves [5], and Picard curves [10, 39].[1] In the remainder of this paper, we restrict our attention to hyperelliptic curves.

A hyperelliptic curve C of genus $g \geq 1$ over K can be defined by a non-singular equation of the form

$$C \ : \ y^2 + h(x)y = f(x), \tag{1}$$

where $f, h \in K[x]$, f is monic, $\deg f = 2g + 1$, and $\deg h \leq g$. A representation of a hyperelliptic curve in this form is sometimes called 'imaginary' since the function field has a single ramified point at infinity, just like imaginary quadratic number fields. If the characteristic of K is not equal to 2, then we can assume without loss of generality that $h(x) = 0$. The set $C(K)$ of K-rational points consists of the point at infinity ∞ and the points $(x, y) \in K \times K$ that satisfy (1). A theorem of Weil implies that

$$(\sqrt{q} - 1)^{2g} \ \leq \ \#\mathrm{Pic}^0_K(C) \ \leq \ (\sqrt{q} + 1)^{2g}, \tag{2}$$

[1]The restriction to curves with a single point at infinity is not essential and there have been several papers such as [94, 117] that give efficient implementation results in the more general case.

so $\#\mathrm{Pic}_K^0(C) \approx q^g$. The cosets of $\mathrm{Pic}_K^0(C)$ can be uniquely represented by so-called reduced divisors, and we will henceforth identify cosets of $\mathrm{Pic}_K^0(C)$ and reduced divisors. Mumford [91] showed that a reduced divisor $D \in \mathrm{Pic}_K^0(C)$ can be compactly represented by a pair of polynomials $a, b \in K[x]$ where a is monic, $\deg b < \deg a \leq g$, and $b^2 + bh - f \equiv 0 \pmod{a}$; we write $D = \mathrm{div}(a, b)$. The degree of D is $\deg a$. Cantor's algorithm [25] can be used to efficiently compute the sum of two reduced divisors and express the result in reduced form[2].

Elliptic curves are the hyperelliptic curves of genus 1. With $g = 1$, equation (1) specializes to the familiar Weierstrass equation

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

where $a_1, a_2, a_3, a_4, a_6 \in K$. If the characteristic of K is not equal to 2 or 3, then a linear change of variables simplifies (3) to

$$E \ : \ y^2 = x^3 + ax + b, \tag{4}$$

where $a, b \in K$. If $\mathrm{div}(c, d)$ is a nonzero divisor in $\mathrm{Pic}_K^0(E)$, then $c(x) = x - u$ and $d(x) = v$ where $(u, v) \in K \times K$ satisfies (3). Thus there is a 1-1 correspondence between elements of $\mathrm{Pic}_K^0(E)$ and points in $E(K)$, with $\mathrm{div}(1, 0)$ corresponding to ∞. Cantor's algorithm for adding reduced divisors coincides with the usual algebraic formulae derived from the chord-and-tangent rule for adding points in $E(K)$.

It remains to consider the hardness of the DLP in divisor class groups. Suppose now that $G = \langle \alpha \rangle$ is an arbitrary cyclic group of order n. Since an instance of the DLP in G can be easily reduced to instances of the DLP in prime-order subgroups of G [97], we can assume without loss of generality that n is prime. The best generic algorithm known for solving the DLP is Pollard's rho method [98] which has a fully-exponential expected running time of $\sqrt{\pi n/2}$ group operations. Nechaev [93] and Shoup [111] proved a lower bound of $\Omega(\sqrt{n}\,)$ for the DLP in generic groups, thus establishing that Pollard's rho algorithm is essentially the best generic algorithm possible for the DLP. Of course, for any particular family of groups there may be a faster (non-generic) algorithm that exploits the representation of group elements. Indeed, every cyclic group of order n is isomorphic to the additive group of integers modulo n with generator 1, and the DLP in the latter group is trivial to solve. Hence the hardness of the DLP in a group depends critically on the representation used for group elements. The important question is whether there are DLP solvers for the divisor class groups of hyperelliptic curves (using Mumford's representation) that are significantly faster than Pollard's rho method. This question will be pursued in §§3 and 4.

As mentioned in §1, hardness of the DHP is also necessary for the security of some DL protocols. There are no groups known for which the DLP is (believed to be) intractable, but where the DHP can be efficiently solved. In fact, there is some evidence that the two problems are polynomial-time

[2]See [87] for an elementary introduction to hyperelliptic curves and Cantor's algorithm.

equivalent. For example, den Boer [17] proved the equivalence in all cyclic groups of order n where $\phi(n)$ has no large prime factors (ϕ is the Euler phi function). For further evidence of this equivalence, see [82, 20].

In the Diffie-Hellman key agreement protocol, one may require the further assurance that a passive adversary cannot learn anything whatsoever about the shared secret α^{ab}. That is, given α^a and α^b, the adversary should not be able to distinguish α^{ab} from a randomly selected group element. An equivalent restatement of this requirement is that the following *decision Diffie-Hellman problem (DDHP)* should be intractable: given the group parameters α, n and a 3-tuple $(\beta_1 = \alpha^a, \beta_2 = \alpha^b, \beta_3 = \alpha^c)$ of group elements, determine whether or not $\beta_3 = \alpha^{ab}$. It is easy to see that DDHP is no harder than the DHP and the DLP. However, there are some groups for which DDHP can be efficiently solved while the DHP (and DLP) are believed to be intractable. One such family of groups will be used in §5 to construct a signature scheme with short signatures.

The requirement that n be prime means that the order of a divisor class group $\mathrm{Pic}^0_K(C)$ selected for cryptographic applications should be divisible by a large prime number. Hence there is a need for fast algorithms for computing $\#\mathrm{Pic}^0_K(C)$. In 1985, Schoof [105] devised the first polynomial-time algorithm for computing $\#E(K)$ where E is an elliptic curve. Since then, there has been tremendous progress in point counting algorithms for elliptic curves (e.g., see [79, 67, 102, 40, 54]), and the problem is considered well solved. Much work has also been done on the problem of computing $\#\mathrm{Pic}^0_K(C)$ where C is a hyperelliptic curve (e.g., see [73, 121, 125, 57]). We will not pursue this topic any further in this paper.

3. Index-Calculus Attacks

Let $G = \langle\alpha\rangle$ be a cyclic group of order r, and suppose that we wish to find $\log_\alpha \beta$ for some $\beta \in G$. The essential ingredient in an index-calculus algorithm is the selection of a subset $\mathcal{F} = \{p_1, p_2, \ldots, p_t\} \subseteq G$, called the *factor base*, having the property that a significant proportion of elements in G can be expressed as a product of elements from $\mathcal{F}$. One then collects linear *relations* in the logarithms of factor base elements by repeatedly selecting random integers $k \in [0, r-1]$ until α^k can be written as a product of elements in $\mathcal{F}$: if $\alpha^k = \prod_{i=1}^t p_i^{c_i}$ then the relation is $\sum_{i=1}^t c_i \log_\alpha p_i \equiv k \pmod r$.[3] Having collected slightly more than t such relations, it is likely that the linear system of equations has rank t in which case the $\log_\alpha p_i$ can be found by Gaussian elimination. Finally, $\log_\alpha \beta$ is obtained by repeatedly selecting random $k \in [0, r-1]$ until $\beta\alpha^k$ can be written as a product of elements in $\mathcal{F}$: if $\beta\alpha^k = \prod_{i=1}^t p_i^{d_i}$, then we have $\log_\alpha \beta = -k + \sum_{i=1}^t d_i \log_\alpha p_i \bmod r$. The running time of the algorithm depends critically on the choice of the factor base $\mathcal{F}$, in particular its size t and the time it takes to decompose a group element into a product of factor base elements.

[3] More sophisticated methods for generating relations may lead to faster algorithms.

If G is the multiplicative group of a finite field, then there are suitable choices for the factor base that yield subexponential-time DLP solvers that are faster than Pollard's rho method; this is the topic of §3.1. Index-calculus algorithms for the divisor class group of hyperelliptic curves are discussed in §3.2. Index-calculus algorithms for elliptic curves that were recently proposed by Semaev, Gaudry and Diem are outlined in §3.3.

3.1. **Finite fields.** Subexponential-time index-calculus DLP solvers are known for all finite fields [1]. We consider the cases of prime fields and characteristic two finite fields.

For the case $G = \mathbb{F}_p^*$ where elements are represented as integers between 1 and $p-1$, a natural choice for $\mathcal{F}$ is the set of the first t prime numbers. An integer is said to be p_t-smooth if all its prime factors are $\leq p_t$. Trial division can be used to efficiently determine p_t-smoothness of an integer in $\mathbb{F}_p^*$. The size t of $\mathcal{F}$ is selected by balancing the running time of the relation collection stage and the time to solve the system of equations. A larger t is preferred because then the probability that a randomly selected integer in $[1, p-1]$ is p_t-smooth is higher. On the other hand, a smaller t is preferred because then few relations are needed and also because the system of linear equations is smaller. The fastest variant of the index-calculus method for solving the DLP in $\mathbb{F}_p^*$ is the number field sieve [59] which has a subexponential expected running time of $L_p[\frac{1}{3}, 1.923]$.[4]

For the case $G = \mathbb{F}_{2^m}^*$ where elements are represented as polynomials in $\mathbb{F}_2[x]$ of degree at most $m-1$ (and multiplication is performed modulo a fixed irreducible polynomial of degree m), a natural choice for $\mathcal{F}$ is the set of irreducible polynomials of degree $\leq b$. A polynomial in $\mathbb{F}_2[x]$ is said to be b-smooth if all its irreducible factors have degree $\leq b$. Again, trial division can be used to efficiently determine b-smoothness of a polynomial in $\mathbb{F}_{2^m}^*$. The fastest variant of the index-calculus method for solving the DLP in $\mathbb{F}_{2^m}^*$ is the function field sieve [72] which has a subexponential expected running time of $L_{2^m}[\frac{1}{3}, 1.526]$.

3.2. **Hyperelliptic curves.** Let C be a genus g hyperelliptic curve over $K = \mathbb{F}_q$ defined by an equation (1). The discrete logarithm problem in (cyclic subgroups of) $\mathrm{Pic}_K^0(C)$ is called the *hyperelliptic curve discrete logarithm problem (HCDLP)*, and its specialization to elliptic curves is called the *elliptic curve discrete logarithm problem (ECDLP)*.

Suppose for simplicity that $\mathrm{Pic}_K^0(C)$ is a cyclic group of order r, as is often the case in cryptographic applications. A reduced divisor $D = \mathrm{div}(a, b) \in \mathrm{Pic}_K^0(C)$ is said to be *prime* if the polynomial $a(x)$ is irreducible over K. If D

[4] $L_n[d, c] = O\left(e^{(c+o(1))(\log n)^d (\log\log n)^{1-d}}\right) = O\left(e^{(\log n)^{d+\epsilon}}\right)$ where c is a positive constant and d is a constant satisfying $0 \leq d \leq 1$. If $0 < d < 1$, this expression is said to be subexponential in $\log n$ since it grows faster than any polynomial function in $\log n$, but is of the form $O(2^{o(\log n)})$. Note that $L_n[0, c]$ is polynomial in $\log n$, and $L_n[1, c]$ is fully exponential in $\log n$.

is not prime, then D can be efficiently expressed as a sum of prime divisors by factoring $a(x)$: if $a = \prod a_i^{c_i}$ is the complete factorization of $a(x)$ over K, then $D = \sum c_i \mathrm{div}(a_i, b_i)$ where $b_i = b \bmod a_i$. This suggests selecting the factor base $\mathcal{F}$ to consist of all prime divisors of degree at most t, for some smoothness bound $t \in [1, g]$. We expect that for roughly half of all irreducible polynomials $a(x)$ of degree $\leq t$, there are two solutions $b(x)$ to $b^2 + bh - f \equiv 0 \pmod{a}$; hence $\#\mathcal{F}$ can be easily estimated. To complete the analysis, one needs to estimate the proportion of smooth reduced divisors.

Enge and Gaudry [36] showed that if θ is a positive constant and $g \geq \theta \log q$, then this index-calculus method for the HCDLP has a subexponential expected running time of

$$L_{q^g}[\tfrac{1}{2}, c] \quad \text{where} \quad c = \sqrt{2}\left(\sqrt{1 + \frac{1}{2\theta}} + \sqrt{\frac{1}{2\theta}}\right). \tag{5}$$

Consequently, for high genus hyperelliptic curves there are DLP solvers that are asymptotically faster than Pollard's rho method (whose running is $O(q^{g/2})$).[5]

Gaudry [53] also showed that if a smoothness bound $t = 1$ is selected (so the factor base only consists of degree one divisors), then the expected running time is

$$O(g^2 g! q \log^2 q + g^3 q^2 \log^2 q). \tag{6}$$

The first term in (6) is the running time for relation generation. If g is fixed then asymptotically this is dominated by the second term, which is the running time for the linear algebra stage. The index-calculus algorithm with smoothness bound $t = 1$ is known as *Gaudry's HCDLP algorithm*. If g is fixed, then the running time (6) can be written as $O(q^{2+\epsilon})$, Hence Gaudry's algorithm is asymptotically faster than Pollard's rho method for hyperelliptic curves of a fixed genus $g \geq 5$. However, the hidden constant in the expression $O(q^{2+\epsilon})$ depends very badly on g. In practice, Gaudry's method is indeed superior for small g (e.g., $g = 5, 6, 7$).

Harley and Thériault (see [119]) suggested reducing the factor base size in Gaudry's algorithm in order to balance the running times of the relation generation and linear algebra stages. Thériault [119] also proposed a "large prime" variant of Gaudry's algorithm. More recently, Gaudry, Thériault and Thomé (GTT) [58] proposed a "double large prime" variant of Gaudry's algorithm utilizing the double large prime strategy that was successful in accelerating integer factorization algorithms [78]. Here, the factor base is chosen to be a subset of the degree one divisors. Degree one divisors that are not in the factor base are called *large primes*. A divisor is defined to be smooth if it can be written as a sum of prime divisors and at most two large primes. Relations are collected as before, and then combined to eliminate

[5]Comparisons between Pollard's rho method and index-calculus methods are problematic because the former has negligible storage requirements while storage requirements can be a bottleneck with index-calculus methods. We will not address this issue any further.

the large primes. For any fixed g the GTT algorithm was shown to have an expected running time of $O(q^{2-\frac{2}{g}})$, and so is faster than Pollard's rho method for genus 3 and 4 hyperelliptic curves as long as q is sufficiently large.

To summarize, it is believed that when $g \geq 3$ the HCDLP over $\mathbb{F}_q$ can be solved faster than Pollard's rho method if q is sufficiently large. This is not the case for general elliptic curves and genus 2 curves[6] although, as we will see in Section 4, there are weak classes of curves whose DLP can be solved faster than Pollard's rho method. Hence for $g \geq 3$ a hyperelliptic curve cryptosystem would require longer keys, and would therefore most likely be slower, than elliptic and genus 2 cryptosystems that provide the same level of security. This explains why divisor class groups of elliptic and genus 2 curves appear to be the most promising groups for implementing DL protocols. Unlike their elliptic curve counterparts, genus 2 cryptosystems have not yet been deployed in practice. This is partly because the group operation for genus 2 curves was thought to be significantly slower than for elliptic curves. However, recent work on speeding the group law for genus 2 curves [77] and on implementing hyperelliptic curve systems [95, 7, 118] suggests that genus 2 systems are quite competitive with elliptic curve systems.

3.3. **Elliptic curves.** Gaudry's index-calculus attack on the HCDLP fails for the ECDLP because all divisors in the divisor class group $\mathrm{Pic}_K^0(E)$ of an elliptic curve E have degree one. (Recall that all reduced divisors in $\mathrm{Pic}_K^0(E)$ are of the form $\mathrm{div}(x-u, v)$ where $(u, v) \in E(K)$.) A different approach is needed for deciding which points in $E(K)$ should belong to the factor base. We next describe four such proposals. In the first, due to Miller [88], the elliptic curve is lifted to a global field and the factor base is comprised of points of small height. In Semaev's proposal [109] for elliptic curves over prime fields, the factor base consists of points that have small x-coordinates. Gaudry [55] considered factor bases that consist of all points whose x-coordinates belong to a subfield of the underlying field K. Finally, in Diem's method [29], the factor base is the set of all points whose x-coordinates lie in a particular subspace of K.

We should mention that most deployments of elliptic curve cryptography use elliptic curves over prime fields or characteristic two fields. Thus, from the point of view of practice the most interesting ECDLP instances are over these fields. For example, the FIPS 186-2 standard [38] for the elliptic curve digital signature algorithm recommends curves over the five prime fields with characteristic $2^{192} - 2^{64} - 1$, $2^{224} - 2^{96} + 1$, $2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$, $2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$, and $2^{521} - 1$. The special form of the primes enables fast modular reduction. Elliptic curves of prime order over these fields provide security levels of 2^{96}, 2^{112}, 2^{128}, 2^{192} and 2^{256}, respectively, in the sense that Pollard's rho method for the ECDLP takes roughly this many

[6]All genus 2 curves are hyperelliptic.

steps. FIPS 186-2 also recommends elliptic curves over the five characteristic two fields $\mathbb{F}_{2^{163}}$, $\mathbb{F}_{2^{233}}$, $\mathbb{F}_{2^{283}}$, $\mathbb{F}_{2^{409}}$ and $\mathbb{F}_{2^{571}}$.

3.3.1. *Miller's index-calculus attack on the ECDLP.* In his 1985 paper [88], Miller considered a possible index-calculus attack on the ECDLP for an elliptic curve E defined over a prime field $\mathbb{F}_p$. In Miller's attack, E is lifted to an elliptic curve $\widetilde{E}$ over the rational numbers $\mathbb{Q}$; i.e., reducing the coefficients of $\widetilde{E}$ modulo p yields E. The factor base $\mathcal{F}$ is then defined to be the points of small height in $\widetilde{E}(\mathbb{Q})$. (The height of a point is related to the number of bits needed to represent the point.) However, Miller argued (see also [114]) that there are very few points of small height in $\widetilde{E}(\mathbb{Q})$. Moreover, finding an efficient method for lifting a point in $E(\mathbb{F}_p)$ to a point in $\widetilde{E}(\mathbb{Q})$ (which is required to map the ECDLP instance from $E(\mathbb{F}_p)$ to $\widetilde{E}(\mathbb{Q})$) looks hopeless.

Silverman [113] proposed a variant of Miller's attack whereby points in $E(\mathbb{F}_p)$ are first lifted to $\mathbb{Q}\times\mathbb{Q}$, after which an elliptic curve passing through these points is found. It was subsequently shown [68] that Silverman's attack is virtually certain to be much slower than Pollard's rho algorithm.

3.3.2. *Semaev's index-calculus attack on the ECDLP.* Suppose that E is an elliptic curve defined over a prime field $\mathbb{F}_p$, and that elements of $\mathbb{F}_p$ are represented as integers in the interval $[0, p-1]$. For simplicity, we will assume that $E(\mathbb{F}_p)$ is cyclic. Semaev [109] considered a factor base

$$\mathcal{F} = \{(x, y) \in E(\mathbb{F}_p) \ : \ 0 \leq x \leq p^{1/n}\}$$

for some fixed integer $n \geq 2$. Roughly half of all $x \in \mathbb{F}_p$ are x-coordinates of (two) points in $E(\mathbb{F}_p)$; hence $\#\mathcal{F} \approx p^{1/n}$.

In the relation generation stage, one attempts to write a randomly selected point $R \in E(\mathbb{F}_p)$ as a sum of points in $\mathcal{F}$. To accomplish this, Semaev introduced the notion of a summation polynomial[7].

Definition 1. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{F}_q$, where the characteristic of $\mathbb{F}_q$ is neither 2 nor 3. The *summation polynomials* $f_n \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ for $n \geq 2$ are defined as follows:

(i) $f_2(x_1, x_2) = x_1 - x_2$.
(ii) $f_3(x_1, x_2, x_3) = (x_1 - x_2)^2 x_3^2 - 2((x_1 + x_2)(x_1 x_2 + a) + 2b)x_3 + ((x_1 x_2 - a)^2 - 4b(x_1 + x_2))$.
(iii) $f_n(x_1, x_2, \ldots, x_n) = \mathrm{Res}_x(f_{n-1}(x_1, \ldots, x_{n-2}, x), f_3(x_{n-1}, x_n, x))$ for $n \geq 4$ where $\mathrm{Res}_x(f, g)$ is the resultant of the polynomials f and g in x.

The algebraic closure of $\mathbb{F}_q$ is denoted by $\overline{\mathbb{F}}_q$.

Theorem 2 ([109])**.** Summation polynomials have the following properties:

[7]Summation polynomials can also be defined for elliptic curves over finite fields of characteristic 2 and 3.

(i) $(x_1, \ldots, x_n) \in \overline{\mathbb{F}}_q^n$ is a root of f_n if and only if there exists $(y_1, \ldots, y_n) \in \overline{\mathbb{F}}_q^n$ such that $P_i = (x_i, y_i) \in E(\overline{\mathbb{F}}_q)$ and $\sum_{i=1}^n P_i = \infty$.
(ii) f_n is symmetric.
(iii) The degree of f_n in x_i is 2^{n-2}.

One way to decompose $R = (x_R, y_R)$ in $\mathcal{F}$ is to find solutions $(x_1, \ldots, x_n) \in \mathbb{F}_p^n$ to

$$f_{n+1}(x_1, x_2, \ldots, x_n, x_R) \equiv 0 \pmod{p}, \text{ such that } x_i \leq p^{1/n}. \tag{7}$$

If such a solution exists and can be found, then one finds the corresponding y-coordinates $\pm y_i$. Suppose that each $y_i \in \mathbb{F}_p$. Then each $P_i = (x_i, y_i)$ is in $\mathcal{F}$ and by Theorem 2(i) there exist $s_i \in \{-1, 1\}$ such that $s_1 P_1 + \cdots + s_n P_n = R$. The sign bits s_i can be found by exhaustive search, thereby yielding a relation.

Now, a reasonable approximation for the size of the set $\{P_1 + P_2 + \cdots + P_n : P_i \in \mathcal{F}\}$ is $p/n!$. Thus the expected number of points R that have to be selected before a relation is obtained is about $n!$. Since a sparse system of u linear equations in u variables can be solved in $O(u^2)$ steps, it follows that the heuristic expected running time of Semaev's algorithm is

$$O(T_{n,p} n! p^{1/n} + p^{2/n}), \tag{8}$$

where $T_{n,p}$ is the time to find the desired small roots in (7).

Fix a value of n. Let us imagine for the moment that there could be an algorithm for solving equation (7) whose complexity as $p \to \infty$ is $T_{n,p} = O(p^{1/n})$. Then the heuristic running time of Semaev's algorithm would be $O(p^{2/n})$. This would be less than the asymptotic running time $(\pi p/2)^{1/2}$ of Pollard's rho algorithm for $n \geq 5$. Since the hidden constants in the running time expression $O(p^{2/n})$ for Semaev's algorithm grow very rapidly with n, the comparison with Pollard's rho algorithm would only be accurate as $p \to \infty$.

Unfortunately, no efficient algorithm is known for solving the polynomial equation (7) even for $n = 5$ (in which case the equation has degree 16 in each of its 5 variables). There is some evidence that such algorithms may exist. For example, Coppersmith [26] devised efficient algorithms for finding small integer solutions to a polynomial in a single variable modulo an integer, and to a polynomial in two variables over the integers. Coppersmith also mentions that his method sometimes extends to more variables. However, current methods are not able to solve equation (7). Nevertheless, it is intriguing that the intractability of the ECDLP depends to some degree on the hardness of finding small solutions to polynomial equations modulo p.

3.3.3. *Gaudry's index-calculus attack on the ECDLP.* Suppose that E is an elliptic curve defined over a finite field $K = \mathbb{F}_{q^n}$ with $n > 1$, and for simplicity assume that $E(\mathbb{F}_{q^n})$ is cyclic. Gaudry [55] considered a factor base

$$\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{q^n}) \ : \ x \in \mathbb{F}_q\}$$

so that $\#\mathcal{F} \approx q$.

In the relation generation stage, one attempts to decompose a randomly selected point $R \in E(\mathbb{F}_{q^n})$ as a sum of points in $\mathcal{F}$. Gaudry observed that this can be accomplished by finding solutions $(x_1, x_2, \ldots, x_n)$ to

$$f_{n+1}(x_1, x_2, \ldots, x_n, x_R) = 0, \text{ such that } x_j \in \mathbb{F}_q, \tag{9}$$

where f_{n+1} is the $(n+1)$st summation polynomial. Note that $f_{n+1} \in \mathbb{F}_{q^n}[x_1, \ldots, x_n]$ since E is defined over $\mathbb{F}_{q^n}$ and since $x_R \in \mathbb{F}_{q^n}$. The conditions $x_j \in \mathbb{F}_q$ in (9) can be expressed algebraically as follows. Select a basis $\{\lambda_1, \ldots, \lambda_n\}$ for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and write x_R and the coefficients of the defining equation for E that appear in the expression $f_{n+1}(x_1, \ldots, x_n, x_R)$ in terms of this basis. Expanding (9) and equating coefficients of the λ_i yields n polynomial equations

$$g_i(x_1, \ldots, x_n) = 0, \text{ for } 1 \leq i \leq n, \tag{10}$$

where $g_i \in \mathbb{F}_q[x_1, \ldots, x_n]$ and the degree of g_i in x_j is at most 2^{n-1}. The solutions $x_j \in \mathbb{F}_q$ to (10) can be found by finding a Gröbner basis for the ideal generated by the g_i, and then finding roots of a sequence of univariate polynomials each of which has degree at most $2^{n(n-1)}$. This is predicted to take time $O(2^{cn(n-1)})$ for some constant c.

The size of the set $\{P_1 + P_2 + \cdots + P_n : P_i \in \mathcal{F}\}$ is approximately $q^n/n!$. Thus the expected number of points R that have to be selected before a relation is obtained is about $n!$. It follows that the heuristic expected running time of Gaudry's index-calculus algorithm is

$$O(2^{cn(n-1)} n! q + q^2). \tag{11}$$

This is exponential in terms of n and $\log q$. However, for fixed n, the running time can be expressed as $O(q^2)$. Thus, for any fixed $n \geq 5$, Gaudry's algorithm for solving the ECDLP over $\mathbb{F}_{q^n}$ is asymptotically faster than Pollard's rho method.

The double large prime idea from the GTT algorithm in §3.2 can also be applied here, thereby reducing the running time of Gaudry's ECDLP algorithm to

$$O(q^{2-\frac{2}{n}}). \tag{12}$$

Hence Gaudry's algorithm is asymptotically faster than Pollard's algorithm even for $n = 3$ and $n = 4$. The constant in the expression (12) is the smallest for $n = 3$. For this case, it is possible that Gaudry's algorithm is indeed faster in practice than Pollard's rho method for values of q that are of practical interest ($2^{160} \leq q^3 \leq 2^{512}$). However further experimentation is needed before this can be decided.

3.3.4. *Diem's index-calculus attack on the ECDLP.* We can view $K = \mathbb{F}_{q^n}$ as an n-dimensional vector space over $\mathbb{F}_q$. In Gaudry's algorithm, the factor base consists of points whose x-coordinates belong to the one-dimensional

subspace $\mathbb{F}_q$. Diem [29] generalized Gaudry's algorithm by considering factor bases of points whose x-coordinates belong to a subspace of arbitrary dimension. We consider a simplified version of Diem's algorithm below.

Suppose that E is an elliptic curve defined over K, and for simplicity assume that $E(K)$ is cyclic. Let $e \geq 3$ be an integer, and define $m = \lceil \frac{n}{e} \rceil$. We randomly select linearly independent $\alpha_1, \ldots, \alpha_m \in K$ and define the m-dimensional subspace $K_m = \langle \alpha_1, \ldots, \alpha_m \rangle$. The factor base is

$$\mathcal{F} = \{(x, y) \in E(K) \ : \ x \in K_m\}$$

so that $\#\mathcal{F} \approx q^m$.

In the relation generation stage, one attempts to decompose a randomly selected point $R \in E(K)$ as a sum of points in $\mathcal{F}$ by finding solutions $(x_1, x_2, \ldots, x_e)$ to

$$f_{e+1}(x_1, x_2, \ldots, x_e, x_R) = 0, \text{ such that } x_i \in K_m. \tag{13}$$

The conditions $x_i \in K_m$ can be expressed algebraically by writing $x_i = x_{i,1}\alpha_1 + x_{i,2}\alpha_2 + \cdots + x_{i,m}\alpha_m$, where the $x_{i,j}$ are new variables which take on values in $\mathbb{F}_q$. Then α_j, x_R and the coefficients of the defining equation for E are written in terms of a basis $\{\lambda_l\}$ for K over $\mathbb{F}_q$. Expanding (13) and equating coefficients of the λ_l yields n polynomial equations

$$g_l(\{x_{i,j}\}) = 0, \text{ for } 1 \leq l \leq n, \tag{14}$$

in em variables, where $g_l \in \mathbb{F}_q[\{x_{i,j}\}]$. As with Gaudry's algorithm, the solutions $x_{i,j} \in \mathbb{F}_q$ to (14) yield solutions $x_i \in K_m$ to (13).

Under some reasonable heuristics, Diem [29] shows that if a, b are constants with $0 < a < b$, then his index-calculus method (with $e \approx \sqrt{\log q}$) has subexponential expected running time $L_{q^n}[\frac{3}{4}, c]$ for $a \log q \leq n \leq b \log q$. Here c is a constant that depends on a and b. It remains to be seen whether Diem's method has any practical implications; the ECDLP over characteristic two finite fields of composite extension degree is of special interest because elliptic curves over such fields have been considered in real-world deployments of elliptic curve cryptography.

4. Links

Instead of directly solving the DLP in a cyclic group G, one may try to (efficiently) embed G in another group H for which faster DLP solvers may be known. An obvious necessary condition for such an embedding to exist is that $\#G$ divide $\#H$. In this section we present embedding results for the case where G is (a subgroup of) the divisor class group of an elliptic curve E over a finite field $\mathbb{F}_q$. Four kinds of embeddings are considered:

- §4.1 Embeddings of $E(\mathbb{F}_q)$ in the multiplicative group $\mathbb{F}_{q^k}^*$ of an extension of $\mathbb{F}_q$.
- §4.2 Mappings from $E(\mathbb{F}_q)$ to $E'(\mathbb{F}_q)$ where E' is an elliptic curve over $\mathbb{F}_q$ with the same number of points as E.

§4.3 Embeddings of $E(\mathbb{F}_q)$ in the divisor class group of a (higher genus) hyperelliptic curve defined over $\mathbb{F}_q$.
§4.4 Embeddings of $E(\mathbb{F}_q)$ in the divisor class group of a (higher genus) hyperelliptic curve defined over a proper subfield of $\mathbb{F}_q$.

4.1. **The Weil and Tate pairings.** Many readers will be familiar with the Weil pairing on an elliptic curve. To recall, let E be an elliptic curve over a field $K = \mathbb{F}_q$, and let r be a positive integer that is coprime to the characteristic of K. Let $\overline{K}$ denote the algebraic closure of K. The set of all r-torsion points in $E(\overline{K})$ is denoted by $E[r]$; it is known that $E[r] \cong (\mathbb{Z}/r\mathbb{Z}) \oplus (\mathbb{Z}/r\mathbb{Z})$. Denote by $\mu_r \subset \overline{K}^*$ the group of r-th roots of 1. The *Weil pairing* is a function

$$e_r : E[r] \times E[r] \to \mu_r$$

which satisfies the following properties (see [112, §III.8]).

(1) Bilinear: $e_r(S_1 + S_2, T) = e_r(S_1, T)e_r(S_2, T)$ and $e_r(S, T_1 + T_2) = e_r(S, T_1)e_r(S, T_2)$.
(2) Non-degenerate: For all $P \in E[r]$ except $P = \infty$, there is some point $Q \in E[r]$ such that $e_r(P, Q) \neq 1$.
(3) Alternating: $e_r(P, P) = 1$ and so $e_r(P, Q) = e_r(Q, P)^{-1}$.

A closely related pairing due to Tate (which was presented in a more explicit form by Lichtenbaum) was introduced to the cryptographic community by Frey and Rück [42] (also see [41]).

The Tate pairing[8] for a curve C over a field $K = \mathbb{F}_q$ is defined as follows. Let D_1 be a divisor representing a class in $\mathrm{Pic}^0_K(C)$ such that rD_1 is principal, and denote by f a function such that $(f) = rD_1$. Let D_2 be any divisor defined over K such that D_1 and D_2 have disjoint support. (One can show that in every divisor class there is a divisor D_2 with support disjoint to D_1.) If $D_2 = \sum_{P \in C} n_P(P)$, then we define

$$f(D_2) = \prod_{P \in C} f(P)^{n_P}.$$

The *Tate pairing* of D_1 and D_2 is defined as

$$\langle D_1, D_2 \rangle_r = f(D_2).$$

One can show that the Tate pairing is well defined as a map

$$\langle \cdot, \cdot \rangle_r \ : \ \mathrm{Pic}^0_K(C)[r] \times \mathrm{Pic}^0_K(C)/r\mathrm{Pic}^0_K(C) \to (K^*)/(K^*)^r.$$

It satisfies the following properties:

(1) Bilinear: $\langle D_1 + D_1', D_2 \rangle_r \equiv \langle D_1, D_2 \rangle_r \langle D_1', D_2 \rangle_r \pmod{(K^*)^r}$ and $\langle D_1, D_2 + D_2' \rangle_r \equiv \langle D_1, D_2 \rangle_r \langle D_1, D_2' \rangle_r \pmod{(K^*)^r}$.

[8]By the 'Tate pairing' on a curve C over a finite field $\mathbb{F}_{p^m}$ we mean the reduction modulo p of the local Tate pairing on a suitable lifting of C to a local field.

(2) Non-degenerate: If $r \mid (q-1)$ then for all $D_1 \in \mathrm{Pic}^0_K(C)[r]$ except the zero divisor class, there is some divisor $D_2 \in \mathrm{Pic}^0_K(C)$ such that $\langle D_1, D_2 \rangle_r \not\equiv 1 \pmod{(K^*)^r}$.

The relationship between the Tate pairing and the Weil pairing is the following. Let E be an elliptic curve over a field $K = \mathbb{F}_q$ such that $E[r] \subset E(K)$ and $r^3 \nmid \#E(K)$. These conditions imply that the points in $E[r]$ may be taken as representatives for the classes $E(K)/rE(K)$. Then if $P, Q \in E[r]$ we have

$$e_r(P,Q) \equiv \langle P,Q\rangle_r / \langle Q,P\rangle_r \pmod{(K^*)^r}.$$

This relation shows that the Tate pairing is usually not symmetric. The fact that the Tate pairing is only defined modulo $(K^*)^r$ is often inconvenient. Hence we usually use the reduced pairing

$$e(P,Q) = \langle P,Q\rangle_r^{(q-1)/r}. \tag{15}$$

The Weil and Tate pairings can be efficiently computed using Miller's algorithm [89] and its variants (e.g., see [11, 48, 32, 34]).

4.1.1. *Weil and Tate pairing attacks.* Suppose now that E is an elliptic curve defined over $\mathbb{F}_q$, and that $\#E(\mathbb{F}_q) = dr$ where r is prime and the co-factor d is small. We further assume that r is not equal to the characteristic of $\mathbb{F}_q$. Our task is to find $\log_P Q$ where $P \in E(\mathbb{F}_q)$ has order r and $Q \in \langle P \rangle$.

Let k be the smallest positive integer for which $q^k \equiv 1 \pmod{r}$. The Weil and Tate pairings (taking $K = \mathbb{F}_{q^k}$ in the above) can be used to embed $\langle P \rangle$ into $\mathbb{F}^*_{q^k}$ [42, 83]. For this reason, k is called the *embedding degree* of $\langle P \rangle$.

Let e denote either the Weil pairing or the reduced Tate pairing (15). The attack proceeds as follows. Choose a point $R \in E$ such that $e(P,R) \neq 1$. The existence of such a point R is guaranteed by non-degeneracy. For the Weil pairing one should take $R \in E[r]$ while for the Tate pairing one can take $R \in E(\mathbb{F}_{q^k})$.[9] Now, bilinearity implies that $S \mapsto e(S,R)$ is an embedding of $\langle P \rangle$ into $\mathbb{F}^*_{q^k}$. To solve the ECDLP instance, one computes $\alpha = e_r(P,R)$ and $\beta = e_r(Q,R)$, and then finds $\log_\alpha \beta$ in $\mathbb{F}^*_{q^k}$ using one of the index-calculus techniques mentioned in §3.1.

One has $k \approx r-1$ for most elliptic curves defined over $\mathbb{F}_q$ (since k is the multiplicative order of q modulo r). For these curves, the reduction is useless because even the arithmetic in $\mathbb{F}_{q^k}$ takes exponential time in terms of the time to perform arithmetic in $\mathbb{F}_q$. However, some special classes of elliptic curves do have small embedding degrees, e.g., supersingular curves[10] all of which have $k \leq 6$. For such elliptic curves, the Weil and Tate pairing reductions yield a subexponential-time ECDLP solver.

Example 3. Consider the supersingular elliptic curve $E : y^2 + y = x^3 + x + 1$ over $K = \mathbb{F}_q = \mathbb{F}_{2^n}$ where n is odd. Then $\#E(\mathbb{F}_2) = 1$, and Weil's theorem

[9] If $r \nmid (q-1)$ then $E[r] \subset E(\mathbb{F}_{q^k})$ [9].

[10] An elliptic curve E defined over a finite field $\mathbb{F}_q$ of characteristic p is *supersingular* if p divides $q+1-\#E(\mathbb{F}_q)$; otherwise, the curve is said to be *non-supersingular* or *ordinary*.

[112, §V.2] shows that $\#E(\mathbb{F}_q) = q + 1 - \sqrt{2q}$ if $n \equiv 1, 7 \pmod 8$, and $\#E(\mathbb{F}_q) = q+1+\sqrt{2q}$ if $n \equiv 3, 5 \pmod 8$. By Schoof's results on the group structure of supersingular elliptic curves [106], we know that $E(\mathbb{F}_q)$ is cyclic. Now,

$$q^4 - 1 = (q-1)(q+1)(q+1+\sqrt{2q})(q+1-\sqrt{2q}).$$

Thus the embedding degree is $k = 4$ and the Weil and Tate pairings can be used to efficiently reduce the ECDLP in $E(\mathbb{F}_q)$ to the DLP in $\mathbb{F}^*_{q^4}$.

Immunity to the Weil and Tate pairing attacks can be assured by checking that r does not divide $q^k - 1$ for all small k for which the DLP in $\mathbb{F}^*_{q^k}$ is considered tractable. One could also avoid the Weil and Tate pairing attacks by selecting an elliptic curve E over a prime field $\mathbb{F}_p$ such that $\#E(\mathbb{F}_p)$ is divisible by p (which by (2) implies that $\#E(\mathbb{F}_p) = p$). Unfortunately for such curves, the ECDLP in $E(\mathbb{F}_p)$ can be efficiently solved [103, 108, 115, 100].

4.2. **Isogenous elliptic curves.** An isogeny is a map which preserves both geometry and arithmetic. More precisely, let E_1 and E_2 be elliptic curves over a field K. An isogeny is a morphism $\psi : E_1 \to E_2$ such that $\psi(\infty_{E_1}) = \infty_{E_2}$ ([112, §III.4]). It can be shown that every such map is a group homomorphism. The degree of an isogeny is essentially the number of points in its kernel[11]. The endomorphism ring $\mathrm{End}(E)$ is the ring of all isogenies from E to itself.

One of the most important invariants under isogeny is the number of points. Indeed, the following result holds.

Theorem 4. Let E_1 and E_2 be elliptic curves over $K = \mathbb{F}_q$. Then there is a (nonzero) isogeny $\psi : E_1 \to E_2$ defined over K if and only if $\#E_1(K) = \#E_2(K)$.

This result is often known as Tate's isogeny theorem, but in the elliptic curve case it was already known to be true due to results of Deuring [27] on the endomorphism structure of elliptic curves over finite fields. Galbraith [44] (see also [49] and [70]), building on work of Kohel, Elkies, Atkin and Vélu, gave an algorithm for computing such an isogeny. If the conductor (essentially, the square part of $t^2 - 4q$ where $t = q + 1 - \#E(\mathbb{F}_q)$) is smooth, then Galbraith's algorithm has an expected running time of $O(q^{1/4})$.

Suppose now that E_1 and E_2 are isogenous elliptic curves that are cryptographically interesting in that $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q) = dr$ where r is prime and d is small. Galbraith's algorithm produces a composition of isogenies of low degree, so if r is a large prime then the kernel of the resulting isogeny $\psi : E_1 \to E_2$ does not contain the order-r subgroup of $E_1(\mathbb{F}_q)$. Hence ψ can be used to map the DLP in $E_1(\mathbb{F}_q)$ to that in $E_2(\mathbb{F}_q)$.

[11]This is true if the isogeny is separable. For the general case, see for example [112, §III.4].

There are many things which are not necessarily invariant under isogeny, such as the group structure of an elliptic curve and the magic number m in a Weil descent attack. We will give more details about the Weil descent application in §4.4.2, but for now we mention some other cryptographic applications of isogenies: efficient point exponentiation [24]; defence against side-channel attacks [116, 2]; and distortion maps for pairing applications [52].

4.3. **Hyperelliptic curves.** Bauer and Hamdy [14] observed that for any positive integer n, the DLP in an elliptic curve over a finite field K can be efficiently reduced to the DLP in the divisor class group of a hyperelliptic curve of genus $g = \lfloor n + \frac{n-1}{2} \rfloor$ also defined over K.

Let $K = \mathbb{F}_q$ be a finite field of characteristic $p \neq 2, 3$, and let E be an elliptic curve defined over K with defining equation $y^2 = x^3 + ax + b$. We further assume that $b \neq 0$. For any odd positive integer n not divisible by p,[12] the curve defined by

$$C_n \ : \ y^2 = x^{3n} + ax^n + b \tag{16}$$

is a hyperelliptic curve of genus $g = (3n-1)/2$ over K. Bauer and Hamdy [14] showed that the map $\Omega_n : E(K) \to \mathrm{Pic}^0_K(C_n)$ defined by

$$\Omega_n \ : \ (u, v) \mapsto \mathrm{div}(x^n - u, v) \tag{17}$$

in an injective homomorphism. Thus, instances of the ECDLP in $E(K)$ can be efficiently mapped to instances of the HCDLP in $\mathrm{Pic}^0_K(C_n)$.

For example, if $n = 3$ then we can efficiently embed $E(K)$ in the divisor class group of a hyperelliptic curve C_3 of genus $g = 4$ over K. This does not make solving the DLP in $E(K)$ any easier since the Gaudry-Thériault-Thomé algorithm (see §3.2) for solving the DLP in $\mathrm{Pic}^0_{C_3}(K)$ has running time $O(q^{3/2})$, which is slower than Pollard's rho method for $E(K)$. Nevertheless the embedding establishes that the existence of an $L_{q^4}[d, c]$ subexponential-time algorithm for the HCDLP in genus 4 hyperelliptic curves over $\mathbb{F}_q$ implies the existence of an $L_q[d, c']$ subexponential-time algorithm for the ECDLP over $\mathbb{F}_q$. (A similar statement can be made for any fixed genus of the form $\lfloor n + \frac{n-1}{2} \rfloor$.) Interestingly, the converse statement is not known to be true.

In contrast to the embedding (17), Weil descent attacks attempt to embed $E(K)$ in the divisor class group of a hyperelliptic curve defined over a proper subfield of K.

4.4. **Weil descent attacks.** In 1998, Frey (see [41]) proposed a novel approach to attack the ECDLP in elliptic curves E over finite fields $\mathbb{F}_{q^n}$. He suggested to find curves X of low genus in the 'Weil restriction of scalars'

[12] It is possible to generalize this idea so that it applies to all p and n; see [14] for the full details.

W_E of E with respect to $\mathbb{F}_{q^n}/\mathbb{F}_q$. One has $E(\mathbb{F}_{q^n}) \simeq W_E(\mathbb{F}_q)$ and can hopefully map the DLP from $W_E(\mathbb{F}_q)$ to $\mathrm{Pic}^0_{\mathbb{F}_q}(X)$. This approach is known to cryptographers as the 'Weil descent methodology'.

4.4.1. *General methodology.* Building on work of Gaudry, Hess and Smart [56], Diem [28] showed that Frey's Weil descent methodology could be formulated using only coverings of curves. We present the Weil descent methodology in this 'covering attacks' formulation.

Let $k = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n}$. Let C be a curve defined over K. Suppose we are trying to solve the discrete logarithm problem in $\mathrm{Pic}^0_K(C)$.

The idea of a covering attack is to find a smooth curve X defined over k such that there is a non-constant rational map $f : X \to C$ which is defined over K. It is well-known that f induces a map (which is also a group homomorphism) $f^* : \mathrm{Pic}^0_K(C) \to \mathrm{Pic}^0_K(X)$ (see [112, §II.3]). There is also a map $N_{K/k} : \mathrm{Pic}^0_K(X) \to \mathrm{Pic}^0_k(X)$ which maps a divisor D to the sum of Galois-conjugates of D. In the ideal class group setting this map is a product of ideals and so is called a norm. We retain this terminology in the divisor class group setting.

Composing $N_{K/k}$ with f^* gives a group homomorphism from the original group $\mathrm{Pic}^0_K(C)$ to the group $\mathrm{Pic}^0_k(X)$ of divisor classes on X over the small field k. This map is called the "conorm-norm map" in the Weil descent literature.

There is a possibility that the original discrete logarithm problem will lie in the kernel of $N_{K/k} \circ f^*$. For example, suppose the original curve C is actually defined over k and the map f is also defined over k (note that the curve X is over k by definition). Then we have the commuting diagram

$$\begin{array}{ccc} \mathrm{Pic}^0_K(C) & \xrightarrow{f^*} & \mathrm{Pic}^0_K(X) \\ \Big\downarrow{\scriptstyle N_{K/k}} & & \Big\downarrow{\scriptstyle N_{K/k}} \\ \mathrm{Pic}^0_k(C) & \xrightarrow{f^*} & \mathrm{Pic}^0_k(X) \end{array}$$

and, since a divisor class in $\mathrm{Pic}^0_K(C)$ of large prime order will have norm zero, it follows that the interesting subgroup is in the kernel.

In many cases, however, the conorm-norm map will preserve the DLP instance. Hence, the discrete logarithm problem in $\mathrm{Pic}^0_K(C)$ can be transferred to a discrete logarithm problem in $\mathrm{Pic}^0_k(X)$. This latter discrete logarithm problem may be solved using an index-calculus algorithm.

The remaining question is how to construct suitable curves X over k. The GHS Weil descent attack addresses this question for elliptic curves defined over characteristic two finite fields.

4.4.2. *GHS Weil descent attack.* The seminal paper of Gaudry, Hess and Smart [56] gave the first practical examples of the Weil descent methodology. We give a rough outline of their approach here.

Let $N = ln$, $q = 2^l$, $k = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n} = \mathbb{F}_{2^N}$. Consider the ordinary elliptic curve E defined over K by the equation

$$E \ : \ y^2 + xy = x^3 + ax^2 + b.$$

We assume that $\#E(K) = dr$ where d is small (e.g., $d = 2$ or 4) and r is prime; hence $r \approx q^n$. We also assume that the following condition holds:

$$n \text{ is odd}, \ \text{ or } \mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0, \ \text{ or } (x+1)^u \mid \mathrm{Ord}_b, \tag{18}$$

where $2^u || n$ and Ord_b is the polynomial $f = \sum c_i x^i \in \mathbb{F}_2[x]$ of least degree such that $\sum c_i b^{q^i} = 0$.

The function field of E is $K_E = K(x, y)$. The change of variables $y = xs + \sqrt{b}$ transforms the equation for E into Artin-Schreier form

$$s^2 + s = x + a + \sqrt{b}/x.$$

Let σ be the q-power Frobenius map, which generates $\mathrm{Gal}(K/k)$. Write $a_i = \sigma^i(a)$ and $b_i = \sigma^i(b)$ for $i = 0, 1, \ldots, n-1$. One can form the function field[13] $F = K(x, s_0, \ldots, s_{n-1})$ where the s_i are defined by the equations

$$s_i^2 + s_i = x + a_i + \sqrt{b_i}/x$$

for $i = 0, \ldots, n-1$. Since this field is defined as a sequence of quadratic Artin-Schreier extensions it has degree over $K(x)$ equal to a power of 2; let $[F : K(x)] = 2^m$. The number $m \in [1, n]$ is often referred to as the 'magic number'. Gaudry, Hess and Smart [56] proved that

$$m = m(b) = \dim_{\mathbb{F}_2} \left(\mathrm{Span}_{\mathbb{F}_2} \left\{ (1, b_0^{1/2}), (1, b_1^{1/2}), \ldots, (1, b_{n-1}^{1/2}) \right\} \right). \tag{19}$$

Here, $b_i^{1/2}$ is viewed as an N-dimensional vector over $\mathbb{F}_2$.

Now F is the function field of some curve Y over K. Lemma 9 of [56] shows that in fact Y is a hyperelliptic curve of genus 2^{m-1} or $2^{m-1} - 1$. Under condition (18) one can show [56] that the action of $\mathrm{Gal}(K/k)$ extends to F and that if F' is the fixed field of F with respect to $\mathrm{Gal}(K/k)$ then F' is the function field of a curve X over k and F is the function field of X over K. It follows that X is birationally equivalent to Y over K and that we are in exactly the framework of a covering attack.

In [56] it is explained how to obtain an explicit hyperelliptic equation for X. In [28, 62] it is shown that, under certain conditions, the kernel of the conorm-norm map has order a power of 2, and so it preserves the discrete logarithm problem in subgroups of large prime order.

[13] Here we use the notation $K(a_1, \ldots, a_m)$ to represent the field generated over K by the a_i.

4.4.3. *Extending the GHS attack.* Galbraith, Hess and Smart [49] used isogenies to extend the reach of the GHS attack. They observed that the magic number m can be different for isogenous elliptic curves. If one is given an elliptic curve E over K for which the GHS attack is not effective then there are two ways to proceed.

The first way is to perform a random walk in the isogeny class of E (i.e., at each step choose a small prime l and construct a 'random' l-isogeny from the current elliptic curve to another one). At each step one checks if the elliptic curve obtained yields a small m, in which case the GHS attack can be applied.

The other way to proceed is to enumerate the curves with small m. For each such curve E_i one can check whether E_i is isogenous to the target curve E. This is easily done by taking a random point $P \in E_i(K)$ and testing to see if $MP = 0$ where $M = \#E(K)$; if this is true then it is likely that $\#E_i(K) = \#E(K)$ in which case the curves are isogenous. If a match is found then one can construct an isogeny from E to E_1 using Galbraith's algorithm. Once the DLP has been transferred from E to E_1 it can be solved on E_1 using the GHS attack.

4.4.4. *Cryptographic implications.* In order for the GHS attack to be considered successful in attacking the ECDLP in $E(K)$, the DLP in $\mathrm{Pic}_k^0(X)$ should be solvable in less time than it takes to solve the ECDLP instance using Pollard's rho algorithm. In general, $m \approx n$ whence $g \approx 2^{n-1}$ and $\#\mathrm{Pic}_k^0(X) \approx q^{2^{n-1}}$ and the GHS attack fails. The GHS attack will only succeed if m is small, say $m \approx \log_2 n$, because then $g \approx n$ and $\#\mathrm{Pic}_k^0(X) \approx q^n$.

The formula (19) was analyzed in [84], and it was shown that the GHS attack fails for all elliptic curves over fields $\mathbb{F}_{2^N}$ where $N \in [160, 600]$ is prime. This is because the hyperelliptic curves X produced either have genus too small (and so the ECDLP instance lies in the kernel of the conorm-norm map), or have genus too large ($g \geq 2^{16} - 1$, whence the HCDLP in $\mathrm{Pic}_k^0(X)$ is infeasible).

However, the GHS attack has been shown to be successful for some elliptic curves over finite fields $\mathbb{F}_{2^N}$ where N is composite. The following example was given in [69].

Example 5. Let the elements of $\mathbb{F}_{2^{124}}$ be represented as polynomials in $\mathbb{F}_2[z]$ modulo the irreducible polynomial $z^{124} + z^{19} + 1$. Let $a = z^{105}$ and

$$\begin{aligned} b =& z^{108}+z^{106}+z^{102}+z^{101}+z^{99}+z^{93}+z^{87}+z^{85}+z^{75}+z^{70}+z^{68}+z^{67}+z^{66} \\ &+z^{64}+z^{62}+z^{59}+z^{58}+z^{56}+z^{55}+z^{54}+z^{53}+z^{51}+z^{50}+z^{49}+z^{48}+z^{46}+z^{45} \\ &+z^{44}+z^{42}+z^{41}+z^{40}+z^{33}+z^{32}+z^{29}+z^{27}+z^{24}+z^{23}+z^{22}+z^{20}+z^{18}+z^{16} \\ &+z^{15}+z^{14}+z^{9}+z^{8}+z^{7}+z^{6}+z^{3}+z^{2}+z. \end{aligned}$$

The elliptic curve $E : y^2 + xy = x^3 + ax^2 + b$ satisfies $\#E(\mathbb{F}_{2^{124}}) = 2r$ where

$$r = 10633823966279326985483775888689817121$$

is prime. Two points P and Q of order r were randomly selected from $E(\mathbb{F}_{2^{124}})$. Then Pollard's rho method for finding $\log_P Q$ is infeasible using existing computer technology. The GHS reduction with $n = 31$ was used to reduce the ECDLP instance (E, P, Q) to an HCDLP instance (C, D_P, D_Q), where $D_P, D_Q \in \mathrm{Pic}^0_{\mathbb{F}_{2^4}}(C)$ and C is a hyperelliptic curve of genus $g = 31$ over $\mathbb{F}_{2^4}$. The defining equation of C is $y^2 + h(x)y = f(x)$ where

$$f(x) = w^3x^{63} + w^7x^{60} + w^3x^{56} + w^3x^{48} + 1,$$
$$h(x) = w^9x^{31} + w^{12}x^{30} + w^8x^{28} + w^{13}x^{24} + w^6x^{16} + w^6,$$

and $\mathbb{F}_{2^4} = \mathbb{F}_2[w]/(w^4 + w + 1)$. We have $\#\mathrm{Pic}^0_{\mathbb{F}_{2^4}}(C) = 2r$.

The index-calculus algorithm described in §3.2 was used to solve the resulting HCDLP instance. A smoothness bound $t = 5$ was selected. This yielded a factor base $\mathcal{F}$ of size 113,728 that was generated in 12 minutes on a single Pentium III machine. The linear relations were generated using 379 days of total CPU time on a network of 208 workstations. Finally, the resulting linear system of equations was solved in 3 days on a single Pentium III machine.

The effectiveness of the GHS attack for composite $N \in [100, 600]$ was further analyzed in [81], where the elliptic curves most susceptible to the GHS attack were identified and enumerated. Finite fields $\mathbb{F}_{2^N}$ where N is divisible by 5 were shown in [86] to be *weak* for elliptic curve cryptography in the sense that the GHS attack can be used to solve the ECDLP significantly faster than Pollard's rho algorithm for all cryptographically interesting elliptic curves over these fields. For example, the ECDLP for all cryptographically interesting elliptic curves over $\mathbb{F}_{2^{600}}$ can be solved about 2^{69} times faster than it takes Pollard's rho method to solve the hardest instances.

4.4.5. *Generalizations.* The basic GHS attack has been generalized and extended in a number of ways.

Arita [6] used Weil descent to reduce the ECDLP over characteristic three finite fields to the DLP in C_{ab} curves. Galbraith [46] generalized the basic GHS attack to hyperelliptic curves over characteristic two finite fields. Diem [28] further generalized the GHS attack to hyperelliptic curves over finite fields of any characteristic and analyzed the properties of the resulting curves X in the odd characteristic case using Kummer theory (see also [120]).

A different generalization was given by Hess [62, 63] for the case of elliptic curves over characteristic two finite fields. Hess' idea is to consider different Artin-Schreier extensions of the form

$$s^2 + s = \beta x + \alpha + \gamma/x$$

(the original GHS method has $\beta = 1$). It happens that an elliptic curve E may be written in the above form with many different choices for α, β and γ. The number m can vary over these choices. The genus bounds are more

complicated and the resulting curves may not be hyperelliptic. Hess' generalized GHS attack has been thoroughly analyzed [63, 85] with the conclusion that fields $\mathbb{F}_{2^N}$ where N is divisible by 3, 5, 6, 7 or 8 are (potentially) weak and should not be used to implement elliptic curve cryptographic protocols.

5. Pairings

Beginning with Joux's work in 2000 [71] (see also [101]), bilinear pairings have become an indispensable tool for designing cryptographic protocols. They have been used to solve protocol problems that were open for many years. In many cases, the pairing-based protocols are very natural and are amenable to simple and convincing security proofs.

We begin in §5.1 by introducing some pairing-based protocols. In §5.2 we discuss some of the computational challenges involved in implementing pairings over elliptic curves. Some open questions about the DDHP are considered in §5.3.

5.1. **Cryptographic protocols using pairings.** Let n be a prime number. Let $G_1 = \langle P \rangle$ be an additively-written group of order n with identity ∞, G_2 be a multiplicatively-written group of order n with identity 1, and let $\hat{e} : G_1 \times G_1 \to G_2$ be a bilinear pairing that is non-degenerate (i.e., $\hat{e}(P, P) \neq 1$) and efficiently computable. In §§5.2 and 5.3 we will show how such bilinear pairings can be obtained by modifying the Tate pairing.

The security of many of the cryptographic protocols that use pairings is based on intractability of the following problem.

Definition 6. Let $\hat{e}$ be a bilinear pairing on (G_1, G_2). The *bilinear Diffie-Hellman problem (BDHP)* is the following: Given P, aP, bP, and cP, compute $\hat{e}(P, P)^{abc}$.

It is easy to see that hardness of the BDHP implies the hardness of the DHP (and also the DLP) in both G_1 and G_2. However, it is not known if the converse is true. For the remainder of this section, we will assume that BDHP is intractable. Examples of pairings for which the BDHP appears intractable will be provided in §5.2.

Note that intractability of BDHP does not imply intractability of the DDHP in G_1; in fact the latter problem can be efficiently solved. Given an instance (P, aP, bP, cP) of the DDHP in G_1, one can efficiently compute $\gamma_1 = \hat{e}(P, cP) = \hat{e}(P, P)^c$ and $\gamma_2 = \hat{e}(aP, bP) = \hat{e}(P, P)^{ab}$. Since $\hat{e}(P, P)$ has order n in G_2, one can then conclude that $cP = abP$ if and only if $\gamma_1 = \gamma_2$.

5.1.1. *One-round three-party key agreement.* The Diffie-Hellman key agreement scheme introduced in §1 can be viewed as a one-round protocol because the messages P_A and P_B exchanged between A and B are independent of each other. The existence of a one-round key agreement protocol involving three parties remained open until Joux [71] devised a simple protocol that uses a bilinear pairing $\hat{e}$ on (G_1, G_2) for which the BDHP is intractable. We present a slightly improved version of Joux's protocol due to Verheul [122].

In Joux's protocol, the three parties A, B, C randomly select secret integers $a, b, c \in [0, n-1]$, respectively. A broadcasts $P_A = aP$ to B and C, B broadcasts $P_B = bP$ to A and C, and C broadcasts $P_C = cP$ to A and B. All three parties can now compute the shared secret $K = \hat{e}(P,P)^{abc}$. For example, A can compute K as $\hat{e}(bP, cP)^a$. A passive adversary is faced with the task of computing K given P, P_A, P_B and P_C; this is precisely an instance of the BDHP. Note that the three messages P_A, P_B, P_C are independent of each other so Joux's scheme is indeed a one-round protocol.

Joux's protocol can be easily generalized to a one-round n-party key agreement protocol using an efficiently computable multilinear map $\hat{e}_n : G_1^{n-1} \to G_2$ for which the analogue of the BDHP is intractable (i.e., given $a_1P, a_2P, \ldots, a_nP$, computing $\hat{e}_n(P, P, \ldots, P)^{a_1 a_2 \cdots a_n}$ should be hard). However, Boneh and Silverberg [22] provided some evidence that for $n > 3$ it may not be possible to construct multilinear maps from algebraic geometry (also see [33]). The existence of a cryptographically suitable multilinear map for $n > 3$ remains an open question.

5.1.2. *Short signatures.* In most DL signature schemes, a signature consists of two group elements (or two integers modulo the group order). For example, in DSA [37], the underlying group $G = \langle \alpha \rangle$ is the subgroup of prime order q of the multiplicative group of the integers modulo a prime p. An entity A's private key is a randomly selected integer $x \in [0, q-1]$ and her public key is $\beta = \alpha^x \bmod p$. To sign a message m, A selects a random integer $k \in [1, q-1]$ and computes $r = (\alpha^k \bmod p) \bmod q$ and $s = k^{-1}(H(m)+xr) \bmod q$ where H is a cryptographic hash function. A's signature on m is the pair of integers (r, s). An entity in possession of A's public key β verifies the signature by checking that $r = (\alpha^{H(m)s^{-1}} \beta^{rs^{-1}} \bmod p) \bmod q$.

Several DL signature schemes with shorter signatures were known; for example, see [92, 96]. However, the existence of a DL signature scheme where signatures consist of a single group element was open until Boneh, Lynn and Shacham (BLS) [21] introduced the following signature scheme that uses a bilinear pairing $\hat{e}$ on (G_1, G_2).

Each entity A selects a random number $x \in [1, n-1]$; A's private key is x, while A's public key is $Q = xP$. To sign a message $m \in \{0,1\}^*$, A computes $M = H(m)$ where $H : \{0,1\}^* \to G_1 \setminus \{\infty\}$ is a cryptographic hash function, and $S = xM$. A's signature on m is S. Any entity who has an authentic copy of A's public key Q can verify the signature by computing $M = H(m)$ and checking that (P, Q, M, S) is a valid Diffie-Hellman quadruple. This is precisely an instance of the DDHP in G_1 which the verifier can solve by checking that $\hat{e}(P, S) = \hat{e}(Q, M)$. Note that a signature S consists of a single element in G_1.

An attacker who wishes to forge A's signature on a message m needs to solve the following problem: Given P, Q, $M = H(m)$, compute S such that $S = xM$. This is precisely an instance of the DHP in G_1. Thus the security of the BLS signature scheme depends on the hardness of the DHP in G_1.

5.1.3. *Identity-based encryption.* When using a public-key encryption scheme to send a message privately to A, user B encrypts the message using A's public key. A uses the private key corresponding to her public key to recover m. It is important that B have an authentic copy of A's public key. Otherwise, if an adversary can somehow induce B to use its public key instead of A's, then the adversary could decrypt messages that were intended only for A.

In practice, B obtains an authentic copy of A's public key from a *certificate*. Such a certificate consists of A's identifying information and public key, and a signature on this data generated by a *certifying authority* (CA). The authenticity of the certificate (and thus also A's public key) can be determined by using the CA's public key to verify the signature. Thus, B a priori only needs an authentic copy of the CA's public key.

There are many practical difficulties with managing public keys and certificates in large-scale deployments of public-key cryptography. In practice, it may be cumbersome for B to obtain A's certificate. Indeed, A may have not yet enrolled in the system and selected a public key. In order to alleviate some of the problems inherent with managing public keys and certificates, Shamir [110] in 1984 introduced the notion of *identity-based cryptography*. Here, a trusted-third party (TTP) has a public key and a private key. An entity A's public key consists of its identifying information ID_A (such as A's name or email address). The TTP uses her private key to generate A's private key, and securely transmits this to A. Clearly the TTP has to be well trusted since it knows all private keys. Any other entity can generate A's public key solely from ID_A, and without obtaining any authenticated data from A.

Shamir proposed an identity-based signature scheme in his 1984 paper. The existence of a practical identity-based encryption scheme remained open until Boneh and Franklin [19] proposed their elegant pairing-based scheme in 2001. This scheme is described next.

Let $\hat{e}$ be a bilinear pairing on (G_1, G_2) for which the BDHP is hard. Let H_1 be a cryptographic hash function that maps bit strings to $G_1 \setminus \{\infty\}$. The TTP selects a private key s at random from $[1, n-1]$, and computes its public key $Q = sP$. It is assumed that all entities have an authentic copy of Q. A's private key is $d_A = sQ_A$, where $Q_A = H_1(\mathrm{ID}_A)$. Note that computing d_A from (P, Q, Q_A) is an instance of the DHP in G_1. Thus the TTP is the only entity who can compute d_A.

An entity B encrypts a message $m \in G_2$ for A as follows. B randomly selects an integer $r \in [1, n-1]$ and computes $Q_A = H_1(\mathrm{ID}_A)$, $C_1 = rP$, and $C_2 = m + \hat{e}(Q_A, Q)^r$. B then sends the ciphertext (C_1, C_2) to A. Note that

$$\hat{e}(d_A, C_1) = \hat{e}(sQ_A, rP) = \hat{e}(Q_A, sP)^r = \hat{e}(Q_A, Q)^r.$$

Thus A can recover m from (C_1, C_2) by using her private key d_A to compute

$$m = C_2 - \hat{e}(d_A, C_1).$$

An attacker who tries to recover m from (C_1, C_2) has to compute $\hat{e}(Q_A, Q)^r$ from (P, Q_A, Q, C_1). This is precisely an instance of the BDHP.

5.2. **Pairing-friendly elliptic curves.** Bilinear pairings can be designed using the Weil or Tate pairings on elliptic curves. We will restrict our discussion to the Tate pairing because it is generally faster to evaluate than the Weil pairing, and also is more suitable when using curves of genus greater than 1.

There are two conditions that an elliptic curve E defined over $\mathbb{F}_q$ must satisfy in order to be considered suitable for pairing applications:

(1) $\#E(\mathbb{F}_q)$ should be divisible by a sufficiently large prime r so that the DLP in the order-r subgroup of $E(\mathbb{F}_q)$ is resistant to Pollard's rho attack (and other known attacks).
(2) Let k be the smallest positive integer such that $r \mid (q^k - 1)$. Then the embedding degree k should be sufficiently large so that the DLP in $\mathbb{F}_{q^k}^*$ withstands index-calculus attacks, but small enough that arithmetic in $\mathbb{F}_{q^k}$ can be efficiently implemented.

Supersingular elliptic curves provide good examples (cf. §4.1). The largest value for k that can be attained in the supersingular case is 6 and this can be realized using supersingular elliptic curves in characteristic three. For example, consider the supersingular curve E over $\mathbb{F}_3$ with defining equation $y^2 = x^3 - x + 1$ (cf. Example 9). Then for odd m, $E(\mathbb{F}_{3^m})$ has embedding degree $k = 6$. Since $\#E(\mathbb{F}_{3^{97}}) \approx 2^{151}$ is prime and the DLP in $\mathbb{F}_{3^{582}}$ is considered intractable, $E(\mathbb{F}_{3^{97}})$ is a viable candidate for pairing applications.

Supersingular curves of genus $g > 1$ can also be used, but there are still limitations on the embedding degrees which can be obtained (see [45, 99] for details).

If a value of k larger than 6 is preferred, then we are led to consider ordinary elliptic curves. We first consider whether suitable curves exist and then how to construct them.

5.2.1. *Existence.* The first results are due to Balasubramanian and Koblitz [9]. They considered the probability that a randomly chosen isogeny class of an elliptic curve E defined over $\mathbb{F}_p$ with $r = \#E(\mathbb{F}_p)$ a prime has embedding degree k (small). Note that they did not have to consider supersingular curves since such curves over $\mathbb{F}_p$ have $p + 1$ points (which is not prime) when $p \geq 5$. Their result is that if $M/2 \leq p \leq M$ and $k < (\log p)^2$ then the probability is at most $c(\log M)^9(\log\log M)^2/M$. Since there are $O(M/\log M)$ choices for p and $O(\sqrt{M})$ isogeny classes of curves for each p, it follows that the expected number of isogeny classes of elliptic curves over $\mathbb{F}_p$ with $M/2 \leq p \leq M$ and with embedding degree $\leq (\log M)^2$ is $O(\sqrt{M})$ (up to polynomial terms).

A related argument is given in [50]. Let $3 \leq k \leq (\log M)^2$. Then the expected number of pairs (q, n), where n is a possible group order (not necessarily prime) of an elliptic curve defined over $\mathbb{F}_q$, where $M/2 < q < M$

is a prime or prime power and where $n \mid (q^k - 1)$, is proportional to $\sqrt{M}$ (up to polynomial terms). This should be compared with the total number of pairs (q, n) without any embedding degree condition, which is $O(M^{3/2})$.

Note that when $k > 3$ then the supersingular curves only occur over fields of small characteristic and so they contribute a negligible proportion of examples. When $k = 3$ one gets supersingular curves over $\mathbb{F}_{p^2}$, but this again contributes only $O(\sqrt{M})$ many curves.

These arguments suggest that ordinary curves suitable for pairing-based cryptography do exist, but that they are rather scarce. For example, we believe that if $3 \leq k \leq (\log M)^2$ then only for $O(\sqrt{M})$ of the primes $p \leq M$ would there be curves over $\mathbb{F}_p$ with embedding degree k.

5.2.2. *Construction.* The problem of finding ordinary curves was considered by Miyaji, Nakabayashi and Takano (MNT) [90]. They presented explicit families of group orders of ordinary elliptic curves with embedding degree 3, 4 and 6.

More precisely, they give polynomials $q(l)$ and $t(l)$ in $\mathbb{Z}[l]$ such that the polynomial $n(l) = q(l)+1-t(l)$ divides the polynomial $\Phi_k(q(l))$, where $\Phi_k(x)$ is the k-th cyclotomic polynomial. For any integer l such that $q = q(l)$ is a prime (or prime power) and such that $|t(l)| \leq 2\sqrt{q}$, there is an elliptic curve E defined over $\mathbb{F}_q$ with $n(l)$ points and embedding degree k. The families they obtained are presented in Table 1. Due to the arguments presented in §5.2.1, we expect these families to be somewhat sparse, and this is perfectly reflected by the fact that the polynomials $q(l)$ are quadratic.

k	$q(l)$	$t(l)$	$n(l)$
3	$12l^2 - 1$	$-1 \pm 6l$	$12l^2 \pm 6l + 1$
4	$l^2 + l + 1$	$-l, l + 1$	$l^2 + 2l + 2, l^2 + 1$
6	$4l^2 + 1$	$1 \pm 2l$	$4l^2 \pm 2l + 1$

TABLE 1. MNT families of elliptic curves

Conjecturally these families contain an infinite number of primes or prime powers q. These results have been generalized by Scott and Barreto [107] and Galbraith, McKee and Valença [50]. More general ways to construct ordinary elliptic curves suitable for pairings with $k > 6$ have been given by several authors [12, 13, 23, 31]. The drawback of these methods is that the group orders of the elliptic curves produced generally have large co-factor d. For example, Brezing and Weng [23] construct elliptic curves defined over $\mathbb{F}_q$ with $k = 8$ and $k = 24$ and where the bitlength of d is approximately one-fifth the bitlength of q. An important research problem is to construct ordinary elliptic curves with embedding degree $6 < k < 32$ whose group orders are prime or almost prime.

A different approach to dealing with the limitations of supersingular curves has been adopted by Rubin and Silverberg [99]. They essentially

give a way to compress points in subgroups of supersingular curves which improves the bandwidth. As a result, one can take a supersingular curve over a larger field without paying such a bandwidth penalty, and this is similar to using an ordinary curve with a larger embedding degree.

5.3. **Distortion maps and DDHP.** Let E be an elliptic curve defined over $\mathbb{F}_q$, and let r be a prime such that $\gcd(r, q) = 1$. The set of r-torsion points $E[r]$ is a two dimensional vector space over $\mathbb{F}_r$. Recall that the Weil pairing is alternating (i.e., $e_r(P, P) = 1$ for all points $P \in E[r]$). Since the Tate pairing is defined on two different groups, it does not necessarily make sense to consider the value $\langle P, P\rangle_r$. However, in the cases most relevant to cryptography one can use $E[r]$ as representatives for the right hand argument, and so it is reasonable to consider the Tate pairing as being defined on $E[r] \times E[r]$. From now on we assume this is the case. The Tate pairing is not necessarily alternating, but there are plenty of situations where a point P paired with itself is trivial.

The bilinear pairings we need must satisfy $\hat{e}(P, P) \neq 1$ for certain points P. One very common way to ensure this is to 'twist' the Tate pairing by some endomorphism ψ. In other words, we define

$$\hat{e}(P, Q) \ := \ \langle P, \psi(Q)\rangle_r^{(q^k-1)/r}.$$

An endomorphism ψ such that $\langle P, \psi(P)\rangle_r \neq 1$ is called a *distortion map* for the point P. The aim of this section is to give some examples of distortion maps.

For the remainder of this section we consider the reduced Tate pairing $e(P, Q) = \langle P, Q\rangle_r^{(q^k-1)/r}$, but all results also hold if $e(P, Q)$ is replaced by the Weil pairing $e_r(P, Q)$.

Lemma 7. Let E be an elliptic curve defined over $\mathbb{F}_q$, and let $r \mid \#E(\mathbb{F}_q)$ be a prime such that the order-r subgroup of $E(\mathbb{F}_q)$ has embedding degree k. If $\{P, Q\}$ is a basis for $E[r]$ and $e(P, P) = 1$, then $e(P, Q) \neq 1$.

Proof. If $e(P, Q) = 1$ then $e(P, aP + bQ) = e(P, P)^a e(P, Q)^b = 1$, but this contradicts non-degeneracy. □

We now give some examples of distortion maps.

Example 8. Let $E : y^2 = x^3 - x$ be an elliptic curve defined over $\mathbb{F}_p$ where $p \equiv 3 \pmod 4$. Then $\#E(\mathbb{F}_p) = p + 1$ and E is supersingular. Suppose r is a large prime dividing $p + 1$. Let $i \in \mathbb{F}_{p^2}$ be such that $i^2 = -1$ and define the automorphism $\psi : (x, y) \mapsto (-x, iy)$ on E. One can show that $\psi^2 = -1$ on E and that $\mathrm{End}(E)$ is an order in the division algebra $\mathbb{Q}(\pi, \psi)$ defined by $\pi^2 = -p$, $\psi^2 = -1$ and $\pi\psi = -\psi\pi$ (so π is the Frobenius).

The embedding degree of $E(\mathbb{F}_p)$ is 2, and $E(\mathbb{F}_{p^2}) \cong E(\mathbb{F}_p) \times E(\mathbb{F}_p)$ as a group. Let $P = (x, y) \in E(\mathbb{F}_p)$ be a point of order r. If $r > 2$ then $y \neq 0$. Now $e(P, P) \in \mathbb{F}_p$ and so $e(P, P) = 1$. But $\psi(P) \in E(\mathbb{F}_{p^2}) \setminus E(\mathbb{F}_p)$ has order r and so $\{P, \psi(P)\}$ forms a basis for $E[r]$. By Lemma 7 we have $e(P, \psi(P)) \neq 1$.

Example 9. Consider the elliptic curve $E_b : y^2 = x^3 - x + b$ defined over $\mathbb{F}_3$ where $b = \pm 1$. This curve is supersingular and one can check that for $\gcd(n, 6) = 1$ the group orders are

$$\#E_b(\mathbb{F}_{3^n}) = 3^n + \epsilon 3^{(n+1)/2} + 1$$

where $\epsilon = 1$ if either $b = 1$ and $n \equiv 1, 11 \pmod{12}$, or $b = -1$ and $n \equiv 5, 7 \pmod{12}$, and $\epsilon = -1$ otherwise. It follows that the embedding degree is $k = 6$.

A useful distortion map is defined as follows. Let $i \in \mathbb{F}_{3^2}$ be such that $i^2 = -1$ and $\alpha \in \mathbb{F}_{3^3}$ be such that $\alpha^3 - \alpha - b = 0$. Then the map $\psi : (x, y) \mapsto (\alpha - x, iy)$ is an automorphism of the curve defined over $\mathbb{F}_{3^6}$ which satisfies $\psi^2 = -1$. If $P \in E(\mathbb{F}_{3^n})$ has order greater than 2 then $\psi(P) \in E(\mathbb{F}_{3^{6n}}) \setminus E(\mathbb{F}_{3^n})$ and $e(P, \psi(P)) \neq 1$.

Example 10. Let E be an elliptic curve defined over $\mathbb{F}_q$ such that there is a large prime $r \mid \#E(\mathbb{F}_q)$. Suppose that the embedding degree of the subgroup of order r is k and assume $k < r$. Let $P \in E(\mathbb{F}_{q^k})$ be such that $e(P, P) = 1$. Define the trace map

$$\mathrm{Tr}(P) = \sum_{i=0}^{k-1} \pi^i(P) \tag{20}$$

where π is the q-power Frobenius map. Note that $\mathrm{Tr}(P) \in E(\mathbb{F}_q)$. The trace map is a group homomorphism, so $\mathrm{Tr}(P)$ has order dividing r. If $\{P, \mathrm{Tr}(P)\}$ is a basis for $E[r]$ then $e(P, \mathrm{Tr}(P)) \neq 1$ and so the trace map can be used as a distortion map for P. Indeed, the Frobenius map π itself can be used as a distortion map, but there are usually good implementation reasons to use the full trace.

It is easy to see that $\mathrm{Tr}(P) \in \langle P \rangle$ if $\pi(P) = \lambda P$ for some integer λ. Indeed, one can show that $\{P, \mathrm{Tr}(P)\}$ is a basis for $E[r]$ if and only if P is not a π-eigenvector (see [47] for details). Note that if $r \mid \#E(\mathbb{F}_q)$ then the π-eigenvalues are 1 and q. The 1-eigenspace is just $E(\mathbb{F}_q)[r]$.

The use of the trace map is completely general and can be applied for both ordinary and supersingular curves. The following result of Schoof and Verheul [122] classifies when a distortion map for a point P exists.

Theorem 11. Let E be an elliptic curve over $\mathbb{F}_q$, let r be a prime and suppose that $E[r] \subseteq E(\mathbb{F}_{q^k})$. Let $P \in E(\mathbb{F}_{q^k})$ have order r and be such that $e(P, P) = 1$.

(i) If E is supersingular then there is a distortion map ψ such that $e(P, \psi(P)) \neq 1$.
(ii) If E is ordinary and if P is not a π-eigenvector then there is a distortion map (namely, the trace map) ψ such that $e(P, \psi(P)) \neq 1$.

Galbraith and Rotger [52] give an algorithm to construct a suitable distortion map for any given supersingular elliptic curve. Hence, we can conclude that DDHP is easy for supersingular curves and for all subgroups of ordinary

curves (having low embedding degree) except for the Frobenius eigenspaces. However, DDHP appears to be hard for the two Frobenius eigenspaces on an ordinary elliptic curve. This property has been used by Boneh, Boyen and Shacham [18, §8.1].

One potential way to attack DDHP in the ordinary case would be to try to 'invert' the trace map. Let $P \in E(\mathbb{F}_q)[r]$ where $k > 1$, and so $e(P, P) = 1$. There are many points Q such that $\mathrm{Tr}(Q) = P$. For example, take $Q = k^{-1}P$; but this still satisfies $e(P, Q) = 1$. Another possibility is to choose a random point $R \in E(\mathbb{F}_{q^k})$, set $R' = \mathrm{Tr}(R)$ and set $Q = k^{-1}(P + R') - R$. If $e(P, R) \neq 1$ then $e(P, Q) \neq 1$. The difficulty is to find an inverse $t(P) = Q$ to the trace map on $\langle P \rangle$ such that $e(P, t(P)) \neq 1$ and $t(nP) = n(t(P))$. Finding such a map, or proving the impossibility of such a map, remains an open problem.

6. Future Research

There are many research directions that one can pursue in discrete logarithm cryptography. The question that is the most fundamental from a practical perspective is the existence of faster algorithms for solving the ECDLP. In particular, more work is needed to fully understand the practical implications of the Weil descent methodology and of Gaudry and Diem's index-calculus methods (and possible variants) for the ECDLP. A worthwhile objective is to find an example of a field $\mathbb{F}_q$ that is *bad* for elliptic curve cryptography in the sense that Pollard's rho method for solving the hardest instances of the ECDLP over $\mathbb{F}_q$ is intractable, but there are ECDLP solvers that can solve all instances of the ECDLP over $\mathbb{F}_q$ using existing computer resources.

Genus two curves have received much attention in recent years. Hence it is important that the same questions be investigated for genus two curves.

The fundamental question in pairing-based cryptography is the hardness of the BDHP. The only viable constructions known for bilinear pairings are from elliptic curves (and, more generally, abelian varieties) that have small embedding degree. These curves were judged to be weak for elliptic curve cryptography in the early 1990's after the discovery of the Weil and Tate pairing attacks and thus the cryptographic community did not pay any further attention to the hardness of the ECDLP for these curves. More investigation of the ECDLP (and BDHP) for these curves is needed in order to increase our confidence in the security of pairing-based cryptographic systems.

Acknowledgements

We are grateful to Claus Diem for his extensive comments on an earlier draft of the paper, and the two anonymous referees for their useful remarks.

References

[1] L. Adleman and J. DeMarrais, "A subexponential algorithm for discrete logarithms over all finite fields", *Mathematics of Computation*, 61 (1993), 1-15.

[2] T. Akishita and T. Takagi, "On the optimal parameter choice for elliptic curve cryptosystems using isogeny", *Public Key Cryptography – PKC 2004*, Lecture Notes in Computer Science, 2947 (2004), 346-359.

[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] ANSI X9.63, *Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*, American National Standards Institute, 2001.

[5] S. Arita, "Construction of secure C_{ab} curves using modular curves", *Algorithmic Number Theory: Fourth International Symposium*, Lecture Notes in Computer Science, 1838 (2000), 113-126.

[6] S. Arita, "Weil descent of elliptic curves over finite fields of characteristic three", *Advances in Cryptology – ASIACRYPT 2000*, Lecture Notes in Computer Science, 1976 (2000), 248-259.

[7] R. Avanzi, "Aspects of hyperelliptic curves over large prime fields in software implementations", *Cryptographic Hardware and Embedded Systems – CHES 2004*, Lecture Notes in Computer Science, 3156 (2004), 148-162.

[8] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press, 2005.

[9] R. Balasubramanian and N. Koblitz, "The improbability that an elliptic curve has sub-exponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm", *Journal of Cryptology*, 11 (1998) 141-145.

[10] E. Barreiro, J. Sarlabous and J. Cherdieu, "Efficient reduction on the jacobian variety of Picard curves", *Coding Theory, Cryptography and Related Areas*, Springer-Verlag, 2000, 13-28.

[11] P. Barreto, H. Kim, B. Lynn and M. Scott, "Efficient implementation of pairing-based cryptosystems", *Advances in Cryptology – CRYPTO 2002*, Lecture Notes in Computer Science, 2442 (2002), 354-368.

[12] P. Barreto, B. Lynn and M. Scott, "Constructing elliptic curves with prescribed embedding degrees", *Security in Communication Networks – SCN 2002*, Lecture Notes in Computer Science, 2576 (2003), 257-267.

[13] P. Barreto, B. Lynn and M. Scott, "Efficient implementation of pairing-based cryptosystems", *Journal of Cryptology*, 17 (2004), 321-334.

[14] M. Bauer and S. Hamdy, "On class group computations using the number field sieve", *Advances in Cryptology – ASIACRYPT 2003*, Lecture Notes in Computer Science, 2894 (2003), 311-325.

[15] I. Blake, G. Seroussi and N. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

[16] I. Blake, G. Seroussi and N. Smart, *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005.

[17] 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.

[18] D. Boneh, X. Boyen and H. Shacham, "Short group signatures", *Advances in Cryptology – CRYPTO 2004*, Lecture Notes in Computer Science, 3152 (2004), 41-55.

[19] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", *SIAM Journal on Computing*, 32 (2003), 586-615.

[20] D. Boneh and R. Lipton, "Algorithms for black-box fields and their application to cryptography", *Advances in Cryptology – CRYPTO '96*, Lecture Notes in Computer Science, 1109 (1996), 283-297.
[21] D. Boneh, B. Lynn and H. Shacham, "Short signatures from the Weil pairing", *Journal of Cryptology*, 7 (2004), 297-319.
[22] D. Boneh and A. Silverberg, "Applications of multilinear forms to cryptography", *Contemporary Mathematics*, 324 (2003), 71-90.
[23] F. Brezing and A. Weng, "Elliptic curves suitable for pairing based cryptography", *Designs, Codes and Cryptography*, to appear.
[24] E. Brier and M. Joye, "Fast point multiplication on elliptic curves through isogenies", *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes: 15th International Symposium, AAECC-15*, Lecture Notes in Computer Science, 2643 (2003), 43-50.
[25] D. Cantor, "Computing in the jacobian of a hyperelliptic curve", *Mathematics of Computation*, 48 (1987), 95-101.
[26] D. Coppersmith, "Small solutions to polynomial equations, with low exponent RSA vulnerabilities", *Journal of Cryptology*, 10 (1997), 233-260.
[27] M. Deuring, "Die Typen der Multiplikatorenringe elliptischer Funktionenkörper", *Abh. Math. Sem. Hansischen Univ.*, 14 (1941), 197-272.
[28] C. Diem, "The GHS attack in odd characteristic", *Journal of the Ramanujan Mathematical Society*, 18 (2003), 1-32.
[29] C. Diem, "On the discrete logarithm problem in elliptic curves over non-prime finite fields", presentation at ECC 2004, Bochum, Germany, 2004.
[30] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory* 22 (1976), 644-654.
[31] R. Dupont and A. Enge and F. Morain, "Building curves with arbitrary small MOV degree over finite prime fields", *Journal of Cryptology*, 18 (2005), 79-89.
[32] I. Duursma and H.-S. Lee, "Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$", *Advances in Cryptology – ASIACRYPT 2003*, Lecture Notes in Computer Science, 2894 (2003), 111-123.
[33] S. Edixhoven, "Sur les couplages de Weil et de Tate", Uni. Rennes Seminar 15 Feb. 2002. Available from http://www.math.univ-rennes1.fr/crypto/seminaire0.html
[34] K. Eisenträger, K. Lauter and P. Montgomery, "Improved Weil and Tate pairings for elliptic and hyperelliptic curves", *Algorithmic Number Theory: 6th International Symposium*, Lecture Notes in Computer Science, 3076 (2004), 169-183.
[35] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Transactions on Information Theory*, 31 (1985), 469-472.
[36] A. Enge and P. Gaudry, "A general framework for subexponential discrete logarithm algorithms", *Acta Arithmetica*, 102 (2002), 83-103.
[37] FIPS 186, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186, National Institute of Standards and Technology, 1994.
[38] FIPS 186-2, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, National Institute of Standards and Technology, 2000.
[39] S. Flon and R. Oyono, "Fast arithmetic on jacobians of Picard curves", *Public Key Cryptography – PKC 2004*, Lecture Notes in Computer Science, 2947 (2004), 55-68.
[40] M. Fouquet, P. Gaudry and R. Harley, "An extension of Satoh's algorithm and its implementation", *Journal of the Ramanujan Mathematical Society*, 15 (2000), 281-318.
[41] G. Frey, "Applications of arithmetical geometry to cryptographic constructions", *Proceedings of the Fifth International Conference on Finite Fields and Applications*, Springer-Verlag, 2001, 128-161.

[42] 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.
[43] W. Fulton, *Algebraic Curves*, Benjamin, 1969.
[44] S. Galbraith, "Constructing isogenies between elliptic curves over finite fields", *LMS Journal of Computation and Mathematics*, 2 (1999), 118-138.
[45] S. Galbraith, "Supersingular curves in cryptography", *Advances in Cryptology – ASIACRYPT 2001*, Lecture Notes in Computer Science, 2248 (2001), 495-513.
[46] S. Galbraith, "Weil descent of Jacobians", *Discrete Applied Mathematics*, 128 (2003), 165-180.
[47] S. Galbraith, "Pairings", Chapter IX of [16], 2005.
[48] S. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate pairing", *Algorithmic Number Theory: 5th International Symposium*, Lecture Notes in Computer Science, 2369 (2002), 324-337.
[49] S. Galbraith, F. Hess and N. Smart, "Extending the GHS Weil descent attack", *Advances in Cryptology – EUROCRYPT 2002*, Lecture Notes in Computer Science, 2332 (2002), 29-44.
[50] S. Galbraith, J. McKee and P. Valença, "Ordinary abelian varieties having small embedding degree" *Cryptology ePrint Archive: Report 2004/365*, 2004. Available from http://eprint.iacr.org/2004/365/
[51] S. Galbraith, S. Paulus and N. Smart, "Arithmetic on superelliptic curves", *Mathematics of Computation*, 71 (2002), 393-405.
[52] S. Galbraith and V. Rotger, "Easy decision Diffie-Hellman groups", *LMS Journal of Computation and Mathematics*, 7 (2004), 201-218.
[53] P. Gaudry, "An algorithm for solving the discrete log problem in hyperelliptic curves", *Advances in Cryptology – EUROCRYPT 2000*, Lecture Notes in Computer Science, 1807 (2000), 19-34.
[54] P. Gaudry, "A comparison and a combination of SST and AGM algorithms for counting points of elliptic curve in characteristic 2", *Advances in Cryptology – ASIACRYPT 2002*, Lecture Notes in Computer Science, 2501 (2002), 311-327.
[55] P. Gaudry, "Index calculus for abelian varieties and the elliptic curve discrete logarithm problem", *Cryptology ePrint Archive: Report 2004/073*, 2004. Available from http://eprint.iacr.org/2004/073/
[56] P. Gaudry, F. Hess and N. Smart, "Constructive and destructive facets of Weil descent on elliptic curves", *Journal of Cryptology*, 15 (2002), 19-46.
[57] P. Gaudry and É. Schost, "Construction of secure random curves of genus 2 over prime fields", *Advances in Cryptology – EUROCRYPT 2004*, Lecture Notes in Computer Science, 3027 (2004), 239-256.
[58] P. Gaudry, N. Thériault and E. Thomé, "A double large prime variation for small genus hyperelliptic index calculus", *Cryptology ePrint Archive: Report 2004/153*, 2004. Available from http://eprint.iacr.org/2004/153/
[59] D. Gordon, "Discrete logarithms in $GF(p)$ using the number field sieve", *SIAM Journal on Discrete Mathematics*, 6 (1993), 124-138.
[60] D. Hankerson, A. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer-Verlag, 2003.
[61] F. Hess, "Computing Riemann-Roch spaces in algebraic function fields and related topics", *Journal of Symbolic Computation*, 33 (2002), 425-445.
[62] F. Hess, "Generalising the GHS attack on the elliptic curve discrete logarithm problem", *LMS Journal of Computation and Mathematics*, 7 (2004), 167-192.
[63] F. Hess, "Weil descent attacks", Chapter VIII of [16], 2005.
[64] M. Huang and D. Ierardi, "Efficient algorithms for the Riemann-Roch problem and for addition in the jacobian of a curve", *Journal of Symbolic Computation*, 18 (1994), 519-539.

[65] IEEE Std 1363-2000, *IEEE Standard Specifications for Public-Key Cryptography*, 2000.

[66] ISO/IEC 15946, *Information Technology – Security Techniques – Cryptography Techniques Based on Elliptic Curves*, Part 1: General (2002), Part 2: Digital Signatures (2002), Part 3: Key Establishment (2002), Part 4: Digital Signatures Giving Message Recovery (2004).

[67] T. Izu, J. Kogure, M. Noro and K. Yokoyama, "Efficient implementation of Schoof's algorithm", *Advances in Cryptology – ASIACRYPT '98*, Lecture Notes in Computer Science, 1514 (1998), 66-79.

[68] M. Jacobson, N. Koblitz, J. Silverman, A. Stein and E. Teske, "Analysis of the xedni calculus attack", *Designs, Codes and Cryptography*, 20 (2000), 41-64.

[69] M. Jacobson, A. Menezes and A. Stein, "Solving elliptic curve discrete logarithm problems using Weil descent", *Journal of the Ramanujan Mathematical Society*, 16 (2001), 231-260.

[70] D. Jao, S. D. Miller and R. Venkatesan, "Ramanujan graphs and the random reducibility of discrete log on isogenous elliptic curves", *Cryptology ePrint Archive: Report 2004/312*, 2004. Available from http://eprint.iacr.org/2004/312/

[71] A. Joux, "A one round protocol for tripartite Diffie-Hellman", *Algorithmic Number Theory: Fourth International Symposium*, Lecture Notes in Computer Science, 1838 (2000), 385-393.

[72] A. Joux and R. Lercier, "The function field sieve is quite special", *Algorithmic Number Theory: 5th International Symposium*, Lecture Notes in Computer Science, 2369 (2002), 431-445.

[73] K. Kedlaya, "Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology", *Journal of the Ramanujan Mathematical Society*, 16 (2001), 323-338.

[74] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, 48 (1987), 203-209.

[75] N. Koblitz, "Hyperelliptic cryptosystems', *Journal of Cryptology*, 1 (1989), 139-150.

[76] N. Koblitz, *Algebraic Aspects of Cryptography*, Springer-Verlag, 1998.

[77] T. Lange, "Formulae for arithmetic on genus 2 hyperelliptic curves", *Applicable Algebra in Engineering, Communication and Computing*, 15 (2005), 295-328.

[78] A. Lenstra and M. Manasse, "Factoring with two large primes", *Mathematics of Computation*, 63 (1994), 785-798.

[79] R. Lercier and F. Morain, "Counting the number of points on elliptic curves over finite fields: strategies and performances", *Advances in Cryptology – EUROCRYPT '95*, Lecture Notes in Computer Science, 921 (1995), 79-94.

[80] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1994.

[81] M. Maurer, A. Menezes and E. Teske, "Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree", *LMS Journal of Computation and Mathematics*, 5 (2002), 127-174.

[82] 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.

[83] 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.

[84] A. Menezes and M. Qu, "Analysis of the Weil descent attack of Gaudry, Hess and Smart", *Topics in Cryptology – CT-RSA 2001*, Lecture Notes in Computer Science, 2020 (2001), 308-318.

[85] A. Menezes and E. Teske, "Cryptographic implications of Hess' generalized GHS attack", *Applicable Algebra in Engineering, Communication and Computing*, to appear.

[86] A. Menezes, E. Teske and A. Weng, "Weak fields for ECC", *Topics in Cryptology – CT-RSA 2004*, Lecture Notes in Computer Science, 2964 (2004), 366-386.
[87] A. Menezes, Y. Wu and R. Zuccherato, "An elementary introduction to hyperelliptic curves", appendix in [76], 1998, 155-178.
[88] V. Miller, "Uses of elliptic curves in cryptography", *Advances in Cryptology – CRYPTO '85*, Lecture Notes in Computer Science, 218 (1986), 417-426.
[89] V. Miller, "The Weil pairing, and its efficient calculation", *Journal of Cryptology*, 17 (2004), 235-261.
[90] 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.
[91] D. Mumford, *Tata Lectures on Theta II*, Progress in Mathematics, volume 43, Birkhäuser, 1984.
[92] D. Naccache and J. Stern, "Signing on a postcard", *Financial Cryptography – FC 2000*, Lecture Notes in Computer Science, 1962 (2001), 121-135.
[93] V. Nechaev, "Complexity of a determinate algorithm for the discrete logarithm problem", *Mathematical Notes*, 55 (1994), 165-172.
[94] S. Paulus and H.-G. Rück, "Real and imaginary quadratic representations of hyperelliptic function fields", *Mathematics of Computation*, 68 (1999), 1233-1241.
[95] J. Pelzl, T. Wollinger, J. Guajardo and C. Paar, "Hyperelliptic curve cryptosystems: closing the performance gap to elliptic curves", *Cryptographic Hardware and Embedded Systems – CHES 2003*, Lecture Notes in Computer Science, 2779 (2003), 351-365.
[96] L. Pintsov and S. Vanstone, "Postal revenue collection in the digital age", *Financial Cryptography – FC 2000*, Lecture Notes in Computer Science, 1962 (2001), 105-120.
[97] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance", *IEEE Transactions on Information Theory*, 24 (1978), 106-110.
[98] J. Pollard, "Monte Carlo methods for index computation mod p", *Mathematics of Computation*, 32 (1978), 918-924.
[99] K. Rubin and A. Silverberg, "Supersingular abelian varieties in cryptology", *Advances in Cryptology – CRYPTO 2002*, Lecture Notes in Computer Science, 2442 (2002), 336-353.
[100] H. Rück, "On the discrete logarithm in the divisor class group of curves", *Mathematics of Computation*, 68 (1999), 805-806.
[101] R. Sakai, K. Ohgishi and M. Kasahara, "Cryptosystems based on pairings", *Proceedings of the 2000 Symposium on Cryptography and Information Security*, Okinawa, Japan, 2000.
[102] T. Satoh, "The canonical lift of an ordinary elliptic curve over a prime field and its point counting", *Journal of the Ramanujan Mathematical Society*, 15 (2000), 247-270.
[103] T. Satoh and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves", *Commentarii Mathematici Universitatis Sancti Pauli*, 47 (1998), 81-92.
[104] C. Schnorr, "Efficient signature generation for smart cards", *Journal of Cryptology*, 4 (1991), 161-174.
[105] R. Schoof, "Elliptic curves over finite fields and the computation of square roots mod p", *Mathematics of Computation*, 44 (1985), 483-494.
[106] R. Schoof, "Nonsingular plane cubic curves over finite fields", *Journal of Combinatorial Theory*, A 46 (1987), 183-211.
[107] M. Scott and P. Barreto, "Generating more MNT elliptic curves", *Designs, Codes and Cryptography*, to appear.

[108] I. Semaev, "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p", *Mathematics of Computation*, 67 (1998), 353-356.
[109] I. Semaev, "Summation polynomial and the discrete logarithm problem on elliptic curves", *Cryptology ePrint Archive: Report 2004/031*, 2004. Available from http://eprint.iacr.org/2004/031/
[110] A. Shamir, "Identity-based cryptosystems and signature schemes", *Advances in Cryptology – Proceedings of CRYPTO 84*, Lecture Notes in Computer Science, 196 (1985), 47-53.
[111] V. Shoup, "Lower bounds for discrete logarithms and related problems", *Advances in Cryptology – EUROCRYPT '97*, Lecture Notes in Computer Science, 1233 (1997), 256-266.
[112] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.
[113] J. Silverman, "The xedni calculus and the elliptic curve discrete logarithm problem", *Designs, Codes and Cryptography*, 20 (2000), 5-40.
[114] J. Silverman and J. Suzuki, "Elliptic curve discrete logarithms and the index calculus", *Advances in Cryptology – ASIACRYPT '98*, Lecture Notes in Computer Science, 1514 (1998), 110-125.
[115] N. Smart, "The discrete logarithm problem on elliptic curves of trace one", *Journal of Cryptology*, 12 (1999), 193-196.
[116] N. Smart, "An analysis of Goubin's refined power analysis attack", *Cryptographic Hardware and Embedded Systems – CHES 2003*, Lecture Notes in Computer Science, 2779 (2003), 281-290.
[117] A. Stein, "Sharp upper bounds for arithmetics in hyperelliptic function fields", *Journal of the Ramanujan Mathematical Society*, 16 (2001), 1-86.
[118] M. Stevens and T. Lange, "Efficient doubling on genus two curves over binary fields", *Selected Areas in Cryptography – SAC 2004*, Lecture Notes in Computer Science, 3357 (2005), 170-181.
[119] N. Thériault, "Index calculus attack for hyperelliptic curves of small genus", *Advances in Cryptology – ASIACRYPT 2003*, Lecture Notes in Computer Science, 2894 (2003), 75-92.
[120] N. Thériault, "Weil descent attack for Kummer extensions", *Journal of the Ramanujan Mathematical Society*, 18 (2003), 281-312.
[121] F. Vercauteren, "Computing zeta functions of hyperelliptic curves over finite fields of characteristic 2", *Advances in Cryptology – CRYPTO 2002*, Lecture Notes in Computer Science, 2442 (2002), 369-384.
[122] E. Verheul, "Evidence that XTR is more secure than supersingular elliptic curve cryptosystems", *Journal of Cryptology*, 17 (2004) 277-296.
[123] E. Volcheck, "Computing in the jacobian of a plane algebraic curve", *Algorithmic Number Theory*, Lecture Notes in Computer Science, (1994), 221-233.
[124] L. Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, 2003.
[125] A. Weng, "Constructing hyperelliptic curves of genus 2 suitable for cryptography", *Mathematics of Computation*, 72 (2003), 435-458.

Mathematics Department, Royal Holloway University of London, Egham, Surrey TW20 0Ex, UK
E-mail address: Steven.Galbraith@rhul.ac.uk

Dept. of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
E-mail address: ajmeneze@uwaterloo.ca