Generating Prime Order Elliptic Curves: Difficulties and Efficiency Considerations *

Elisavet Konstantinou[1,2], Aristides Kontogeorgis[3],
Yannis C. Stamatiou[1,3,4], and Christos Zaroliagis[1,2]

[1] Computer Technology Institute, P.O. Box 1122, 26110 Patras, Greece
[2] Dept of Computer Eng. & Informatics, Univ. of Patras, 26500 Patras, Greece
[3] Dept of Mathematics, Univ. of the Aegean, Karlovassi, 83200, Samos, Greece
[4] Joint Research Group (JRG) on Communications and Information Systems Security (Univ. of the Aegean and Athens Univ. of Economics and Business)
e-mail: {konstane,zaro}@ceid.upatras.gr,kontogar@aegean.gr, stamatiu@aegean.gr

Abstract. We consider the generation of prime order elliptic curves (ECs) over a prime field $\mathbb{F}_p$ using the Complex Multiplication (CM) method. A crucial step of this method is to compute the roots of a special type of class field polynomials with the most commonly used being the Hilbert and Weber ones, uniquely determined by the CM discriminant D. In attempting to construct prime order ECs using Weber polynomials two difficulties arise (in addition to the necessary transformations of the roots of such polynomials to those of their Hilbert counterparts). The first one is that the requirement of prime order necessitates that $D \equiv 3 \pmod 8$, which gives Weber polynomials with degree three times larger than the degree of their corresponding Hilbert polynomials (a fact that could affect efficiency). The second difficulty is that these Weber polynomials do not have roots in $\mathbb{F}_p$. In this paper we show how to overcome the above difficulties and provide efficient methods for generating ECs of prime order supported by a thorough experimental study. In particular, we show that such Weber polynomials have roots in $\mathbb{F}_{p^3}$ and present a set of transformations for mapping roots of Weber polynomials in $\mathbb{F}_{p^3}$ to roots of their corresponding Hilbert polynomials in $\mathbb{F}_p$. We also show how a new class of polynomials, with degree equal to their corresponding Hilbert counterparts (and hence having roots in $\mathbb{F}_p$), can be used in the CM method to generate prime order ECs. Finally, we compare experimentally the efficiency of using this new class against the use of the aforementioned Weber polynomials.

1 Introduction

The generation of elliptic curves (ECs) with good security properties has been one of the central considerations in Elliptic Curve Cryptography. One of the most

* This work was partially supported by the Action IRAKLITOS (Fellowships for Research in the University of Patras) with matching funds from EC and the Greek Ministry of Education.

efficient methods that can be employed for the construction of ECs with specified order is the *Complex Multiplication* (CM) method [1, 17]. Briefly, the CM method starts with the specification of a discriminant value D, the determination of the order p of the underlying prime field and the order m of the EC. It then computes a special polynomial, called *Hilbert* polynomial, which is uniquely determined by D and locates one of its roots modulo p. This root can be used to construct the parameters of an EC with order m over the field $\mathbb{F}_p$. A major drawback of Hilbert polynomials is that their coefficients grow very large with D and hence possess high computational demands. In order to eliminate this drawback, an alternative class of polynomials with much smaller coefficients, called *Weber* polynomials, can be used instead. The issue with Weber polynomials, however, is that their roots (modulo p) cannot be used to construct directly the parameters of the EC but they first have to be transformed into the roots of their corresponding Hilbert polynomials.

The CM method is not by itself adequate for applications that require robust ECs against cryptanalytic attacks. It turns out that the *properties* of the order of an EC play a central role in establishing cryptanalytic robustness. One way to establish robustness is to generate ECs whose order satisfies a certain number of properties designed to guard against the currently known most effective attacks [18, 24, 25]. An equally important alternative to cryptographic strength (see e.g., [26]) requires that the order of the generated EC is a prime number. Note that in certain applications it is necessary to have ECs of prime order [6]. Prime order ECs defined in various fields were also treated in [2, 16, 20, 23].

In this paper we follow the latter approach and study the use of the CM method for generating ECs of prime order in $\mathbb{F}_p$. Although ECs with no restrictions on their order may be generated more efficiently using a point counting (such as Schoof's [28]) algorithm[5], the requirement of prime order can severely change the situation. Point counting algorithms first choose the parameters of the EC and then compute its order. If this order is found non-prime, then another set of EC parameters is generated and the process is repeated. This can be seen, approximately, as sampling from the set of ECs of prime order (for a fixed p). There is well supported theoretical and experimental evidence [11] that this probability is, asymptotically, $\frac{c_p}{\log p}$, where c_p is a constant depending on p and satisfying $0.44 \leq c_p \leq 0.62$. Thus, it appears that prime orders are not especially favored by the point counting approach, as also noted in [11]. CM, on the other hand, starts with a prime number (the order of the EC) and *then* constructs the parameters thus avoiding this averse prime order probability.

In attempting to construct prime order ECs using Weber polynomials two additional difficulties arise. The first one is that the prime order requirement necessitates that $D \equiv 3 \pmod 8$, which in turn results in Weber polynomials with degree three times larger than the degree of their corresponding Hilbert polynomial. The second and most crucial difficulty is that such Weber polyno-

[5] There are cases where point counting algorithms can be very inefficient compared to the CM method, e.g., when p is large and the discriminant value is small.

mials (used for the construction of prime order ECs) do not have roots in $\mathbb{F}_p$ for certain values of p, as it is shown in Section 3.

Our work addresses the difficulties outlined above with an eye to applications and the practitioner's needs. We pay particular attention to support our theoretical findings with a thorough experimental study, thus shedding more light in the use of polynomials for the efficient generation of prime order ECs using the CM method, and providing guidance to the practitioner with respect to the resolution of these difficulties. In particular, we make the following contributions: (i) We show that Weber polynomials defined on values of $D \equiv 3 \pmod 8$ and used in the CM method for generating ECs of prime order have roots in the extension field $\mathbb{F}_{p^3}$ and not in $\mathbb{F}_p$. (ii) We present a set of simplified transformations that map the roots of the Weber polynomials in $\mathbb{F}_{p^3}$ to the roots of their corresponding Hilbert polynomials in $\mathbb{F}_p$. This implies that the particular Weber polynomials can be used to generate prime order ECs with the CM method. (iii) We show how a new class of polynomials can be used in the CM method for generating prime order ECs. The advantage of these polynomials is that they have the same degree with their corresponding Hilbert polynomials and hence have roots in $\mathbb{F}_p$. (iv) We perform a comparative experimental study regarding the efficiency of the CM method using the aforementioned Weber polynomials against using the new class of polynomials. Although it may seem that the use of Weber polynomials is inefficient due to their high degree and the fact that their roots lie in $\mathbb{F}_{p^3}$ (which requires operations with polynomials of degree 2), we provide experimental evidence which demonstrates that this is not always the case.

We would like to note that the case $D \equiv 3 \pmod 8$ can also be useful for the generation of ECs that do not necessarily have prime order [29] or for the generation of special curves, such as MNT curves [19, 20]. This makes our analysis for class polynomials with such discriminants even more useful.

The rest of the paper is organized as follows. In Section 2 we review some basic definitions and facts about ECs, the CM method, the Hilbert polynomials, and discuss some of their properties relevant to the generation of ECs. In Section 3 we present properties of Weber polynomials with $D \equiv 3 \pmod 8$ and describe their use in the CM method. In Section 4 we elaborate on the construction of a new class of polynomials that can also be used in the CM method. Finally, in Section 5 we present our experimental results concerning the efficiency of the CM method using Weber polynomials against using the new class of polynomials.

2 A Brief Overview of Elliptic Curve Theory and Complex Multiplication

This section contains a brief introduction to elliptic curve theory, to the Complex Multiplication method for generating prime order elliptic curves and to the Hilbert class field polynomials. Our aim is to facilitate the reading of the sections that follow. For full coverage of the necessary concepts and terms, the interested reader may consult [5]. Also, the proofs of certain theorems require

basic knowledge of algebraic number theory and Galois theory. The interested reader is referred to [8, 31, 32] for definitions not given here due to lack of space.

2.1 Preliminaries of Elliptic Curve Theory

An *elliptic curve* defined over a finite field $\mathbb{F}_p$, $p > 3$ and prime, is denoted by $E(\mathbb{F}_p)$ and contains the points $(x, y) \in \mathbb{F}_p$ (in affine coordinates) that satisfy the equation (in $\mathbb{F}_p$)

$$y^2 = x^3 + ax + b, \tag{1}$$

with $a, b \in \mathbb{F}_p$ satisfying $4a^3 + 27b^2 \neq 0$. The set of these points equipped with a properly defined point addition operation and a special point, denoted by $\mathcal{O}$ and called *point at infinity* (zero element for the addition operation), forms an Abelian group. This is the *Elliptic Curve group* and the point $\mathcal{O}$ is its identity element (see [5, 30] for more details on this group).

The *order*, denoted by m, is the number of points that belong in $E(\mathbb{F}_p)$. The numbers m and p are related by the *Frobenius trace* $t = p + 1 - m$. Hasse's theorem (see e.g., [5, 30]) implies that $|t| \leq 2\sqrt{p}$. Given a point $P \in E(\mathbb{F}_p)$, its *order* is the smallest positive integer n such that $nP = \mathcal{O}$. By Langrange's theorem, the order of a point $P \in E(\mathbb{F}_p)$ divides the order m of the group $E(\mathbb{F}_p)$. Thus, $mP = \mathcal{O}$ for any $P \in E(\mathbb{F}_p)$ and, consequently, the order of a point is always less than or equal to the order of the elliptic curve.

Two of the most important quantities of an elliptic curve $E(\mathbb{F}_p)$ defined through Eq. (1) are the *curve discriminant* Δ and the *j-invariant*: $\Delta = -16(4a^3 + 27b^2)$ and $j = -1728(4a)^3/\Delta$. Given a j-invariant $j_0 \in \mathbb{F}_p$ (with $j_0 \neq 0, 1728$) *two* ECs can be constructed. If $k = j_0/(1728 - j_0) \bmod p$, one of these curves is given by Eq. (1) by setting $a = 3k \bmod p$ and $b = 2k \bmod p$. The second curve (the *twist* of the first) is given by the equation

$$y^2 = x^3 + ac^2x + bc^3 \tag{2}$$

with c any quadratic non-residue of $\mathbb{F}_p$. If m_1 and m_2 denote the orders of an elliptic curve and its twist respectively, then $m_1 + m_2 = 2p + 2$ which implies that if one of the curves has order $p + 1 - t$, then its twist has order $p + 1 + t$, or vice versa (see [5, Lemma VIII.3]).

2.2 The Complex Multiplication Method

As stated in the previous section, given a j-invariant one may readily construct an EC. Finding a suitable j-invariant for a curve that has a given order m can be accomplished through the theory of *Complex Multiplication* (CM) of elliptic curves over the rationals. This method is called the *CM method* and in what follows we will give a brief account of it.

By Hasse's theorem, $Z = 4p-(p+1-m)^2$ must be positive and, thus, there is a unique factorization $Z = Dv^2$, with D a square free positive integer. Therefore

$$4p = u^2 + Dv^2 \tag{3}$$

for some integer u that satisfies the equation

$$m = p + 1 \pm u. \tag{4}$$

The negative parameter $-D$ is called a *CM discriminant for the prime* p. For convenience throughout the paper, we will use (the positive integer) D to refer to the CM discriminant. The CM method uses D to determine a j-invariant. This j-invariant in turn, will lead to the construction of an EC of order $p+1-u$ or $p+1+u$.

The method works as follows. Given a prime p, the smallest D is chosen for which there exists some integer u for which Eq. (3) holds. If neither of the possible orders $p+1-u$ and $p+1+u$ is suitable for our purposes, the process is repeated with a new D. If at least one of these orders is suitable, then the method proceeds with the construction of the *Hilbert polynomial* (uniquely defined by D) and the determination of its roots modulo p. Any root of the Hilbert polynomial can be used as a j-invariant. From this the corresponding EC and its twist can be constructed as described in Section 2.1. In order to find which one of the curves has the desired suitable order ($m = p + 1 - u$ or $m = p + 1 + u$), the method uses Langrange's theorem as follows: it repeatedly chooses points P at random in each EC until a point is found in one of the curves for which $mP \neq \mathcal{O}$. This implies that the curve we seek is the other one. It turns out that the most time consuming part of the CM method is the construction of the Hilbert polynomial. These polynomials have very large coefficients and their construction requires the use of high precision floating point arithmetic with complex numbers.

We now turn to the generation of prime order ECs. If m should be a prime number, then it is obvious that u should be odd. It is also easy to show that D should be congruent to 3 (mod 8) and v should be odd, too. In this paper, we follow a variant of the CM method for the construction of prime order elliptic curves. We first determine a discriminant $D \equiv 3 \pmod 8$ and then we construct the two prime numbers p and m. The most trivial way to do this, is by choosing at random odd integers u and v and then check whether p and m are prime using Eq. (3) and Eq. (4). Next, a Weber polynomial corresponding to the discriminant value D is constructed and we locate a root of it. This root, however, cannot lead to the construction of the j-invariant directly, since j-invariants are roots of the Hilbert polynomials. Therefore, we must transform this root to a root of the corresponding (constructed with the same discriminant) Hilbert polynomial. The necessary transformations are given in Section 3.

2.3 Hilbert Polynomials

Every CM discriminant D defines a unique Hilbert polynomial, denoted by $H_D(x)$. Given a positive D, the Hilbert polynomial $H_D(x) \in \mathbb{Z}[x]$ is defined as

$$H_D(x) = \prod_{\tau} (x - j(\tau)) \tag{5}$$

for values of τ satisfying $\tau = (-\beta + \sqrt{-D})/2\alpha$, for all integers α, β, and γ such that (i) $\beta^2 - 4\alpha\gamma = -D$, (ii) $|\beta| \leq \alpha \leq \sqrt{D/3}$, (iii) $\alpha \leq \gamma$, (iv)

$\gcd(\alpha, \beta, \gamma) = 1$, and (v) if $|\beta| = \alpha$ or $\alpha = \gamma$, then $\beta \geq 0$. The 3-tuple of integers $[\alpha, \beta, \gamma]$ that satisfies these conditions is called a *primitive, reduced quadratic form* of $-D$, with τ being a root of the quadratic equation $\alpha z^2 + \beta z + \gamma = 0$. Clearly, the set of primitive reduced quadratic forms of a given discriminant is finite. The quantity $j(\tau)$ in Eq. (5) is called *class invariant* and is defined as follows. Let $z = e^{2\pi\sqrt{-1}\tau}$ and $h(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)}$, where $\Delta(\tau) = \eta(\tau)^{24} = z\left(1 + \sum_{n\geq 1}(-1)^n\left(z^{n(3n-1)/2} + z^{n(3n+1)/2}\right)\right)^{24}$. Then, $j(\tau) = \frac{(256h(\tau)+1)^3}{h(\tau)}$.

Let h be the number of primitive reduced quadratic forms, which determines the *degree* (or *class number*) of $H_D(x)$. Then, the bit precision required for the generation of $H_D(x)$ can be estimated (see [17]) by

$$\text{H-Prec}(D) \approx \frac{\ln 10}{\ln 2}(h/4 + 5) + \frac{\pi\sqrt{D}}{\ln 2}\sum_{\tau}\frac{1}{\alpha}$$

with the sum running over the same values of τ as the product in Eq. (5). Hilbert polynomials have roots roots modulo p under certain conditions stated in the following theorem.

Theorem 1. *A Hilbert polynomial $H_D(x)$ with degree h has exactly h roots modulo p if and only if the equation $4p = u^2 + Dv^2$ has integer solutions and p does not divide the discriminant $\Delta(H_D)$ of the polynomial.*

Proof. Let H_K be the Hilbert class field of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$, and let $\mathcal{O}_{H_K}$ and $\mathcal{O}_K$ be the rings of algebraic integers of H_K and K respectively.

Let p be a prime such that $4p = u^2 + Dv^2$ has integer solutions. Then, according to [8, Th. 5.26] p splits completely in H_K. Let $H_D(x) \in \mathbb{Z}[x]$ be the Hilbert polynomial with root the real algebraic integer $j(\tau)$. Proposition 5.29 in [8] implies that $H_D(x)$ has a root modulo p if and only if p splits in H_K and does not divide its discriminant[6] $\Delta(H_D)$. But since $\frac{\mathcal{O}_{H_K}}{p\mathcal{O}_{H_K}}/\mathbb{F}_p$ is Galois, $H_D(x)$ has not only one root modulo p, but h distinct roots modulo p. □

There are finitely many primes dividing the discriminant $\Delta(H_D)$ of the Hilbert polynomial and infinitely many primes to choose. In elliptic curve cryptosystems the prime p is at least 160 bits. Therefore, an arbitrary prime almost certainly does not divide the discriminant.

3 The CM Method Using Weber Polynomials

In this section we define Weber polynomials for discriminant values $D \equiv 3 \pmod 8$ and prove that they do not have roots in $\mathbb{F}_p$ for certain primes p, but they do have roots in the extension field $\mathbb{F}_{p^3}$. We then discuss their efficiency when used in the CM method, and present a transformation that maps roots of Weber polynomials in $\mathbb{F}_{p^3}$ into the roots of their Hilbert counterparts in $\mathbb{F}_p$.

[6] For a definition of the discriminant of a polynomial see [7].

3.1 Weber Polynomials and Their Roots in Finite Fields

Weber polynomials are defined using the Weber functions (see [1, 13]):

$$f(y) = q^{-1/48}\prod_{r=1}^{\infty}(1+q^{(r-1)/2}) \qquad f_1(y) = q^{-1/48}\prod_{r=1}^{\infty}(1-q^{(r-1)/2})$$
$$f_2(y) = \sqrt{2}\ \ q^{1/24}\prod_{r=1}^{\infty}(1+q^{r}) \qquad \text{where } q = e^{2\pi y\sqrt{-1}}.$$

The Weber polynomial $W_D(x) \in \mathbb{Z}[x]$ for $D \equiv 3 \pmod 8$ is defined as

$$W_D(x) = \prod_{\ell}(x - g(\ell)) \tag{6}$$

where $\ell = \frac{-b+\sqrt{-D}}{a}$ satisfies the equation $ay^2+2by+c = 0$ for which $b^2-ac = -D$ and (i) $\gcd(a, b, c) = 1$, (ii) $|2b| \le a \le c$, and (iii) if either $a = |2b|$ or $a = c$, then $b \ge 0$. Let $\zeta = e^{\pi\sqrt{-1}/24}$. The class invariant $g(\ell)$ for $W_D(x)$ is defined by

$$g(\ell) = \begin{cases} \zeta^{b(c-a-a^2c)} \cdot f(\ell) & \text{if } 2 \nmid a \text{ and } 2 \nmid c \\ -(-1)^{\frac{a^2-1}{8}} \cdot \zeta^{b(ac^2-a-2c)} \cdot f_1(\ell) & \text{if } 2 \nmid a \text{ and } 2 \mid c \\ -(-1)^{\frac{c^2-1}{8}} \cdot \zeta^{b(c-a-5ac^2)} \cdot f_2(\ell) & \text{if } 2 \mid a \text{ and } 2 \nmid c \end{cases} \tag{7}$$

if $D \equiv 3 \pmod 8$ and $D \not\equiv 0 \pmod 3$, and

$$g(\ell) = \begin{cases} \frac{1}{2}\zeta^{3b(c-a-a^2c)} \cdot f^3(\ell) & \text{if } 2 \nmid a \text{ and } 2 \nmid c \\ -\frac{1}{2}(-1)^{\frac{3(a^2-1)}{8}} \cdot \zeta^{3b(ac^2-a-2c)} \cdot f_1^3(\ell) & \text{if } 2 \nmid a \text{ and } 2 \mid c \\ -\frac{1}{2}(-1)^{\frac{3(c^2-1)}{8}} \cdot \zeta^{3b(c-a-5ac^2)} \cdot f_2^3(\ell) & \text{if } 2 \mid a \text{ and } 2 \nmid c \end{cases} \tag{8}$$

if $D \equiv 3 \pmod 8$ and $D \equiv 0 \pmod 3$.

For these cases of the discriminant ($D \equiv 3 \pmod 8$), the Weber polynomial $W_D(x)$ has degree three times larger than the degree of its corresponding Hilbert polynomial $H_D(x)$. An upper bound for the precision requirements of Weber polynomials for both cases of D was presented in [16] and is equal to $3h + \frac{\pi\sqrt{D}}{24\ln 2}\sum_\ell \frac{1}{\alpha}$ for $D \not\equiv 0 \pmod 3$ and to $3h + \frac{\pi\sqrt{D}}{8\ln 2}\sum_\ell \frac{1}{\alpha}$ for $D \equiv 0 \pmod 3$. The sum runs over the same values of ℓ as the product of Eq. (6) and $3h$ is the degree of the Weber polynomial (h is the degree of the corresponding Hilbert polynomial).

Consider the modular function

$$\Phi_2(x, j) = (x - 16)^3 - jx \tag{9}$$

where j is a class invariant for the Hilbert polynomial. The three roots of the equation $\Phi_2(x, j) = 0$ are the powers f^{24}, $-f_1^{24}$ and $-f_2^{24}$ of the Weber functions. A transformation (used in the CM method) from roots of Weber polynomials

to roots of Hilbert polynomials was presented in [16], and is derived from the modular equation $\Phi_2(x, j) = 0$. The transformation for $D \not\equiv 0 \pmod 3$ is

$$R_H = \frac{(2^{12} R_W^{-24} - 16)^3}{2^{12} R_W^{-24}} \tag{10}$$

and for $D \equiv 0 \pmod 3$ is

$$R_H = \frac{(2^4 R_W^{-8} - 16)^3}{2^4 R_W^{-8}} \tag{11}$$

where R_W is a root of $W_D(x)$ and R_H is a root of $H_D(x)$. To use these transformations we have to locate R_W on a specific field, an issue not addressed in [16].

In the rest of this section we will show that when u, v are odd numbers and $D \equiv 3 \pmod 8$, then $W_D(x)$ does not have roots modulo p, but its roots belong to the extension field $\mathbb{F}_{p^3}$ (recall that the order $m = p+1 \pm u$ of the elliptic curve can be prime only if u is odd, which means that in Eq. (3) v must be odd, too).

Theorem 2. *If the equation $4p = u^2 + Dv^2$ has a solution and u, v are odd integers, then the Weber polynomial $W_D(x)$ with degree $3h$ ($D \equiv 3 \pmod 8$) has no roots modulo p.*

Proof. Given an integer c, let $\left(\frac{c}{2}\right)$ be the *Kronecker* symbol. From [22, Th. 3.1] we conclude that if $\left(\frac{-Dv^2}{2}\right) = -1$, then the polynomial $\Phi_2(x, j) \pmod p$ is irreducible modulo p. This means that if we could prove that $\left(\frac{-Dv^2}{2}\right) = -1$, then the equation $\Phi_2(x, j) = 0 \pmod p$ would have no roots $x \pmod p$ for a given $j \pmod p$. This j will be a root of Hilbert polynomial modulo p, which we know from Theorem 1 that always exists. But if there is no $x \pmod p$ that satisfies the equation $\Phi_2(x, j) = 0 \pmod p$, then the Weber polynomial cannot have a root modulo p either. If it had, then according to the transformations there would also exist an $x \pmod p$ which is a contradiction. We must prove now that $\left(\frac{-Dv^2}{2}\right) = -1$. Using the Kronecker symbol we know that $\left(\frac{-Dv^2}{2}\right) = -1$ if $-Dv^2$ is odd and $-Dv^2 \equiv \pm 3 \pmod 8$. We will show that $Dv^2 \equiv 3 \pmod 8$. Clearly, since $D \equiv 3 \pmod 8 = 8d_1 + 3$ and $v = 2v_1 + 1$ is odd, then Dv^2 is also odd. We have $Dv^2 = (8d_1 + 3)(2v_1 + 1)^2 = (8d_1 + 3)(4v_1^2 + 4v_1 + 1)$. That is, $Dv^2 \equiv 3(4v_1^2 + 4v_1 + 1) \pmod 8$ and because $v_1^2 + v_1$ is even then it is easily seen that $Dv^2 \equiv 3 \pmod 8$ which completes the proof. □

The next theorem establishes the main result of this section.

Theorem 3. *If the equation $4p = u^2 + Dv^2$ has a solution with u, v odd integers, then the Weber polynomial $W_D(x)$ has h monic irreducible factors of degree 3 modulo p. Thus, the polynomial has $3h$ roots in the extension field $\mathbb{F}_{p^3}$.*

Proof. We have proved in Theorem 2 that the Weber polynomial does not have roots modulo p if u, v are odd numbers and that the polynomial $\Phi_2(x, j)$ is irreducible modulo p. This means that $\Phi_2(x, j) = 0$ has three roots $x \in \mathbb{F}_{p^3}$ for a root $j \in \mathbb{F}_p$ of the Hilbert polynomial. According to Eq. (10) and Eq. (11), $x = 2^{12} R_W^{-24}$ if $D \not\equiv 0 \pmod 3$, and $x = 2^4 R_W^{-8}$ if $D \equiv 0 \pmod 3$. Thus, there are at least three roots of the Weber polynomial that correspond to a root $j \in \mathbb{F}_p$ of the Hilbert polynomial, and which are either in $\mathbb{F}_{p^3}$ or in an extension field of greater degree (at most 72 if $D \not\equiv 0 \pmod 3$ and at most 24 if $D \equiv 0 \pmod 3$).

Let $R_{W,j}$ be a root of the Weber polynomial that corresponds to a root j of the Hilbert polynomial. Let $f_j(x)$ be the minimal polynomial of $R_{W,j} \pmod p$. The degree of this polynomial will be at least 3, because the root $R_{W,j}$ is at least in $\mathbb{F}_{p^3}$. Then, the Weber polynomial can be written as

$$W_D(x) = \prod_j f_j(x) \pmod p. \tag{12}$$

Since the degree of the Weber polynomial is $3h$ and the roots j modulo p of the Hilbert polynomial are h (see Theorem 1) we have that every minimal polynomial $f_j(x)$ will have degree 3. Thus, Weber polynomials have h irreducible cubic factors. Every factor has 3 roots in $\mathbb{F}_{p^3}$, which means that there are totally $3h$ roots in $\mathbb{F}_{p^3}$. □

3.2 The Use of Weber Polynomials in the CM Method

In this subsection we will elaborate on the use of Weber polynomials for the generation of prime order ECs. The idea is that we replace Hilbert polynomials with Weber polynomials and then try to compute a root of the Hilbert polynomial from a root of its corresponding Weber polynomial. To compute the desired Hilbert root, we proceed in three stages. First, we construct the corresponding Weber polynomial. Second, we compute its roots in $\mathbb{F}_{p^3}$. Finally, we transform the Weber roots to the desired Hilbert roots in $\mathbb{F}_p$. The first stage is accomplished using the definition of Weber polynomials in Section 3.1. To compute a root of $W_D(x)$ in $\mathbb{F}_{p^3}$, we have to find an irreducible factor (modulo p) of degree 3 of the polynomial. This is achieved using Algorithm 3.4.6 from [7]. The irreducible factor has 3 roots in $\mathbb{F}_{p^3}$ from which it suffices to choose one, in order to accomplish the third stage.

Suppose that $x^3 + ax^2 + bx + c$ is an irreducible factor modulo p of the Weber polynomial. From this irreducible factor, we can compute three roots (one suffices for the CM method) of the Weber polynomial if we have already defined the reduction polynomial of the extension field $\mathbb{F}_{p^3}$. We simply set the reduction polynomial to be equal to the irreducible factor $x^3 + ax^2 + bx + c$ and then a root of the Weber polynomial would be just x.

Let us see an example: if $W_{403}(x) = x^6 - 12x^5 - 26x^4 + 4x^3 + 36x^2 + 20x + 4$ and $p = 72210766188035272971116573500 9$ then a factor of the Weber polynomial modulo p is $x^3 + 53084199835573195933109366113 8x^2 + 2654209991778659796655 46830567x + 7221076618803527 29711165735007$. Note that 403 is not divisible by 3 and $72210766188035272971116573500 7 = p - 2 \equiv -2 \pmod p$.

The following lemma allows us to determine the constant term of the irreducible factor and consequently to simplify the roots' transformation as we will see later.

Lemma 1. *Let $x^3 + ax^2 + bx + c$ be an irreducible factor (modulo p) of the Weber polynomial with $D \equiv 3 \pmod 8$. Then, the following hold: (i) if $D \equiv 0 \pmod 3$, then $c = -1$; (ii) if $D \not\equiv 0 \pmod 3$, then $c = -2$.*

Proof. The constant term of the Weber polynomial is equal to $(-1)^h$ for the first case of D and $(-2)^h$ for the second case (see [14]). The Galois group of the extension H_K/K operates on the roots modulo p of $H_D(x)$, and therefore on the cubic irreducible factors of $W_D(x)$ (every root of $H_D(x)$ corresponds to three roots of $W_D(x)$ and thus to a cubic irreducible factor). Since every element in this Galois group induces the identity on $\mathbb{F}_p$, all cubic factors of $W_D(x)$ will have the same constant term. Because the constant term of a monic polynomial is equal to the product of the constant terms of its monic irreducible factors, it can be easily seen that $c = -1$ for the first case of D and $c = -2$ for the second. □

We are now ready to present the transformations for mapping a Weber root in $\mathbb{F}_{p^3}$ to its corresponding Hilbert root in $\mathbb{F}_p$. Suppose that $R_W = x$ is a root of a Weber polynomial $W_D(x)$ in the extension field $\mathbb{F}_{p^3}$. The calculations in the transformations must be in $\mathbb{F}_{p^3}$ with reduction polynomial $x^3 + ax^2 + bx + c$, since R_W is a root in $\mathbb{F}_{p^3}$.

The transformations may seem quite complicated because of the arithmetic operations that take place in the extension field, but they can be simplified due to Lemma 1. Consider the case $D \not\equiv 0 \pmod 3$ for which an irreducible factor of the Weber polynomial is equal to $x^3 + ax^2 + bx - 2$. Then, $R_W^{-24} = x^{-24} = (\frac{x^2+ax+b}{x(x^2+ax+b)})^{24} = (\frac{x^2+ax+b}{2})^{24}$. This means that $2^{12}R_W^{-24} = \frac{(x^2+ax+b)^{24}}{2^{12}}$. Substituting it to Eq. (10) we finally have:

$$R_H = \frac{((x^2 + ax + b)^{24} - 2^{16})^3}{2^{24}(x^2 + ax + b)^{24}}. \tag{13}$$

Similarly, for $D \equiv 0 \pmod 3$ the transformation becomes:

$$R_H = \frac{2^8((x^2 + ax + b)^8 - 1)^3}{(x^2 + ax + b)^8}. \tag{14}$$

The nominator and the denominator of the two transformations are elements of $\mathbb{F}_{p^3}$. However we know that R_H is in $\mathbb{F}_p$ and we can find its value dividing only the leading coefficients of these two elements modulo p. To illustrate the above transformations, consider again the Weber polynomial W_{403}. Let p be a prime as in the previous example, and let the reduction polynomial be the factor of the $W_{403}(x)$ presented also in the previous example. Then, $((x^2+ax+b)^{24}-2^{16})^3 = 485216670393361675137940525358x^2+498390024660218217560914441491x+437505083747867349301080018378$ and $(x^2+ax+b)^{24} = 372203635398289746518033$

$419220x^2+19347185129379715850547880668 6x+10581862220484269140828428 9782$. The root R_H of the Hilbert polynomial is equal to $\frac{485216670393361675137940525358}{2^{24}37220363539828974651803341922 0} \pmod p = 188541528108458443856585415294$.

4 The CM Method Using a New Class of Polynomials

Even though Weber polynomials have much smaller coefficients than Hilbert polynomials and can be computed very efficiently, the fact that their degree for $D \equiv 3 \pmod 8$ is three times larger than the degree of the corresponding Hilbert polynomials can be a potential problem, because it involves computations in extension fields. Moreover, the computation of a cubic factor modulo p in a polynomial with degree $3h$ is more time consuming than the computation of a single root modulo p of a polynomial with degree h.

To alleviate these problems, we can use in the CM method a relatively new class of polynomials which have degree h like Hilbert polynomials. In particular, two types of polynomials can be constructed in $\mathbb{Z}[x]$ using two families of η-products: $m_l(z) = \frac{\eta(z/l)}{\eta(z)}$ [21] for an integer l, and $m_{p_1,p_2}(z) = \frac{\eta(z/p_1)\eta(z/p_2)}{\eta(z/(p_1p_2))\eta(z)}$ [10], where p_1, p_2 are primes such that $24|(p_1-1)(p_2-1)$. We will refer to the minimal polynomials of these products (powers of which generate the Hilbert class field and are called class invariants like $j(\tau)$) as $M_{D,l}(x)$ and $M_{D,p_1,p_2}(x)$, respectively, where D is the discriminant used for their construction.

The polynomials are obtained from these two families by evaluating their value at a suitably chosen system of quadratic forms. Once a polynomial is computed, we can use the modular equations $\Phi_l(x,j) = 0$ or $\Phi_{p_1,p_2}(x,j) = 0$, in order to compute a root modulo p of the Hilbert polynomial from a root modulo p of the $M_{D,l}(x)$ or the $M_{D,p_1,p_2}(x)$ polynomial, respectively. In this section we will construct polynomials using only the m_l family for prime values of l, in particular for $l = 3, 5, 7, 13$. The reason is that only for these values of l the modular equations have degree 1 in j. For all other values of l or for the m_{p_1,p_2} family, the degree in j is at least 2 (which makes the computations more "heavy"), the coefficients of the modular equations are quite large (which makes their use less efficient) and moreover, the computation of $m_{p_1,p_2}(z)$ involves the computation of four η-products and not two like $m_l(z)$.

In order to construct the polynomial $M_{D,l}(x)$ with $l = 3, 5, 7, 13$, we used Theorem 2 from [9] which for our purposes boils down to the following statement.

Theorem 4. *[9] Let $l \in \{3, 5, 7, 13\}$ and $D > 0$ a discriminant such that $l|D$. Choose the power m_l^e as specified in Table 1 . Assume $Q = [A, B, C]$ is a primitive quadratic form of discriminant D with $\gcd(A, l) = 1$, $\gcd(A, B, C) = 1$ and $B^2 \equiv -D \pmod{4l}$. If $\tau_Q = \frac{-B+\sqrt{-D}}{2A}$, then the minimal polynomial of $m_l^e(\tau_Q)$ has integer coefficients and can be computed from an l-system.*

An l-system is a system $S = \{(A_i, B_i, C_i)\}_{1 \le i \le h}$ of representatives of the reduced primitive quadratic forms of a discriminant $-D$ such that $B_i^2 - 4A_iC_i = -D$, $\gcd(A_i, l) = 1$ and $B_r \equiv B_s \pmod{2l}$ for all $1 \le r, s \le h$. For a more formal definition see [27].

l	class invariant
3	m_3^{12}
5	m_5^6
7	m_7^4
13	m_{13}^2

Table 1. Class invariants for different values of l.

Although the construction of $M_{D,l}(x)$ polynomials is explained in [9, 21, 22], the required computation of the primitive forms is not provided. In the following, we provide all the details for computing these forms, which we also used in our implementation. Possibly there are alternative ways to generate the same polynomial $M_{D,l}(x)$ with other, equivalent forms.

For the construction of the polynomials $M_{D,l}(x)$, and according to Theorem 4, the condition $B_r \equiv B_s \pmod{2l}$ can be replaced by the condition $B_i^2 \equiv -D \pmod{4l}$ and because $D \equiv 0 \pmod{l}$, we can write $B_i = l + 2lk_i \equiv l \pmod{2l}$ for an integer $k_i \geq 1$. In particular, $M_{D,l}(x) = \prod_{\tau_Q}(x - m_l^e(\tau_Q))$ where $Q = [A_i, B_i, C_i]$ is a primitive form satisfying the conditions $\gcd(A_i, l) = 1$, $B_i = l + 2lk_i$ and $\tau_Q = \frac{-B_i + \sqrt{-D}}{2A_i}$. The set of forms $[A_i, B_i, C_i]_{1 \leq i \leq h}$ can be computed from the set of the reduced primitive quadratic forms $[\alpha, \beta, \gamma]$ that are used for the construction of $H_D(x)$.

A form $[A_i, B_i, C_i]$ can be computed from a reduced primitive quadratic form $[\alpha, \beta, \gamma]$ using (at most) two transformations from [27, Prop. 3]. The first one transforms a form $[a, b, c]$ to an equivalent (having the same discriminant $-D$) form $[a, b + 2ak, c + bk + ak^2]$ for an integer k and the second transforms a form $[a, b, c]$ to an equivalent form $[a + bn + cn^2, b + 2cn, c]$ for an integer n. In order to compute a form $[A_i, B_i, C_i]$ we first transform a reduced primitive form $[\alpha, \beta, \gamma]$ to a form $[\alpha_1, \beta_1, \gamma_1]$ such that β_1 and γ_1 are divided by l, using the first transformation. This means that we choose an integer k such that $\beta_1 = \beta + 2\alpha k \equiv 0 \pmod{l}$ and $\gamma_1 = \gamma + \beta k + \alpha k^2 \equiv 0 \pmod{l}$. If $\alpha \equiv 0 \pmod{l}$, we just set $\alpha_1 = \gamma$ and $\gamma_1 = \alpha$, and we do not apply the transformation ($\beta_1 = \beta \equiv 0 \pmod{l}$, because $D \equiv 0 \pmod{l}$). After this transformation, we use the second transformation from [27] to compute the final form $[A_i, B_i, C_i]$ from $[\alpha_1, \beta_1, \gamma_1]$. Thus, $A_i = \alpha_1 + \beta_1 n + \gamma_1 n^2$, $B_i = \beta_1 + 2\gamma_1 n$ and $C_i = \gamma_1$ for an integer n such that $A_i > B_i > C_i$.

It is easy to see why this process yields a form that satisfies the desired conditions. The requirement $A_i > B_i > C_i$ exists because our experiments showed that it is necessary for the proper construction of the polynomial $M_{D,l}(x)$. For example, for $D = 51$ the reduced forms are $[1, 1, 13], [3, 3, 5]$ and the corresponding forms $[A_i, B_i, C_i]$ for $l = 3$ are $[67, 63, 15], [11, 9, 3]$.

The invariants $m_l^e(\tau)$ are related with $j(\tau)$ through the modular equation $\Phi_l(m_l^e(\tau), j(\tau)) = 0$, based on the definitions of $\Phi_l(x, j)$ for the different values of l given in Table 2.

l	$\Phi_l(x, j)$
3	$(x + 27)(x + 3)^3 - jx$
5	$(x^2 + 10x + 5)^3 - jx$
7	$(x^2 + 13x + 49)(x^2 + 5x + 1)^3 - jx$
13	$(x^2 + 5x + 13)(x^4 + 7x^3 + 20x^2 + 19x + 1)^3 - jx$

Table 2. Modular functions for different values of l.

Theorem 5. *A polynomial $M_{D,l}(x)$ has h roots modulo p if and only if the equation $4p = u^2 + Dv^2$ has an integer solution and p does not divide the discriminant $\Delta(M_{D,l})$ of the polynomial.*

Proof. It follows the same lines as that of Theorem 1. We know that the class invariants m_l^e generate the Hilbert class field, and therefore Proposition 5.29 from [8] hold. This implies that $M_{D,l}(x)$ has a root modulo p when $4p = u^2 + Dv^2$ has an integer solution, and since $\frac{\mathcal{O}_{H_K}}{p\mathcal{O}_{H_K}}/\mathbb{F}_p$ is Galois, the polynomial $M_{D,l}(x)$ has h distinct solutions modulo p. □

The polynomials $M_{D,l}(x)$ can be used in the CM method in a more straightforward way, compared to that of Weber polynomials for the case of prime order elliptic curves. Since $M_{D,l}(x)$ has roots R_M modulo p, we use an algorithm for their computation (for example Berlekamp's algorithm [4]) and then we can compute the roots R_H modulo p of the corresponding Hilbert polynomial $H_D(x)$ from the modular equation $\Phi_l(R_M, R_H) = 0$.

We finally note that the precision required for the construction of the $M_{D,l}(x)$ polynomials is approximately $\frac{1}{l}$H-Prec(D) [9].

5 Implementation and Experimental Results

All of our implementations were made in ANSI C using the (ANSI C) GNUMP [12] library for high precision floating point arithmetic and also for the generation and manipulation of integers of unlimited precision. The implementation includes the construction of the Hilbert, Weber and $M_{D,l}(x)$ polynomials, algorithms for the computation of roots modulo p of a polynomial, algorithms for the computation of a cubic factor of a polynomial modulo p, and of course all the steps of the CM method for the generation of prime order elliptic curves. All implementations and experiments have been carried out on a Pentium III (933 MHz) running Linux and equipped with 256 MB of main memory.

Our experiments first focused on the bit precision and the time requirements needed for the construction of Weber and $M_{D,l}(x)$ polynomials with $D \equiv 3 \pmod 8$. We also conducted experiments with Hilbert polynomials and we noticed, as expected, that their construction is much less efficient than the construction of Weber or $M_{D,l}(x)$ polynomials for all values of D and l. For this reason we do not report on these polynomials here (experimental studies regarding Hilbert and other polynomials can be found e.g., in [3, 15]). Concerning

Weber polynomials we used discriminants $D \not\equiv 0 \pmod 3$. We avoid discriminants $D \equiv 0 \pmod 3$ because the precision requirements are greater than those of the case $D \not\equiv 0 \pmod 3$. We have considered various values of D and h and report on our experimental results in Figure 1 and Figure 2. We noticed, as the theory dictates, that the precision required for the construction of Weber polynomials $W_D(x)$ is less than the precision required for the construction of $M_{D,l}(x)$ polynomials for all the values of l that we examined (in Section 4 we explained why we consider these particular values of l). Among the $M_{D,l}(x)$ polynomials the least precision is required for the construction of $M_{D,13}(x)$, followed by the construction of $M_{D,7}(x)$, followed by the construction of $M_{D,5}(x)$. The greatest requirements in precision are set by the $M_{D,3}(x)$ polynomials.

The same ordering can be observed in the construction time. For Figure 2 (time in seconds) we used the same values of D as in Figure 1 and also in this figure the differences among the polynomials are very clear. We observed that the time for the construction of $M_{D,l}(x)$ depends not only on the precision requirements of the polynomials, but also on the convergence rate of η-products. The greater the l, the slower the convergence. This is why in Figure 2 the differences do not seem to be analogous with the differences in Figure 1. This favors Weber polynomials, as the η-products in their construction converge faster than any of the $M_{D,l}(x)$ polynomials, making their generation even more efficient.

The coefficients of the Weber polynomials are also smaller than the coefficients of the $M_{D,l}(x)$ polynomials, following the same relative order with precision and time. However, the disadvantage of Weber polynomials is that their degree is three times larger than the degree of the $M_{D,l}(x)$ polynomials. Therefore, the space required for the storage of a Weber polynomial $W_D(x)$ can be larger than the space required for the storage of $M_{D,13}(x)$ or $M_{D,7}(x)$. Actually, it turns out that $M_{D,l}(x)$ polynomials can be even more advantageous when it comes to storage requirements as our experiments showed. Suppose that $M_{D,l}(x) = x^h + M_1 x^{h-1} + ... + M_{h-1}x + M_h$ and h is even. We noticed that every coefficient M_i of $M_{D,l}(x)$ is divisible by l. Moreover, when $l = 13$, then $M_h = 13^{h/2}$ and $\frac{M_{h-i}}{M_i} = 13^{h/2-i}$ for $1 \leq i \leq (h/2-1)$. For $l = 7$, $M_h = 7^h$, $\frac{M_{h-i}}{M_i} = 7^{h-2i}$; for $l = 5$, $M_h = 5^{3h/2}$, $\frac{M_{h-i}}{M_i} = 5^{3h/2-3i}$; and finally for $l = 3$ we have $M_h = 3^{3h}$, $\frac{M_{h-i}}{M_i} = 3^{3h-6i}$. Using these properties of the $M_{D,l}(x)$ polynomials, we can reduce the space required for their storage (if someone wants to store them for subsequent use).

This is not the only advantage of $M_{D,l}(x)$ against $W_D(x)$. The large degree of the Weber polynomials is a disadvantage for the time efficiency of the CM method, because the time for finding a cubic factor of the polynomial can be much larger than the time for finding a single root modulo p of a polynomial with three times smaller degree. In Table 3 we report on the time (in seconds) that is required for the computation of a cubic factor modulo p of $W_D(x)$, denoted by T_W, and the time that is required for the computation of a linear factor modulo p of the $M_{D,l}(x)$ polynomials denoted by T_M, for various values of l. The prime p has size 160 bits. C_W and C_M is the time required for the construction of the $W_D(x)$ and the $M_{D,l}(x)$ polynomials, respectively. The degree of $W_D(x)$ is $3h$.

Note that $C_W + T_W$ (resp. $C_M + T_M$) is the time that mostly dominates and differentiates the use of polynomials (Weber versus $M_{D,l}(x)$) in the CM method, since the time for the other steps of the method is practically independent of the polynomials used.

D	h	l	T_W	C_W	T_M	C_M
403	2	13	0.12	0.63	0.01	0.38
1027	4	13	0.40	1.31	0.02	0.36
2035	8	5	1.53	2.35	0.07	1.31
2795	12	13	3.88	3.60	0.13	2.12
4403	20	7	13.12	5.15	0.44	8.71
5603	22	13	16.97	6.94	0.50	8.38
6995	32	5	41.05	9.64	1.72	36.03
22435	32	5	41.05	17.80	1.72	72.94

Table 3. Time for the computation of a cubic factor of Weber polynomials and of a linear factor of the $M_{D,l}(x)$ polynomials, together with their construction time.

We observe from Table 3 that C_W+T_W is almost always larger than C_M+T_M, implying that the use of Weber polynomials is more time consuming than the use of the $M_{D,l}(x)$ polynomials. However, we also observed that in some cases when D increases, h is of moderate size and $l \in \{3, 5\}$, the construction of the $M_{D,l}(x)$ polynomials may become less efficient (cf. last line of Table 3) and the total time of the CM method with these polynomials can be larger than the time required by the method when their corresponding Weber polynomials are used.

In conclusion, the type of polynomial that one should use depends on the particular application. If the main focus is on time or precision regarding the construction of the polynomials, then Weber polynomials should be preferred. If the focus is on fast and frequent generation of ECs and which implies storage of polynomials for subsequent use in the CM method, then the $M_{D,l}(x)$ polynomials ($l \neq 3$) must be preferred. Finally, if the class polynomials are computed online with the CM method, then the selection of the proper polynomial depends on the value of D and h. Notice though, that Weber polynomials can be constructed for any value of $D \equiv 3 \pmod 8$, while $M_{D,l}(x)$ polynomial add a restriction for D, demanding that $D \equiv 0 \pmod l$.

References

1. A.O.L. Atkin and F. Morain, Elliptic curves and primality proving, *Mathematics of Computation* 61(1993), pp. 29-67.
2. H. Baier, Elliptic Curves of Prime Order over Optimal Extension Fields for Use in Cryptography, in *Progress in Cryptology* – INDOCRYPT 2001, LNCS Vol. 2247 (Springer-Verlag, 2001), pp. 99-107.
3. H. Baier, Efficient Algorithms for Generating Elliptic Curves over Finite Fields Suitable for Use in Cryptography, PhD Thesis, Dept. of Computer Science, Technical Univ. of Darmstadt, May 2002.

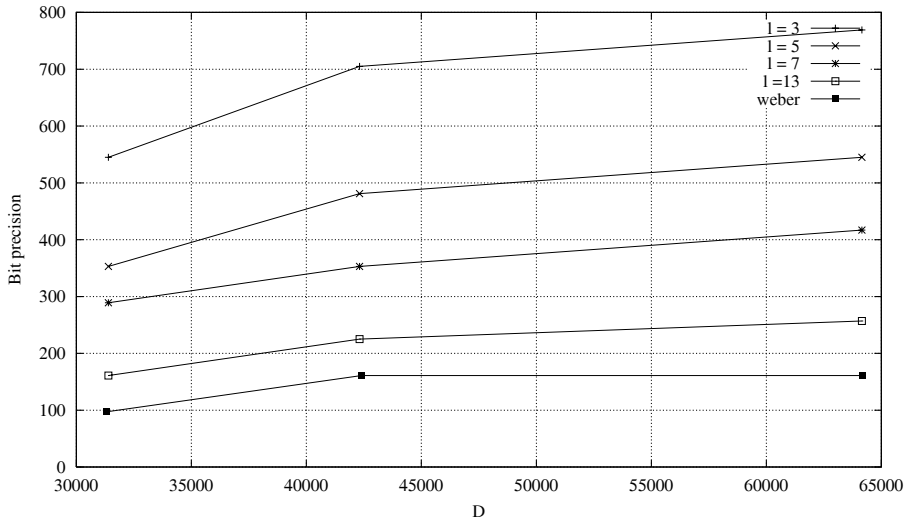

Fig. 1. Bit precision for the construction of class polynomials

4. E. R. Berlekamp, Factoring polynomials over large finite fields, *Mathematics of Computation* 24(1970), pp. 713-735.
5. I. Blake, G. Seroussi, and N. Smart, *Elliptic curves in cryptography* , London Mathematical Society Lecture Note Series 265, Cambridge University Press, 1999.
6. D. Boneh, B. Lynn, and H. Shacham, Short signatures from the Weil pairing, in *ASIACRYPT 2001*, LNCS 2248, pp. 514-532, Springer-Verlag, 2001.
7. H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, **138**, Springer-Verlag, Berlin, 1993.
8. D. A. Cox, *Primes of the form* $x^2 + ny^2$, John Wiley and Sons, New York, 1989.
9. A. Enge and F. Morain, Comparing invariants for class fields of imaginary quadratic fields, in *Algebraic Number Theory* – ANTS V, Lecture Notes in Computer Science Vol. 2369, Springer-Verlag, pp. 252-266, 2002.
10. A. Enge and R. Schertz, Constructing elliptic curves from modular curves of positive genus, Preprint, 2003.
11. S. Galbraith and J. McKee, The probability that the number of points on an elliptic curve over a finite field is prime, *Journal of the London Mathematical Society*, 62(2000), no. 3, pp. 671-684.
12. GNU multiple precision library, edition 3.1.1, September 2000. Available at: `http://www.swox.com/gmp`.
13. IEEE P1363/D13, *Standard Specifications for Public-Key Cryptography*, 1999. `http://grouper.ieee.org/groups/1363/tradPK/draft.html`.
14. E. Kaltofen and N. Yui, Explicit construction of the Hilbert class fields of imaginary quadratic fields by integer lattice reduction. Research Report 89-13, Rensselaer Polytechnic Institute, May 1989.
15. E. Konstantinou, Y. Stamatiou, and C. Zaroliagis, On the Efficient Generation of Elliptic Curves over Prime Fields, in *Cryptographic Hardware and Embedded Systems* – CHES 2002, Lecture Notes in Computer Science Vol. 2523, Springer-Verlag, pp. 333-348, 2002.

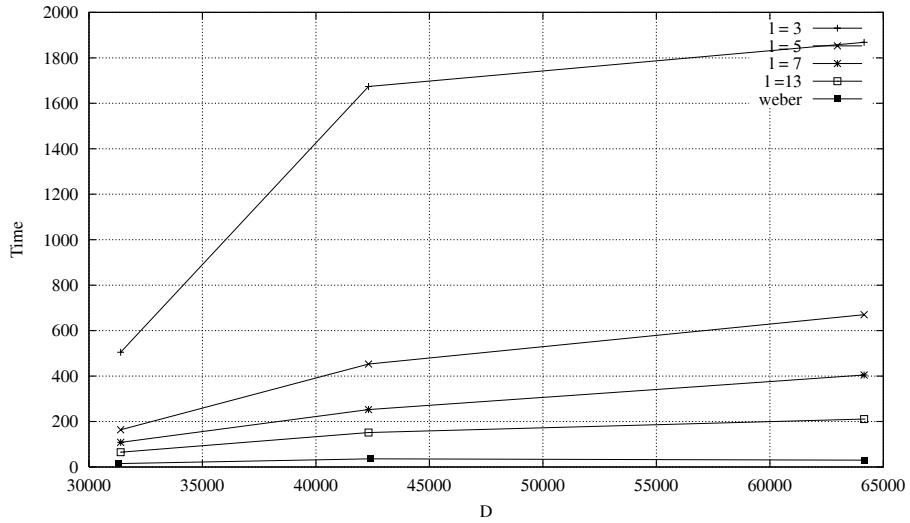

Fig. 2. Time requirements for the construction of class polynomials

16. E. Konstantinou, Y.C. Stamatiou, and C. Zaroliagis, On the Construction of Prime Order Elliptic Curves, in *Progress in Cryptology* – INDOCRYPT 2003, Lecture Notes in Computer Science Vol. 2904, Springer-Verlag, pp. 309-322, 2003.
17. G.J. Lay and H. Zimmer, Constructing Elliptic Curves with Given Group Order over Large Finite Fields, in *Algorithmic Number Theory* – ANTS-I, Lecture Notes in Computer Science Vol. 877, Springer-Verlag, pp. 250-263, 1994.
18. A. J. Menezes, T. Okamoto and S. A. Vanstone, Reducing elliptic curve logarithms to a finite field, *IEEE Trans. Info. Theory*, 39(1993), pp. 1639-1646.
19. A. Miyaji, M. Nakabayashi, and S. Takano, Characterization of Elliptic Curve Traces under FR-reduction, in *International Conference on Information Security and Cryptology* – ICISC 2000, Lecture Notes in Computer Science Vol. 2015, Springer-Verlag, pp. 90-108, 2001.
20. A. Miyaji, M. Nakabayashi, and S. Takano, New explicit conditions of elliptic curve traces for FR-reduction, *IEICE Transactions on Fundamentals*, E84-A(5):1234-1243, 2001.
21. F. Morain, Modular curves and class invariants, Preprint, June 2000.
22. F. Morain, Computing the cardinality of CM elliptic curves using torsion points, Preprint, October 2002.
23. Y. Nogami and Y. Morikawa, Fast generation of elliptic curves with prime order over $F_{p^{2^c}}$, in *Proc. of the International workshop on Coding and Cryptography*, March 2003.
24. G. C. Pohlig and M. E. Hellman, An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance, *IEEE Trans. Info. Theory*, 24 (1978), pp. 106-110.
25. T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, *Comm. Math. Univ. Sancti Pauli*, 47(1998), pp. 81-91.

26. E. Savaş, T.A. Schmidt, and Ç.K. Koç, Generating Elliptic Curves of Prime Order, in *Cryptographic Hardware and Embedded Systems* – CHES 2001, LNCS Vol. 2162 (Springer-Verlag, 2001), pp. 145-161.
27. R. Schertz, Weber's class invariants revisited, *Journal de Théorie des Nombres de Bordeaux* **4**, pp. 325-343, 2002.
28. R. Schoof, Counting points on elliptic curves over finite fields, *J. Theorie des Nombres de Bordeaux*, 7(1995), pp.219-254.
29. M. Scott and P. S.L.M. Barreto, Generating more MNT elliptic curves, Cryptology ePrint Archive, Report 2004/058, 2004.
30. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, GTM 106, 1986.
31. I. Stewart, *Galois Theory*, Third Edition, Chapman & Hall/CRC, Boca Raton, FL, 2004.
32. I. Stewart and D. Tall, *Algebraic Number Theory*, Second Edition, Chapman & Hall, London, 1987.