Rational Groups of Elliptic Curves Suitable for Cryptography

David R. Kohel

Abstract. We give an overview of methods of construction of elliptic curves which contain a subgroup of large prime order. Variations on the standard random curve selection and complex multiplication methods are presented for constructing elliptic curves containing a subgroup of large prime order. The results of random curve selection and the CM method are qualitatively contrasted in terms of the randomness of the resulting curves; in particular we note that the CM method fails any reasonable measure of randomness if applied over a base field of predetermined characteristic. We analyze both practical and theoretical considerations in the choice of the group of points used for cryptographic applications.

1. Introduction

An elliptic curve E over a finite field k is a nonsingular projective plane curve defined by a Weierstrass equation

$$Y^2Z + (a_1X + a_3Z)YZ = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

with all a_i in k. There is a unique point $O = (0 : 1 : 0)$ on the line $Z = 0$, which is specified as a distinguished point of the elliptic curve. It is thus standard to set $x = X/Z$ and $y = Y/Z$ and defined E to be defined by the affine model

$$y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6,$$

of the curve, together with the distinguished point O at infinity.

The elliptic curve E over of field k can be identified with the set of points

$$E(\overline{k}) = \{O\} \cup \{(\alpha, \beta) \,|\, \alpha, \beta \in \overline{k},\ \beta^2 + (a_1\alpha + a_3)\beta = \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6\},$$

where $\overline{k}$ is an algebraic closure of k. Conversely the equation of the curve E is the unique equation interpolating the points in the set $E(\overline{k})$.

The set $E(\overline{k})$ has the structure of an abelian group with identity O, under the rule which says that three collinear points sum to O. More generally for any field extension K/k we have a finite subgroup $E(K)$ of K-rational points, and for any k-algebra homomorphism $K \to L$ we have a homomorphism of groups $E(K) \to E(L)$. We thus, in particular, distinguish the groups $E(K)$, from the

geometric object E/k, which is a map associating a group to each field extension K/k and defining compatible systems of maps between them.

The theory of elliptic curves and its connections to modular forms and class field theory has a long and active history. This theory is treated, from a modern viewpoint, in books of Silverman [26, 27], Hüsemoller [9], and Knapp [10]. Groups of points on elliptic curves were suggested for use in cryptography independently by Koblitz [11] and Miller [21]. The acceptance of elliptic curve cryptography is attested in the new generation of books emphasizing elliptic curves over finite fields from a cryptographic point of view, including the books of Menezes [19]; Blake, Serousii and Smart [1]; and Enge [5].

A general group $E(K)$ has the advantage over the corresponding multiplicative group K^* of the field, because the discrete logarithm problem appears to be harder in general for the former. Moreover, for any given field K there exists a large choice of curves. The multiplicative group K^* can, in fact, be interpreted as the group of points on a degenerate elliptic curve, or singular cubic curve (see Chapter 3, §7, Hüsemoler [9]). It is therefore not unreasonable to expect that a generic discrete logarithm algorithm for elliptic curves would apply as well to the multiplicative group of a field.

In this paper we describe methods for constructing point groups of elliptic curves of use for cryptography, and present some variants on the standard random curve and complex multiplication (CM) constructions. Because the structure of the groups $E(K)$ is governed by the structure of the endomorphism ring of E, we begin with background on endomorphisms of elliptic curves. In the following sections we describe variants of the random curve and CM methods for construction of curves with known numbers of points. Examples are chosen for pedagogic purposes. In particular the bit size of the point groups (> 350) are in excess of the current recommendations of 160–250 bits for commercial applications (see Lenstra and Verheul [16]), but demonstrate the effectiveness of a construction where point counting becomes nontrivial. On the other hand, this bit size is not unreasonably large for military applications in which a 50 year life span of confidentiality is insufficient or in cases where an additional security margin is sought. We take the conservative position that to ensure a sufficiently general construction, the elliptic curve should be chosen at random from a pool large enough to be effectively innumerable. This contrasts in particular with suggestions for use of curves over small fields, curves generated by the complex multiplication method over any field of prespecified characteristic, or, in the extreme, of one of the two ordinary elliptic curves over $\mathbb{F}_2$. In this view, the given example of the CM method over a field of characteristic 2 is taken purely for the sake of comparison of the CM and random curve methods, since the use of the CM method over a field of fixed characteristic violates this principle. In the final section we discuss this randomness criterion, make qualitative contrasts of "random" and "CM" curves, and discuss the implications of cryptographic use of point groups over proper extensions of the base field, in particular in light of the work of Gaudry, Hess and Smart [7].

2. Endomorphism Structure of Elliptic Curves

The structure of the abelian groups $E(K)$ is intimately related to the endomorphism ring structure of E and, in particular, to the distinguished Frobenius element. We therefore we recall some background material on endomorphisms of elliptic curves as a means of constructing and analyzing rational point groups appropriate for cryptographic use.

An endomorphism $\phi : E \to E$ is a rational polynomial map

$$(x, y) \mapsto (f(x), g(x, y)),$$

where $g(x, y) = g_1(x)y + g_0(x)$ with $f(x)$, $g_1(x)$, and $g_0(x)$ in $k(x)$, such that

$$g(x, y)^2 + (a_1 f(x) + a_3)g(x, y) = f(x)^3 + a_2 f(x)^2 + a_4 f(x) + a_6,$$

and which takes O to O. As a consequence of the definition, an endomorphism ϕ induces a homomorphism $E(K) \to E(K)$ for any field extension K/k. Thus the addition law on the curve gives a well-defined addition of endomorphisms, and composition defines a compatible associative multiplication operation. This gives a ring structure to the set $\mathrm{End}_k(E)$ of endomorphisms, in which the multiplication-by-n maps $[n]$ define a subring isomorphic to $\mathbb{Z}$.

For an elliptic curve E/k, where $|k| = q$, we define the distinguished *Frobenius endomorphism* $\phi : E \to E$ by

$$(x, y) \mapsto (x^q, y^q).$$

Clearly $\phi(P) = P$ if and only if the point P is in $E(k)$. By a standard result of Hasse (see Silverman [26]), the Frobenius endomorphism satisfies a characteristic equation $X^2 - tX + q = 0$, where t is an integer satisfying $|t| \leq 2\sqrt{q}$.

If the trace of Frobenius t is congruent to 0 mod p, we say that the curve is *supersingular*, otherwise we call it *ordinary*. Menezes, Okamoto and Vanstone [20] have proved that the discrete logarithm on supersingular elliptic curves can be reduced to a discrete logarithm in the multiplicative group of a finite extension field of degree generally 2, and at most 6, over the base field. This reduction to finite fields holds in general. However, in the ordinary case, Koblitz [12] has proved that the degree of the extension is generically large. We thus consider only the ordinary case for the purpose of cryptography. The following theorem, however, on the structure of endomorphisms, holds in general.

Theorem 1. *Let ψ be an endomorphism of E not contained in $\mathbb{Z}$. Then ψ has an irreducible characteristic polynomial $X^2 + aX + b$ and generates a ring isomorphic to the imaginary quadratic order $\mathcal{O} = \mathbb{Z}[X]/(X^2 + aX + b)$. The map*

$$\rho = [n] + [m]\psi \longmapsto \widehat{\rho} = [n - am] - [m]\psi$$

defines an automorphism of $\mathbb{Z}[\psi]$ and $\mathrm{Tr}(\rho) = \rho + \widehat{\rho}$ and $\mathrm{N}(\rho) = \rho\widehat{\rho}$ agree with the trace and norm from $\mathcal{O}$ to $\mathbb{Z}$. In particular we have $\mathrm{Tr}(\psi) = -[a]$ and $\mathrm{N}(\psi) = [b]$.

Proof. This follows from the standard properties of the dual isogeny, for which we refer to Chapter III §6 of Silverman [26], noting that $\widehat{\rho}$ is the dual of ρ and $\mathrm{N}(\rho)$ is its degree. □

For an ordinary elliptic curve E, the endomorphism ring $\mathrm{End}_k(E)$ is a commutative ring of rank 2 over $\mathbb{Z}$, and the full endomorphism ring is generated by an element ψ satisfying $\phi = [n] + [m]\psi$ for integers n and m. If K is a field extension of degree r over k, then ϕ^r acts as the identity on the points in $E(K)$, so that $\phi^r - 1$ is in the kernel of the action of $\mathrm{End}_k(E)$ on $E(K)$. In fact the following stronger result holds.

Theorem 2. *There exists a noncanonical isomorphism of* $\mathrm{End}_k(E)$*-modules*

$$E(K) \cong \mathrm{End}_k(E)/(\phi^r - 1).$$

In particular, the number $|E(K)|$ *of* K*-rational points is given by* $\mathrm{N}(\phi^r - 1)$.

Proof. The isomorphism appears in Theorem 1 of Lenstra [15]. An analysis of this isomorphism shows that

$$\mathrm{End}_k(E)/(\phi^r - 1) \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/(\mathrm{N}(\phi^r - 1)/m_1)\mathbb{Z},$$

where m_1 is the largest divisor of $[\mathrm{End}_k(E) : \mathbb{Z}[\phi]]$ such that $\phi^r \equiv 1 \bmod m_1$. □

This isomorphism will be the main tool used for the construction and analysis of groups of rational points on elliptic curves. The group order $N(\phi^r - 1)$ can be rapidly computed from Theorem 1. Let t be the trace of of Frobenius, and write

$$X^r - 1 \equiv uX + v \bmod (X^2 - tX + q).$$

Then we find the explicit form

$$N(\phi^r - 1) = u^2 q + t\,uv + v^2,$$

for the number of points in $E(K)$. We note that $m = [\mathrm{End}_k(E) : \mathbb{Z}[\phi]]$ is a well-defined invariant of the curve E/k, and together with the trace t, suffices to determine the group structure of $E(K)$ for all extensions K/k. For further information in this direction we refer to the thesis of the author [13].

An elliptic curve over a finite field can be considered as the reduction of an elliptic curve over a number ring. As such it is an element of a two parameter family. The first parameter is the j-invariant of the curve, and the second is the prime of reduction. There are two approaches to the problem of choosing suitable elliptic curves for cryptographic use, which correspond to fixing one of the parameters and choosing the second at random. In the *complex multiplication* (CM) method we choose a suitable j-invariant of a curve, and the prime of reduction is determined subsequently. The *random curve* method first fixes the base field, essentially fixing a prime of reduction, then selects random curves to find one with good properties. We explore aspects of these two methods in the sections which follow.

3. Random Curve Selection

We let k be fixed, and choose E/k at random. The order of $E(k)$ can be computed in polynomial time using the SEA method of Schoof [24], with improvements of Elkies [4] and Atkin. We continue until we find a curve whose order is divisible by a large prime.

When the construction time is critical or a sophisticated point counting algorithm unavailable, we can consider the following variant of the random curve method. Let K be a fixed finite field, and let k be a proper subfield. We choose E/k at random, compute the group order $E(k)$ over the smaller field. Then by Theorem 2, the order of $E(K)$ is given by $\mathrm{N}(\phi^r - 1)$, where ϕ is the Frobenius endomorphism relative to k. Since $\mathrm{N}(\phi - 1)$ is a divisor of relatively small order, the objective is to find a large prime factor in

$$|E(K)/E(k)| = \mathrm{N}(\phi^r - 1)/\mathrm{N}(\phi - 1).$$

Example 3. Choosing random elliptic curves over $k = \mathbb{F}_{2^{31}}$, we obtain a particular example:

$$y^2 + xy = x^3 + \gamma,$$

having $\mathrm{Tr}(\phi) = 77689$, where $\gamma = w^{217980880}$ and $w^{31} + w^3 + 1 = 0$. Over an extension $K = \mathbb{F}_{2^{403}}$ of degree 13, we find the order of the group $E(K)/E(k)$ to be:

$$\mathrm{N}(\phi^{13} - 1)/\mathrm{N}(\phi - 1) = 79 \cdot p_{366}$$

containing a 366-bit prime factor p_{366}.

We note that the endomorphism ring has discriminant $D = -2554353871$ and class number 42966. The size of the class number makes this curve impractical to construct by the complex multiplication method which follows. We return to the implications of this in the final section.

4. CM Constructions

For any negative integer D congruent to 0 or 1 mod 4, there exists, up to isomorphism, a unique imaginary quadratic order $\mathcal{O} = \mathbb{Z}[(D + \sqrt{D})/2]$. In the complex multiplication method we choose a discriminant D of an imaginary quadratic order and find a finite field of q elements such that $m^2 D = t^2 - 4q$ for integers t and m and such that $q - t + 1$ contains a large prime factor. We denote by (D/p) the Legendre symbol for the prime p. The existence and construction of an elliptic curve with this discriminant is given by the following theorem.

Theorem 4. *For $\mathcal{O}$ to be the endomorphism ring of an ordinary elliptic curve E over k of characteristic p, it is necessary and sufficient that*

1. *$D = \mathrm{disc}(\mathcal{O})$ satisfies $(D/p) = 1$; and*
2. *The order in the class group of a prime over p divides $[k : \mathbb{F}_p]$.*

Proof. The results follow from the classical class field theory for complex multiplication, going back to Deuring [3]. The first condition ensures that the elliptic curve is ordinary, and follows from Chapter 10 or Theorem 12 of Chapter 13 in Lang [14]. The second condition defines the minimal field of definition of E, and is a consequence of Theorem7 of Chapter 12 of the same volume. □

4.1. Class Polynomial Construction

In order to construct an elliptic curve with complex multiplication we use some classical constructions of class field theory. The following theorem is the effective variant of Theorem 4 used to produce the j-invariant of a particular elliptic curve.

Theorem 5. *Let $\mathcal{O}$ be an imaginary quadratic order of discriminant D and class number $h(\mathcal{O})$. There exists a unique monic irreducible polynomial $H_D(X)$ of degree $h(\mathcal{O})$ such that E is an ordinary elliptic curve over a field k of characteristic p with endomorphism ring $\mathcal{O}$ if and only if $(D/p) = 1$ and the j-invariant of E is a root of $H_D(X) \bmod p$ in k.*

The theorem is effective, since the roots of the class polynomial $H_D(X)$ can be computed over $\mathbb{C}$ as special values of the modular function $j(\tau)$ on points τ representing the R-ideal classes (see Section 7.6.2 of Cohen [2]). By computing the roots to sufficient precision, the polynomial $H_D(X)$ is determined as an element of $\mathbb{Z}[X]$. For the discriminant -47, we find that $H_{-47}(X)$ equals

$$X^5 + 2257834125X^4 - 9987963828125X^3 + 5115161850595703125X^2 \\ - 14982472850828613281250X + 160429296006238708496093750$$

On the other hand the size of the coefficients rapidly becomes an obstacle, as suggested by this small example. For D in restricted congruence classes we obtain alternative class polynomials over $\mathbb{Z}$ with smaller coefficients. For instance Yui and Zagier [31] prove the existence of a class polynomial $W_D(X)$ defined for $D \equiv 1 \bmod 8$ and $D \neq 0 \bmod 3$ using Weber functions. The class polynomial $W_{-47}(X)$ takes the more compact form:

$$X^5 - 2X^4 + 3X^3 - 3X^2 + X + 1.$$

A root α of this equation corresponds to the j-invariant $j = (\alpha^{24} - 16)^3/\alpha^{24}$, from which we can construct a curve with the desired endomorphism ring j-invariant j is by Theorem 6 which follows.

Since one is interested only in the roots of the class polynomials modulo a prime, the size of the coefficients of $W_D(X)$, computed using special values of analytic functions in $\mathbb{C}$, is only relevant to prevent coefficient explosion over $\mathbb{Z}$. Similar class polynomials, of reduced coefficient size, can be defined for discriminants in other congruence classes (see Gee [8]).

4.2. Isomorphism Classes of Elliptic Curves

In order to pass from a class polynomial to an elliptic curve with known number of points, we require a construction for curves with given j-invariant. An elliptic curve, however, may have several nonisomorphic *twists* with the same j-invariant.

The following theorem classifies all elliptic curves over a finite field k with given j-invariant.

Theorem 6. *Let j be an element of a finite field k, and denote by ${k^*}^n$ the subgroup of n-th residues in k^*.*

If k has characteristic 2, then all isomorphism classes of curves E with j-invariant j are given by the following equations:

(1) $y^2 + a_3 y = x^3 + a_4 x + a_6$, *if* $j = 0$,
(2) $y^2 + xy = x^3 + a_2 x^2 - 1/j$, *if* $j \neq 0$.

In the first, supersingular, case, the coefficient a_3 is a unit whose class in ${k^*}/{k^*}^3$ is determined by the isomorphism class of the curve. Two curves with coefficients a_3, a_4, a_6 and a'_3, a'_4, a'_6 are isomorphic exactly when $a'_3 = u^3 a_3$; when a'_4 and $u^4 a_4$ are in the same additive class mod $\ker(\mathrm{Tr}^k_\ell)$, where $\ell = k \cap \mathbb{F}_4$; and when a'_6 and $u^6 a_6$ are in the same additive class mod $\ker(\mathrm{Tr}^k_{\mathbb{F}_2})$. In the second, ordinary, case, the isomorphism class is uniquely determined by the class of a_2 mod $\ker(\mathrm{Tr}^k_{\mathbb{F}_2})$.

If k has characteristic 3, then all isomorphism classes of curves with j-invariant j are given by the following equations:

(1) $y^2 = x^3 + a_4 x + a_6$, *if* $j = 0$,
(2) $y^2 = x^3 + a_2 x^2 - a_2^3/j$, *if* $j \neq 0$.

In the first, supersingular, case, the coefficient a_4 is a unit whose class in ${k^*}/{k^*}^4$ is determined by the isomorphism class of the curve. Two curves with coefficients a_4, a_6 and a'_4 a'_6 are isomorphic exactly when $a_4 = u^4 a'_4$ and the equation $r^3 + a_4 r + a_6 = u^6 a'_6$ has a solution r in k. In the second, ordinary, case, the isomorphism class is uniquely determined by the class of a_2 in ${k^*}/{k^*}^2$.

If k has characteristic ≥ 5, then all isomorphism classes of curves with j-invariant j are given by the following equations with t in k^*:

(1) $y^2 = x^3 + a_6$, *if* $j = 0$,
(2) $y^2 = x^3 + a_4 x$, *if* $j = 12^3$,
(3) $y^2 = x^3 - a_2^2 jx/48(j - 1728) + a_2^3 j/864(j - 1728)$ *otherwise.*

The isomorphism class is uniquely determined by the class of a_n in ${k^*}/{k^*}^n$.

Proof. This follows by explicit verification, starting from the form of an isomorphism given in Appendix A of Silverman [26]. For the conditions in characteristic 2, we observe that $a \equiv b \bmod \ker(\mathrm{Tr}^k_{\mathbb{F}_2})$ is equivalent to $\mathrm{Tr}^k_{\mathbb{F}_2}(a) = \mathrm{Tr}^k_{\mathbb{F}_2}(b)$ and also to the existence of a solution r to the equation $r^2 + r = a + b$ over k. □

We note that Morain [22] finds a more refined expression for the supersingular elliptic curves in characteristic 3, which also classifies the corresponding trace. This builds on Schoof [25], who does a complete enumeration of the abstract isomorphism classes of elliptic curves in terms of endomorphism rings structure. A more refined analysis of the supersingular case in characteristic 2 would provide a similar classification of the trace in terms of explicit equations.

4.3. CM Example

By Theorem 4 and Theorem 5 the degree of the field extension $k/\mathbb{F}_p$ must divide the degree of the class polynomial $H_D(X)$ or of an alternate class polynomial. For large degree extensions over $\mathbb{F}_p$ of small characteristic, the computation of the class polynomial becomes computationally expensive. To compensate, we indicate how to employ an intermediate degree extension to useful effect.

By sieving over small discriminants, we choose a discriminant $D = -8647$ with class number 31, the class group being generated by a prime $\mathfrak{p}_2$ over 2. Therefore there exists a curve E over $k = \mathbb{F}_{2^{31}}$ with endomorphism ring of this discriminant. Prior to doing any computations with curves, we find that the ring $\mathbb{Z}[\phi]$ generated by Frobenius is isomorphic to $\mathbb{Z}[X]/(X^2 - tX + 2^{31})$, where $t = \pm 35875$.

Over a degree 13 extension $K = \mathbb{F}_{2^{403}}/k$ we find that the group order of $E(K)/E(k)$ is either equal to a large composite number with small prime factors if $t = -35875$, or equals

$$\mathrm{N}(\phi^{13} - 1)/\mathrm{N}(\phi - 1) = 157 \cdot 7333 \cdot p_{352},$$

for a 352-bit prime p_{352} when $t = 35875$.

In order to construct an elliptic curve with this trace, we compute the Weber class polynomial $W_{-8647}(X)$, which takes the form:

$$\begin{aligned} X^{31} &- 33X^{30} + 135X^{29} + 1585X^{28} + 16905X^{27} + 77577X^{26} \\ &+ 261396X^{25} + 677142X^{24} + 1406953X^{23} + 2509293X^{22} \\ &+ 4044270X^{21} + 6101029X^{20} + 8852701X^{19} + 12285213X^{18} \\ &+ 15808518X^{17} + 18153439X^{16} + 17693230X^{15} + 13330467X^{14} \\ &+ 5493408X^{13} - 3612428X^{12} - 10816811X^{11} - 13646625X^{10} \\ &- 11600862X^9 - 6330185X^8 - 678696X^7 + 3083034X^6 \\ &+ 4212540X^5 + 3382143X^4 + 1882711X^3 + 683247X^2 \\ &+ 136725X + 1 \end{aligned}$$

Then $W_{-8647}(X) \bmod 2$ has a root $\alpha = w^{1023401681}$ over $\mathbb{F}_2[w] = \mathbb{F}_{2^{31}}$, where w has minimal polynomial $X^{31} + X^3 + 1$. From the associated j-invariant, we first construct the curve $y^2 + xy = x^3 + \gamma$ by Theorem 6, where $\gamma = w^{1878640454}$ and find that the trace of the Frobenius endomorphism is -35875. Passing to the quadratic twist we find the curve

$$y^2 + xy = x^3 + x^2 + \gamma,$$

with the desired trace 35875.

4.4. Sieving for Discriminants

For a fixed field k of cardinality $q = p^s$ one can sieve for discriminants D up to a particular bound which satisfy the conditions of Theorem 4. The condition $(D/p) = 1$ implies that there exists a prime $\mathfrak{p}$ over p, and one can quickly test if

$\mathfrak{p}^s$ is a principal ideal. The following corollary of Theorem 4 gives a more direct approach to finding a suitable D.

Corollary 7. *Let k be a field of q elements and let m be an integer coprime to q. For any integer t such that $t^2 \equiv 4q \bmod m^2$ with $|t| \leq 2\sqrt{q}$, the integer $D = (t^2 - 4q)/m^2$ is the discriminant of the endomorphism ring of an ordinary elliptic curve over k.*

While this approach is constructive, using factorization modulo the prime divisors of m and Hensel lifting, the problem remains that the computation of class polynomials appears to have exponential complexity, which effectively implies an absolute bound on the discriminant. Thus, in practice, it is necessary to choose m sufficiently large such that $|D|$ is of a prescribed size.

5. Cryptographic Considerations

5.1. Enumerability of Curves

In the examples, we have specified the exact field $\mathbb{F}_{2^{31}}$ over which we are to choose an elliptic curve. The size of the field is sufficiently large that it is meaningful to speak of a randomly selected curve as being generic. However, if the CM method is used, then the number of curves available for use becomes severely constrained. The discriminants with $|D| < 10^4$, $D \equiv 1 \bmod 8$, and in which a prime over 2 has order 31 in the class group are limited to the 11 values

$$-719, -911, -2471, -2927, -3727, -4159, -4247, -4951, -6439, -7639, -8647.$$

With $|D| < 10^5$, $|D| < 10^6$, and $|D| < 10^7$ these numbers are 50, 191, and 623, respectively. The expected size of the class number of D and the size of the coefficients of a class polynomial place an effective absolute upper bound on the size of $|D|$. Thus for fixed field k there are a very constrained set of discriminants of small absolute value which can be the endomorphism ring of a curve over k. Thus, as the above example shows, the CM method, when used over fixed base ring or characteristic, is tantamount to prescribing a fixed enumerable set of curves of use for cryptography. In order to regain a reasonable concept of randomness, the CM method should only be applied in a context where the characteristic of the finite field is not prespecified.

5.2. Qualitative Distinction of CM and Random Curves

The methods presented here for computing class polynomials severely limit the size of a CM discriminant. As indicated above this means that the number of constructible curves over any particular field will be be contained in an enumerable set of curves. These curves will have the property that the discriminant of the endomorphism ring is exceptionally small compared to the general case. Indeed the method by which a curve was produced can be effectively determined by the size of the discriminant. While defined over the same field, the random curve method gave rise to a curve with $D = -2554353871$ and class number 42966,

while in the CM method we constructed a curve of discriminant $D = -8647$ with class number 31. While no specific attacks profit exceptionally from the special form of elliptic curves constructed by the CM method, the potential remains.

5.3. Working over Field Extensions

In both examples given above we chose to define a curve over a field k and work in the group of rational points over a proper extension K. By working over an extension field of degree r, one loses r bits due to the small subgroup $E(k)$ of order $\mathrm{N}(\phi - 1)$. The benefit is a more time efficient construction of the elliptic curve.

One advantage of these sort of composite degree extensions is the use of the Frobenius endomorphism with respect to k on the group $E(K)$. The Frobenius endomorphism can be rapidly computed without divisions in the field K. The following corollary of Theorem 2 describes the action of Frobenius on the cyclic subgroups of interest in cryptography.

Corollary 8. *Let E be an elliptic curve over k and let K be an extension of degree r over k. Suppose that n is a prime divisor of $|E(K)|$ and is coprime to $|E(K)|/n$. Then $E(K)$ contains a subgroup H of order n and*

$$\mathrm{End}_k(E)/(\phi^r - 1, n) \cong H \cong \mathbb{Z}/n\mathbb{Z},$$

where $(\phi^r - 1, n)$ is the ideal generated by $\phi^r - 1$ and n. In particular ϕ acts as $[a]$ on H for some r-th root of unity modulo n.

This permits scalar multiplication to be computed in base ϕ or base 2. Indeed, the work of Müller [23] in characteristic 2 and Smart [28] in odd characteristic, based on [18] and [29], exploit base ϕ representations for efficiency of scalar multiplication. The work of Wiener and Zuccherato [30] and Gallant, Lambert, and Vanstone [6], shows that an attacker also benefits by a factor of $r^{1/2}$, where $r = [K : k]$, in the discrete logarithm on such a curve. Since the algorithm remains exponential, this work is relevant when applied to a cryptosystem of critical security margin.

The recent work of Gaudry, Hess, and Smart [7] shows how the process of Weil decent in characteristic 2 can reduce a discrete logarithm on an elliptic curve over and extension k of $\mathbb{F}_2$ to a discrete logarithm in the Jacobian J of a hyperelliptic curve $\mathcal{C}$ over a proper subfield ℓ. This method maps the discrete logarithm in $E(k)$ to that in $J(\ell)$, with an explicit criterion for testing whether the map is injective. This, however, does not apply to the discrete logarithm problem in the point group $E(K)$ when K is a proper extension K/k. Thus an interesting open question is whether a discrete logarithm in $E(K)$ can be mapped injectively into a discrete logarithm problem in $J(L)$ for a proper subfield L of K. The method of Gaudry et al. was found to be effective when the extension degree was < 5. In the event of an affirmative answer to this question, the choice of base field $\mathbb{F}_{2^{31}}$ of the examples taken for this exposition should be of sufficiently large prime degree over $\mathbb{F}_2$ that the size of the genus of the curve $\mathcal{C}$ found by Weil descent would make this

reduction an impractical means of attack. Moreover, the same construction, when applied in odd characteristic, even $p = 3$, fails to give a reduction to a discrete logarithm on a curve of particularly simple form.

We note that the use of a proper subgroup of $E(K)$, as presented in the examples, is potentially susceptible to the protocol attack of Lim and Lee [17]. The proper design of an encryption protocol, while not treated here, is of equal importance to the proper construction and choice of the group. In this instance, to prevent the leakage of bits, the design of a cryptoscheme on such a group must incorporate a verification of the order of an input message, or include a premultiplication by the cofactor, to eliminate the telltale "witness" to the secret key.

Acknowledgements. The author is grateful to the referees for helpful comments.

References

[1] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*, London Mathematical Society, Lecture Notes Series, **265**, Cambridge University Press, 1999.

[2] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, **138**, Springer-Verlag, Berlin, 1993.

[3] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hamburg, **14**, (1941), 197–272.

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

[5] A. Enge, *Elliptic Curves and their Application to Cryptography: An Introduction*, Kluwer Academic Publishers, Boston, 1999.

[6] R. Gallant, R. Lambert, and S. Vanstone, *Improving the parallelized Pollard lambda search on binary anomalous curves*, Math. Comp., to appear.

[7] P. Gaudry, F. Hess, and N. P. Smart, *Constructive and destructive facets of Weil descent on elliptic curves*, HP Labs Technical Report, 2000.

[8] A. Gee, *Class invariants by Shimura's reciprocity law*, Les XXèmes Journées Arithmétiques (Limoges 1997), J. Théor. Nombres Bordeaux **11** (1999), no. 1, 45–72

[9] D. Husemöller, *Elliptic Curves*, Springer-Verlag, New York, 1987.

[10] A. Knapp, *Elliptic curves*, Mathematical Notes, **40**, Princeton University Press, Princeton, NJ, 1992.

[11] N. Koblitz, *Elliptic curve cryptosystems*, Math. Comp., **48** (1987), 203–209.

[12] N. Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, J. Cryptography, **11** (1998), no. 2, 141–145.

[13] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, Thesis, U.C. Berkeley, 1996.

[14] S. Lang, *Elliptic functions*, Springer–Verlag, New York, 1987.

[15] H. W. Lenstra, Jr., *Complex multiplication structure of elliptic curves*, Journal of Number Theory, **56** (1996), no. 2, 227–241.

[16] A. K. Lenstra and E. R. Verheul, *Selecting Cryptographic Key Sizes*, In H. Imai and Y. Zheng, eds., *Proceedings of the Third International Workshop on Practice and Theory in Public Key Cryptosystems, PCK 2000*, Lecture Notes in Computer Science, **1751**, 2000, 446-465.

[17] C. H. Lim and P. J. Lee, *A key recovery attack on discrete log-based schemes using a prime order subgroup*, In B. S. Kaliski, Jr., ed., *Advances in cryptology—CRYPTO '97 (Santa Barbara, CA, 1997)*, Lecture Notes in Computer Science, **1294**, Springer, Berlin, 1997, 249–263.

[18] W. Meier and O. Shaffelbach, *Efficient multiplication on certain nonsupersingular elliptic curves*, in *Advances in Cryptology—CRYPTO '92 (Santa Barbara, CA, 1992)*, 333–344, Lecture Notes in Comp. Sci., **740**, Springer, Berlin, 1993.

[19] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, Boston, MA, 1993.

[20] A. J. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Trans. Inf. Theory, **39** (1993), no. 5, 1639–1646.

[21] V. Miller, *Uses of elliptic curves in cryptography*, Advances in Cryptology – CRYPTO'85, Springer, 1986, 417-426.

[22] F. Morain, *Classes d'isomorphismes des courbes elliptiques supersingulières en caractéristique* ≥ 3, Util. Math., **52** (1997), 241–253.

[23] V. Müller, *Fast multiplication on elliptic curves over small fields of characteristic two* J. Cryptology, **11** (1998), no. 4, 219–234.

[24] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Mathematics of Computation, **44**, (1985), 483–494.

[25] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A, **46**, no. 2, (1987), 183–211.

[26] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, **106**, Springer-Verlag, New York, 1986.

[27] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, **151**, Springer-Verlag, New York, 1994.

[28] N. Smart, *Elliptic curve cryptosystems over small fields of odd characteristic*, J. Cryptology, **12** (1999), no. 2, 141–151.

[29] J. Solinas, *An Improved Algorithm for Arithmetic on a Family of Elliptic Curves*, in *Advances in Cryptology – CRYPTO'97 (Santa Barbara 1997)*, 357–371, Lecture Notes in Comp. Sci., **1294**, Springer, Berlin, 1997.

[30] M. Wiener and R. Zuccherato, *Faster attachs on elliptic curve cryptosystems*, in *Selected areas in cryptography (Kingston, ON, 1998)*, 190–200, Lecture Notes in Comp. Sci., **1556**, Springer–Verlag, Berlin, 1999.

[31] N. Yui and D. Zagier, *On the singular values of Weber modular functions*, Math. Comp., **66** (1997), no. 220, 1645–1662.

David R. Kohel
School of Mathematics and Statistics, F07
University of Sydney, NSW 2006,
Sydney, Australia
E-mail address: kohel@maths.usyd.edu.au