Elliptic Curves of Prime Order over Optimal Extension Fields for Use in Cryptography

Harald Baier*

Darmstadt University of Technology, Computer Science Department,
Alexanderstr. 10, 64283 Darmstadt, Germany,
hbaier@cdc.informatik.tu-darmstadt.de

Abstract. We present an algorithm for generating elliptic curves of prime order over Optimal Extension Fields suitable for use in cryptography. The algorithm is based on the theory of Complex Multiplication. Furthermore, we demonstrate the efficiency of the algorithm in practice by giving practical running times. In addition, we present statistics on the number of cryptographically strong elliptic curves of prime order for Optimal Extension Fields of cardinality $(2^{32} + c)^5$ with $c < 0$. We conclude that there are sufficiently many curves in this case.

Keywords: complex multiplication, cryptography, elliptic curve, Optimal Extension Field

1 Introduction

Since their proposal for use in cryptography about 15 years ago ([Kob87], [Mil86]), elliptic curve cryptography has gained a lot of attention in the cryptographic community due to their short key lengths. However, as of today, only two families of finite fields have found consideration in practice: Finite fields of characteristic 2 and finite prime fields of large characteristic. Algorithms to find elliptic curves for use in cryptography are well known for both families of fields.

Recently, a new type of finite fields was proposed for use in practice: Optimal Extension Fields ([BP98], [BP01]). Optimal Extension Fields consider the hardware in use (i.e. the word size of the processor) and thus yield an efficient way of implementing finite field arithmetic, especially the inversion. As the inversion is the most time-consuming step for adding points on elliptic curves over finite fields, Optimal Extension Fields have the potential to be considered as a third family of finite fields for elliptic curve cryptography.

In order to decide whether an elliptic curve is suitable for use in cryptography, we have to know its group order. However, when choosing random curves and using the efficient point counting algorithms, we have to choose a couple of curves before finding a suitable one. This turns out to be rather slow. Hence, we make

* supported by FairPay, a project funded by the German Department of Trade and Industry

C. Pandu Rangan, C. Ding (Eds.): INDOCRYPT 2001, LNCS 2247, pp. 99–107, 2001.

use of the Complex Multiplication Theory to find suitable elliptic curves over Optimal Extension Fields. Due to security reasons we restrict to elliptic curves of prime order. We will develop a closed algorithm solving this task.

Processors of word size 32-bit play a crucial role in practice. Hence, we will show that our algorithm is very fast in this case. Let p be a 32-bit prime with $2^{32} - p < 2^{16}$. Our algorithm finds a cryptographically strong elliptic curve of prime order over an Optimal Extension Field $\mathbb{F}_{p^5}$ in about 22 seconds using an ordinary PC. In addition, we present data on the number of suitable elliptic curves over Optimal Extension Fields of the form $\mathbb{F}_{p^5}$. We conclude that, for fields of this form, their quantity is sufficiently large.

The paper is organized as follows: In the next section we review the basic definitions of Optimal Extension Fields and elliptic curves suitable for use in cryptography. We present our generating algorithm in Sect. 3. Finally, in Sect. 4 we present sample running times of our implementation and discuss statistics on the number of elliptic curves of prime order over fields of the form $\mathbb{F}_{p^5}$ with a 32-bit prime p.

2 Elliptic Curves over Optimal Extension Fields

We review the definition and some properties of Optimal Extension Fields and elliptic curves. Furthermore, we list the conditions on elliptic curves suitable for use in cryptography. Let us first turn to Optimal Extension Fields.

Definition 1. *Let c be a rational integer, and let $p = 2^n + c$ be prime with $n \in \mathbb{N}$. Furthermore, assume $|c| \leq \sqrt{2^n}$, and let $m \in \mathbb{N}$. If there is a $\omega \in \mathbb{F}_p$ such that the binomial $X^m - \omega$ is irreducible in $\mathbb{F}_p[X]$, then $\mathbb{F}_{p^m}$ is called an* Optimal Extension Field.

The basic idea of introducing Optimal Extension Fields is to adapt the arithmetic over finite extension fields to the hardware in use (see [BP98], [BP01]). For instance, when implementing an elliptic curve cryptosystem on a 32-bit processor, one may choose $n = 32$ and $c < 0$ such that $2^{32} + c$ is prime. Hence, the arithmetic in $\mathbb{F}_p$ fits in a word size. Furthermore, let ω be as in definition 1. We represent $\mathbb{F}_{p^m}$ as the factor ring $\mathbb{F}_p[X]/(X^m - \omega)$ with respect to the polynomial basis $\{1, X, X^2, \ldots, X^{m-1}\}$. Hence, in $\mathbb{F}_{p^m}$ the identity $X^m = \omega$ holds, yielding an easy reduction of X^k for $k \geq m$.

Bailey and Paar [BP01] distinguish two special types of Optimal Extension Fields: First, if $|c| = 1$, the according Optimal Extension Field is called a *Type I* OEF. Second, if $X^m - 2$ is irreducible in $\mathbb{F}_p[X]$, they name the according field *Type II* OEF. In this paper we do not make use of Type I OEFs.

In order to decide whether an irreducible binomial of degree m exists in $\mathbb{F}_p[X]$ we make use of the following theorem, which we prove in [Bai01b].

Theorem 1. *Let p and m be rational primes. For $\omega \in \mathbb{F}_p^\times$ the following properties are equivalent:*

1. *The binomial $X^m - \omega$ is irreducible in $\mathbb{F}_p[X]$.*

2. *m divides the order e of ω in $\mathbb{F}_p^\times$, but not $\frac{p-1}{e}$.*
3. *We have $m \mid p-1$ and $\omega^{\frac{p-1}{m}} \not\equiv 1 \bmod p$.*

Using the property that $\mathbb{F}_p^\times$ is a cyclic group, the following corollary is an easy consequence of property 3 in theorem 1.

Corollary 1. *Let p and m be primes. There exists an irreducible binomial of degree m in $\mathbb{F}_p[X]$ if and only if $m \mid p-1$.*

Next, we review a few basic facts concerning elliptic curves over finite fields and define cryptographically strong ones. Let p be a prime number, $p > 3$, and let $q = p^m$ with $m \in \mathbb{N}$. An *elliptic curve* over the field $\mathbb{F}_q$ is a pair $E = (a, b) \in \mathbb{F}_q^2$ with $4a^3 + 27b^2 \neq 0$. A *point* on E is a solution $(x, y) \in \mathbb{F}_q^2$ of $y^2 = x^3 + ax + b$ or the point at infinity O obtained by considering the projective closure of this equation. The set of points on E over $\mathbb{F}_q$ is denoted by $E(\mathbb{F}_q)$. It turns out that $E(\mathbb{F}_q)$ carries a group structure with the point at infinity acting as the identity element.

We call the elliptic curve E *cryptographically strong* if it satisfies the following conditions: We have $|E(\mathbb{F}_q)| = k \cdot r$ with a prime $r > 2^{159}$ and a positive integer $k \leq 4$. The first requirement avoids generic attacks as the ρ-algorithm of Pollard, while the second one is due to efficiency reasons. If $m \geq 2$ and $p \geq 11$ this condition implies that E is not defined over $\mathbb{F}_p$. In addition, in order to avoid anomalous curves, the primes r and p are different. Finally, the order of q in the multiplicative group $\mathbb{F}_r^\times$ is at least $\left\lceil \frac{2000}{\log_2(q)} \right\rceil$; hence, we exclude curves which are amenable to the attack of Menezes, Okamoto, and Vanstone. An explanation of either attack may be found in [BSS99].

In addition, the German Information Security Agency (GISA) requires the class number of the maximal order containing the endomorphism ring of E to be at least 200. Although there is no consensus on this requirement in the community, we take it into account for the following two reasons: First, in order to provide curves for digital signatures being in conformance with the German Digital Signature Act, we have to respect the requirements of the GISA. Second, we want to show that our algorithm is *not* restricted to discriminants of small class numbers. However, our algorithm is applicable to the case of small class numbers either.

In this paper we focus on Optimal Extension Fields of the form p^5 with a 32-bit prime p. The reason for the choice $m = 5$ is twofold. Due to a theorem of Hasse we have $|E(\mathbb{F}_q)| \approx q$. Hence, in order to generate an elliptic curve of prime order r with $r \approx 2^{160}$ we have to ensure $m \geq 5$. Second, we restrict to extension fields of prime degree as some of our sub-algorithms of section 3 are very efficient in this case. However, the security implications of the Weil-descent ([GHS01]) on these curves are not yet clear. Nevertheless, the generalization to composite m is easy.

We are not aware of any further efficient algorithm to find an elliptic curve over an Optimal Extension Field of characteristic ≥ 5 respecting all these requirements. Although the Schoof-Elkies-Atkin (SEA) algorithm is polynomial

time for arbitrary finite fields and efficiently implemented for Optimal Extension Fields, it turns out to be much slower in practice. The main reason is that we have to choose a number of curves and determine their cardinalities before finding a suitable one. Furthermore, the very efficient Satoh-algorithm for fields of characteristic 2 ([FGH01]) does not apply to Optimal Extension Fields.

3 The Generating Algorithm

Our generating algorithm `oefCurve`, presented at the end of this section, makes use of the theory of Complex Multiplication. A good reference of this theory in the scope of elliptic curve cryptography may be found in [AM93], [LZ94], and [BB00]. We sketch the most important theory used in our algorithm. A central term is that of an *imaginary quadratic discriminant*, which is a negative integer Δ congruent 0 or 1 modulo 4. Our aim is to find a prime power p^m and an elliptic curve defined over a field $\mathbb{F}_{p^m}$, but not over $\mathbb{F}_p$. In order to do this we first have to find a prime power p^m and a discriminant Δ, such that the norm equation

$$t^2 - \Delta y^2 = 4p^m \tag{1}$$

has a solution $(t, y) \in \mathbb{Z}^2$, while the equation $t'^2 - \Delta y'^2 = 4p$ does not have a solution $(t', y') \in \mathbb{Z}$. If this is true, using Complex Multiplication, we find elliptic curves $E_{1,q}$ and $E_{2,q}$ over $\mathbb{F}_{p^m}$, both not defined over $\mathbb{F}_p$, with

$$|E_{1,q}(\mathbb{F}_{p^m})| = p^m + 1 - t, \quad |E_{2,q}(\mathbb{F}_{p^m})| = p^m + 1 + t \tag{2}$$

analogously as explained in [BB00].

Let $H \in \mathbb{Z}[X]$ be the the minimal polynomial of $j(\frac{\Delta+\sqrt{\Delta}}{2})$ where j denotes the well-known modular function j. Modulo p the polynomial H splits into irreducible factors of degree m, while it splits in $\mathbb{F}_{p^m}[X]$ into pairwise distinct linear factors. Let $j_q \in \mathbb{F}_{p^m}$ be a zero of H mod p. If $\Delta < -4$, we have $j_q \notin \{0; 1728\}$, and for any non-square $s_q \in \mathbb{F}_{p^m}$ we set

$$\kappa_q = \frac{j_q}{1728 - j_q}, \quad (a_q, b_q) = (3\kappa_q, 2\kappa_q)\ . \tag{3}$$

Then we have

$$\{E_{1,q}, E_{2,q}\} = \{(a_q, b_q), (a_q s_q^2, b_q s_q^3)\}. \tag{4}$$

After this construction it is not known which of the curves is $E_{1,q}$ and which is $E_{2,q}$. However, by choosing points on each curve and testing whether their order is a divisor of $p^m + 1 + t$ or $p^m + 1 - t$, the curves $E_{1,q}$ and $E_{2,q}$ can be identified.

Thus we can decide whether one of the curves $E_{1,q}$ or $E_{2,q}$ is cryptographically strong before we actually construct those curves. We only need to know the primes p and m and the norm representation of p^m as in (1). From (2) we deduce the orders of $E_{1,q}$ and $E_{2,q}$, and we can check whether one of the curves respects *all* conditions from the previous section.

Input of our algorithm `oefCurve`(n, m, h_0) is a positive integer n (e.g. the word size of the processor in use), the degree m of the Optimal Extension Field over its prime field, and an integer $h_0 \geq 200$. The algorithm returns a prime $p < 2^n$ such that $\mathbb{F}_{p^m}$ is an Optimal Extension Field, an irreducible binomial $X^m - \omega$ in $\mathbb{F}_p[X]$, and an elliptic curve E of prime order r defined over $\mathbb{F}_{p^m}$ respecting all requirements of Sect. 2. Furthermore, the endomorphism ring of E is a maximal order of class number at least h_0. In addition, `oefCurve` returns a generating point of $E(\mathbb{F}_{p^m})$. In order to get reasonable results we have to ensure $n \cdot m \geq 160$ and that m is prime.

We next explain our main algorithm `oefCurve`. It splits into several sub-algorithms, which we discuss in what follows. The first sub-algorithm `findField`(n, m, h_0) determines an Optimal Extension Field of cardinality p^m and a prime r being the group order of a cryptographically strong elliptic curve defined over $\mathbb{F}_{p^m} \setminus \mathbb{F}_p$. To be more precise, `findField` computes among other things a prime p of the form $2^n + c$ with $c < 0$ and $|c| < \sqrt{2^n}$ such that $m \mid p-1$. Although it is not clear if such a prime p exists for a random tuple (n, m), the asymptotic density of such primes for growing n is $\frac{1}{(m-1)\cdot\log(2^n)}$ due to the Prime Number Theorem and a theorem of Dirichlet on the number of primes in arithmetic progressions. Hence, for example, if $n = 32$ and $m = 5$ (i.e. the case we are most interested in), there should be about $\frac{2^{16}}{4\log(2^{32})} = 739$ primes congruent 1 modulo 5 in the interval $[2^{32} - 2^{16}, 2^{32}]$. However, the exact number is 733. Thus we may assume, that an appropriate prime p exists.

In order to be successful, `findField` has to solve the norm equation (1) for some Δ and p. We explain how to find appropriate Δ and p. A necessary condition on Δ for E to be of prime order is $\Delta \equiv 5 \bmod 8$. We assume that a sufficiently large database of fundamental imaginary quadratic discriminants $\Delta \equiv 5 \bmod 8$ of class number at least 200 is to our disposal. In our tests we make use of a database containing all such fundamental discriminants $\Delta > -6000000$. Our function `nextDiscriminant`(h, Δ) returns the maximal fundamental discriminant $\Delta' \equiv 5 \bmod 8$ of class number h with $\Delta' < \Delta$.

The algorithm is exponential in $\log(h)$ In addition, it depends on the bit-length of Δ. Thus we want h and $|\Delta|$ to be as small as possible. A necessary condition, due to class field theory, we have to take care of is $m \mid h(\Delta)$. Hence we set $h = \min\{h' \in \mathbb{N} : h' \geq h_0, m \mid h'\}$. Let $\Delta \equiv 5 \bmod 8$ be maximal of class number h. We set $p = \max\{p' \in \mathbb{Z} : p' < 2^n, p' \equiv 1 \bmod m, p' \text{ prime}\}$. We determine whether the norm equation $t^2 - \Delta y^2 = 4p$ has a solution $(t, y) \in \mathbb{Z}^2$ by using an algorithm due to Cornacchia ([Coh95], p.34-36): `cornacchia`(Δ, p) gets an imaginary quadratic discriminant Δ and a prime p as input and returns $t \neq 0$ if the according norm equation has an integer solution, and 0 otherwise. If $t^2 - \Delta y^2 = 4p$ has no integer solution, we turn to the norm equation $t^2 - \Delta y^2 = 4p^m$. In order to decide whether this equation has an integer solution or not, we extended the algorithm of Cornacchia to prime powers: `cornacchiaPrimePower`(Δ, p^m) gets an imaginary quadratic discriminant Δ and a prime power p^m as input. It returns $t \neq 0$ if the norm equation (1) has an integer solution, and 0 otherwise.

If we have found a prime p with an integer solution of the norm equation for p^m, but not for p, we make use of (2) to check for the conditions of section 2. Analogously to [BB00] this task is performed by the function `isStrong`(p^m, N); it returns the prime r if N turns out to be the order of a cryptographically strong elliptic curve over $\mathbb{F}_{p^m}$, and 0 otherwise. This yields our algorithm `findField`(n, m, h_0).

`findField`(n, m, h_0)

Input: A positive integer n, a prime m, such that $nm \geq 160$, and an integer $h_0 \geq 200$.
Output: A prime p of bit-length n, such that $\mathbb{F}_{p^m}$ is an Optimal Extension Field, if such a p exists.
A prime r and a discriminant Δ, such that r is the cardinality of a cryptographically strong elliptic curve defined over $\mathbb{F}_{p^m} \setminus \mathbb{F}_p$ having a maximal order of discriminant Δ as endomorphism ring with $h(\Delta) \geq h_0$.

$p \leftarrow \max\{p' \in \mathbb{Z} : p < 2^n, p' \equiv 1 \bmod m, p' \text{ prime}\}$;
if $2^n - p > \sqrt{2^n}$ **then**
  output("No OEF found. Terminating."); terminate;
$h \leftarrow \min\{h' \in \mathbb{N} : h' \geq h_0, m \mid h'\}$;
while `true` **do**
  $\Delta \leftarrow$ `nextDiscriminant`$(h, 0)$;
  while $\Delta > -6000000$ **do**
    $p \leftarrow \max\{p' \in \mathbb{N} : p' < 2^n, p' \equiv 1 \bmod m, p' \text{ prime}\}$;
    while $2^n - p < \sqrt{2^n}$ **do**
      $t \leftarrow$ `cornacchia`(Δ, p);
      if $t = 0$ **then**
        $t \leftarrow$ `cornacchiaPrimePower`(Δ, p^m);
        if $t \neq 0$ **then**
          if $(r \leftarrow$ `isStrong`$(p^m, p^m + 1 - t)) \neq 0$ AND $r = p^m + 1 - t$ **then**
            return(p, r, Δ);
          else if $(r \leftarrow$ `isStrong`$(p^m, p^m + 1 + t)) \neq 0$ AND $r = p^m + 1 + t$ **then**
            return(p, r, Δ);
      $p \leftarrow \max\{p' \in \mathbb{Z} : p' < p, p' \equiv 1 \bmod m, p' \text{ prime}\}$;
    $\Delta \leftarrow$ `nextDiscriminant`(h, Δ);
  $h \leftarrow h + m$;

Once knowing the cardinality p^m of an Optimal Extension Field, we turn to the computation of an irreducible binomial $X^m - \omega$ in $\mathbb{F}_p[X]$. Our algorithm `findBinomial`(p, m) is a straightforward consequence of theorem 1 and corollary 1.

We remark that if $X^m - \omega$ is reducible in $\mathbb{F}_p[X]$, $X^m - \omega^d$ is reducible either for all $d \in \mathbb{N}$. However, due to the simplicity of algorithm `findBinomial`(p, m) we do not take this fact into account.

Finally, we turn to algorithm `findOEFCurve`(Δ, p, r). This algorithm bases on `findCurve`(Δ, p, l) in [BB00]. The main differences come from the sub-algorithm `findRoot`. As explained above, given a root j_q of $H \bmod p$ in $\mathbb{F}_{p^m}$, `findOEFCurve`

`findBinomial`(p, m)

Input: Rational primes p and m with $p \equiv 1 \bmod m$.
Output: An irreducible binomial $X^m - \omega$ in $\mathbb{F}_p[X]$ with minimal $\omega \in \mathbb{N}$.

$\omega \leftarrow 2$;
while true **do**
  $d \leftarrow \omega^{\frac{p-1}{m}} \bmod p$;
  if $d \neq 1$ **then**
    return$(X^m - \omega)$;
  $\omega \leftarrow \omega + 1$;

`findOEFCurve`(Δ, p, r)

Input: A fundamental imaginary quadratic discriminant $\Delta \equiv 5 \bmod 8$.
  A prime power p^m such that there exists an elliptic curve of prime order r over $\mathbb{F}_{p^m}$.
Output: An elliptic curve E over $\mathbb{F}_{p^m}$ with $|E(\mathbb{F}_{p^m})| = r$ and endomorphism ring of discriminant Δ.
  A generating point G of $E(\mathbb{F}_{p^m})$.

$j_q \leftarrow$ `findRoot`(Δ, p^m);
Select a non-square $s_q \in \mathbb{F}_{p^m}$;
$E_1 \leftarrow (a_q, b_q)$; $E_2 \leftarrow (a_q s_q^2, b_q s_q^3)$; //assign curve parameters
$G_1 \in_R (E_1(\mathbb{F}_{p^m})) \setminus \{O\}$; $G_2 \in_R (E_2(\mathbb{F}_{p^m})) \setminus \{O\}$; //choose random points
if $rG_1 = O$ AND $rG_2 \neq O$ **then**
  return (E_1, G_1);
else
  return (E_2, G_2);

computes the coefficients of elliptic curves over $\mathbb{F}_{p^m}$ of order $p^m + 1 \pm t$, and it decides by trial and error, which of these curves is of order r.

We next discuss `findRoot`(Δ, p^m), i.e. the proceeding to determine a root of $H \bmod p$ in $\mathbb{F}_{p^m}$. The first step of `findRoot`(Δ, p^m) consists in determining a generating polynomial of the Hilbert class field of $\mathbb{Q}(\sqrt{\Delta})$. In the literature one finds some proposals of polynomials with rather small coefficients. If $3 \nmid \Delta$ we compute a polynomial due to Atkin and Morain (see [AM93]). To be more precise, in this case we determine the minimal polynomial of $e^{2\pi i/3} \cdot \gamma_2(\frac{\Delta+\sqrt{\Delta}}{2})$ over $\mathbb{Q}(\sqrt{\Delta})$, where γ_2 is the unique cube root of j which is real-valued on the imaginary axis. We denote this polynomial by P_γ. Let $\gamma_{2,q} \in \mathbb{F}_{p^m}$ be a root of $P_\gamma \bmod p$. Then $\gamma_{2,q}^3$ is a root of $H \bmod p$. If we have $3 \mid \Delta$, we compute the Hilbert polynomial H. For an efficient computation of P_γ or H we refer to [Bai01a].

It remains to explain how to get a root of a polynomial $P \bmod p$ that splits completely to linear factors in $\mathbb{F}_{p^m}[X]$. As in [BB00] we make use of the LiDIA-function `find_root`(p^m, P). As input this function requires a prime power p^m and a polynomial $P \in \mathbb{Z}[X]$, such that $P \bmod p$ splits into linear factors in $\mathbb{F}_{p^m}[X]$.

It returns a zero of $P \bmod p$ in $\mathbb{F}_{p^m}$. `find_root` uses the Cantor-Zassenhaus split (see [Coh95]) and a polynomial arithmetic due to Shoup [Sho95].

We finally present the main algorithm `oefCurve`. Given n, m, and h_0, `oefCurve` first invokes `findField`(n, m, h_0). Once p, r, and Δ are determined, it calls the functions `findBinomial` and `findOEFCurve`. Finally, `oefCurve` returns (p, r, f, E, G).

4 Running Times and Statistics

We implemented our algorithms in C++ using the library LiDIA 2.0 and the GNU compiler 2.95.2 setting the optimization flag -O2 and using gmp 2.0.2 as underlying multiprecision package. The timings were measured on a Pentium III running Linux 2.2.14 at 850 MHz and having 128 MB of main memory. Hence the timings may be measured on any modern personal computer either. We present some sample running times of `oefCurve`$(32, 5, h_0)$ and CPU-timings for $200 \leq h_0 \leq 250$, $10 \mid h_0$, in table 1. More timings and statistical data may be found in [Bai01b].

Table 1. Data delivered by `oefCurve`$(32, 5, h_0)$.

h_0	h	Δ	p	ω	CPU-time in seconds
200	200	-125579	4294920991	2	21.8
210	210	-265235	4294903891	7	52.8
220	220	-268931	4294931761	2	65.3
230	230	-405803	4294931071	2	64.0
240	240	-170651	4294946191	2	38.5
250	250	-254579	4294940641	3	54.6

Finally, we give some statistical data on the number of non-isomorphic elliptic curves of prime order over Optimal Extension Fields $\mathbb{F}_{p^5}$ where p is a 32-bit prime. First, we determine for each class number h with $200 \leq h \leq 400$, h divisible by 5, the number of pairs (Δ, p), where $\Delta > -6000000$ is a fundamental discriminant congruent 5 mod 8 and p a 32-bit prime, such that there exists a cryptographically strong elliptic curve of prime order r over $\mathbb{F}_{p^5}$ having an endomorphism ring of discriminant Δ. In all, there are 5579 such tuples. Furthermore, in 4563 of the cases, the according field $\mathbb{F}_{p^5}$ is a Type II OEF. Next, we determine the number of non-isomorphic elliptic curves for the tuples (Δ, p) as above. For each such tuple (Δ, p) there are $h(\Delta)$ non-isomorphic elliptic curves having the properties cited above. In all, there are 1546830 non-isomorphic curves, and 1263850 of them are defined over a Type II OEF. We deduce that, even in our special case, the set of non-isomorphic curves for use in cryptography is sufficiently large to choose from.

References

[AM93] A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computation*, 61:29–67, 1993.

[Bai01a] H. Baier. Efficient Computation of Singular Moduli with Application in Cryptography. In *Fundamentals of Computing Theory, Proceedings of FCT 2001*, LNCS 2138, pages 71–82, Berlin, 2001. Springer-Verlag.

[Bai01b] H. Baier. Elliptic Curves of Prime Order over Optimal Extension Fields for Use in Cryptography. Technical Report, Darmstadt University of Technology, 2001. Technical Report No. TI-11/01.

[BB00] H. Baier and J. Buchmann. Efficient Construction of Cryptographically Strong Elliptic Curves. In *Progress in Cryptology - INDOCRYPT2000*, LNCS 1977, pages 191–202, Berlin, 2000. Springer-Verlag.

[BP98] D. Bailey and C. Paar. Optimal Extension Fields for fast Arithmetic in Public-Key Algorithms. In *Advances in Cryptology - CRYPTO'98*, LNCS 1462, pages 472–485, Berlin, 1998. Springer-Verlag.

[BP01] D. Bailey and C. Paar. Efficient Arithmetic in Finite Field Extensions with Application in Elliptic Curve Cryptography. *Journal of Cryptology*, 2001. to appear.

[BSS99] I. Blake, G. Seroussi, and N. Smart. Elliptic Curves in Cryptography. Cambridge University Press, 1999.

[Coh95] H. Cohen. A Course in Computational Algebraic Number Theory. Springer-Verlag, 1995.

[FGH01] M. Fouquet, P. Gaudry, and R. Harley. Finding Secure Curves with the Satoh-FGH Algorithm and an Eary-Abort Strategy. In *Proceedings of Eurocrypt 2001*, LNCS 2045, pages 14–29, Berlin, 2001. Springer-Verlag.

[GHS01] P. Gaudry, F. Hess, and N.P. Smart. Constructive and descructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, 2001. to appear.

[Kob87] N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48:203–209, 1987.

[LZ94] G.-J. Lay and H.G. Zimmer. Constructing elliptic curves with given group order over large finite fields. In *Proceedings of ANTS I*, LNCS 877, pages 250–263, 1994.

[Mil86] V. Miller. Use of Elliptic Curves in Cryptography. In *Proceedings of CRYPTO '85*, LNCS 218, pages 417–426, Berlin, 1986. Springer-Verlag.

[Sho95] V. Shoup. A new polynomial factorization algorithm and its implementation. *Journal of Symbolic Computation*, 20:363–397, 1995.