Generating Anomalous Elliptic Curves

Franck Leprévost [a], Jean Monnerat [b,1], Sébastien Varrette [a], Serge Vaudenay [b]

[a] *Université du Luxembourg, LIASIT, 162 A, Avenue de la Faïencerie, L-1511 Luxembourg*

[b] *EPFL, LASEC, CH-1015 Lausanne, Switzerland*

Abstract

In 1999, Smart has shown how to solve in linear time ECDLP for elliptic curves of trace 1 defined over a prime finite field $\mathbf{F}_p$, the so-called anomalous elliptic curves. In this article, we show how to construct such cryptographically weak curves for primes p of industrial length, using complex multiplication theory.

Key words: elliptic curve, discrete logarithm problem, trace of Frobenius, complex multiplication, anomalous curve

1 Introduction

During the last decade, a considerable amount of work has been dedicated to the cryptography based on the Elliptic Curve Discrete Logarithm Problem (ECDLP). The motivation of this development is that there is no known sub-exponential algorithm which solves the ECDLP in general. The principal applications based on this problem are the cryptosystems based on the ElGamal scheme, like *e.g.* the standard signature scheme ECDSA [1].

Although the ECDLP is believed to be hard in general, it has been shown that some special curves do not possess a difficult ECDLP so that malicious parties could in principle purposely generate cryptographically weak elliptic curves. In

Email addresses: Franck.Leprevost@univ.lu (Franck Leprévost), Jean.Monnerat@epfl.ch (Jean Monnerat), Sebastien.Varrette@imag.fr (Sébastien Varrette), Serge.Vaudenay@epfl.ch (Serge Vaudenay).

[1] Supported in part by a grant of the Swiss National Science Foundation, 200021-101453/1.

1999, Smart provided a very efficient method for solving the ECDLP in linear time when the underlying elliptic curve is anomalous, i.e. when the number of rational points on $\mathbf{F}_p$ is equal to the prime number p. This corresponds to curves of trace one. In this paper, we show that checking if a given elliptic curve defined over a prime field $\mathbf{F}_p$ is anomalous or not is a crucial step, since a malicious entity can effectively generate elliptic curves of trace one efficiently.

2 The Attack of Smart

In this section, we explain the attack of Smart [9] and recall most of the required background. This is essentially a summary of [6]. Most of the results concerning elliptic curves can be also found in [8].

2.1 Some Background

In this subsection, we present some background required in order to understand the attack of Smart.

P-adic numbers. Let a be in $\mathbf{Q}$ and p be a prime integer. We can write a as $a = p^r \frac{m}{n}$, where $r \in \mathbf{N}$ and $m, n \in \mathbf{Z}$ are not multiples of p. Then, we define $\mathrm{ord}_p(a) := r$ and the norm of a nonzero a as $|a|_p := p^{-r}$. The set of p-adic numbers is defined as the completion of the rational numbers with respect to the metric d_p given by $d_p(a, b) := |a - b|_p$. Thus, every p-adic numbers can be written uniquely in the form of an infinite series $c_{-n}p^{-n} + \cdots + c_0 + c_1 p + \cdots + c_m p^m + \cdots$, where the c_i's are integers such that $0 \leq c_i \leq p - 1$. We denote the set of the p-adic numbers as $\mathbf{Q}_p$. The p-adic numbers a such that $\mathrm{ord}_p(a) \geq 0$ form the set of the p-adic integers denoted as $\mathbf{Z}_p$. More details on p-adic numbers can be found in [4].

Expansion around $\mathcal{O}$. We consider an elliptic curve E given by the Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and defined on a field K. We resume here how we can represent the rational points of E around $\mathcal{O}$ with one parameter in K. We first do the change of variables $z = -x/y$ and $w = -1/y$. The point $\mathcal{O}$ is now represented as the pair $(0, 0)$ in the (z, w)-plane. The Weierstrass equation becomes $w = z^3 + a_1zw + a_2z^2w + a_3w^2 + a_4zw^2 + a_6w^3$. By substituing this equation into itself recursively, we can represent w in a formal power series $w(z)$ in z. Hence, we get $x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3z - (a_4 + a_1a_3)z^2 - \cdots$ and $y(z) = -\frac{x(z)}{z}$. We notice that the parameter z can describe the points of this elliptic curve only when the series $x(z)$ converges. For instance, this is the case when $K = \mathbf{Q}_p$, $z \in p\mathbf{Z}_p$, and $a_1, a_2, a_3, a_4, a_6 \in \mathbf{Z}_p$. The addition law of E can be described in the coordi-

nate z with a formal power series. Hence, the addition of two points z_1 and z_2 is given by $F(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 \ldots$. In the case $K = \mathbf{Q}_p$, we define the group $\hat{E}(p\mathbf{Z}_p)$ as the set $p\mathbf{Z}_p$ with the addition law $\oplus$ induced by F, i.e. $z_1 \oplus z_2 := F(z_1, z_2)$.

Reduction modulo p. Let E be an elliptic curve defined over $\mathbf{Q}_p$ and given by a Weierstrass equation. This equation can be written with coefficients in $\mathbf{Z}_p$. If we reduce the coefficients modulo p of this equation, we get another curve defined over $\mathbf{F}_p$ denoted by $\bar{E}$, and called the reduction of E modulo p. We point out that points of E can be also reduced to points of $\bar{E}$. This is done by expressing a point of E in projective coordinates with p-adic integers such that at least one of them lies in $\mathbf{Z}_p \backslash p\mathbf{Z}_p$ and then reducing each such coordinate modulo p. Thus, we have a reduction map $E(\mathbf{Q}_p) \longrightarrow \bar{E}(\mathbf{F}_p)$ mapping a point P to its reduced point $\bar{P}$. From now on, we assume that the reduced curve $\bar{E}/\mathbf{F}_p$ is non-singular. We define $E_1(\mathbf{Q}_p) = \{P \in E(\mathbf{Q}_p) | \bar{P} = \mathcal{O}\}$. It is the set of points that reduce to the point at infinity. It can be shown that the function ϑ_p mapping from $\hat{E}(p\mathbf{Z}_p)$ to $E_1(\mathbf{Q}_p)$ and defined by $\vartheta_p(z) := \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$ is a group isomorphism. By defining for an integer $n > 0$ the subgroup $E_n(\mathbf{Q}_p) = \{P \in E(\mathbf{Q}_p) \,|\mathrm{ord}_p(x(P)) \leq -2n\} \cup \{\mathcal{O}\}$, where $x(P)$ denotes the x-coordinate of P, we can also prove that ϑ_p induces an isomorphism between $E_n(\mathbf{Q}_p)$ and $\hat{E}(p^n\mathbf{Z}_p)$, where this group is the set $p^n\mathbf{Z}_p$ with the group law defined by F.

The formal logarithm. The formal logarithm is a function allowing to transform the group $\hat{E}(p\mathbf{Z}_p)$ in the group $p\mathbf{Z}_p$ with usual addition. To this end, we have to find an ismorphism $\log_{\mathcal{F}}$ satisfying $\log_{\mathcal{F}} F(z_1, z_2) = \log_{\mathcal{F}}(z_1) + \log_{\mathcal{F}}(z_2)$ for all $z_1, z_2 \in p\mathbf{Z}_p$. This function can be expressed by a series of the form $\log_{\mathcal{F}}(T) = T + \frac{d_1}{2}T^2 + \frac{d_2}{3}T^3 + \cdots$. It can also be proved that $\log_{\mathcal{F}}$ induces an isomorphism from $\hat{E}(p^n\mathbf{Z}_p)$ to $p^n\mathbf{Z}_p$.

From the above statements, we can deduce that $E_n(\mathbf{Q}_p) \simeq p^n\mathbf{Z}_p$ since

$$\log_{\mathcal{F}} \circ \vartheta_p^{-1}(E_n(\mathbf{Q}_p)) = p^n\mathbf{Z}_p,$$

and the function $\psi_p := \log_{\mathcal{F}} \circ \vartheta_p^{-1}$ is a group isomorphism. Thus, we remark that $E_n(\mathbf{Q}_p)/E_{n+1}(\mathbf{Q}_p) \simeq p^n\mathbf{Z}_p/p^{n+1}\mathbf{Z}_p \simeq \mathbf{F}_p^+$, where $\mathbf{F}_p^+$ denotes the additive group of $\mathbf{F}_p$ i.e., $(\mathbf{Z}/p\mathbf{Z}, +)$. Furthermore, it turns out that $E(\mathbf{Q}_p)/E_1(\mathbf{Q}_p)$ is isomorphic to $\bar{E}(\mathbf{F}_p)$.

Lift of an elliptic curve. Let $\bar{E}$ be defined over $\mathbf{F}_p$. An elliptic curve E defined over $\mathbf{Q}_p$ is called a lift of $\bar{E}$ if E reduces to $\bar{E}$ modulo p. Similarly, a point $P \in E(\mathbf{Q}_p)$ is said to be a lift of a point $\bar{P} \in \bar{E}(\mathbf{F}_p)$ if it reduces to $\bar{P}$ modulo p. We immediatly observe that a lift of a given elliptic curve or of a point is not unique. One method to find a lift of a given $\bar{P} \in \bar{E}(\mathbf{F}_p)$ works as follows. We first consider E given by the same Weierstrass equation as $\bar{E}$. The x-coordinate of P is set to be equal to that of $\bar{P}$. Then, the y-coordinate

can be computed by looking at the p-adic expansion satisfying the Weierstrass equation. This can be done using a Hensel lifting. Indeed, this method allows to find successively each term of the right p-adic expansion. Indeed, if we have a solution of a polynomial equation modulo p^i, the Hensel lifting provides a method to find a solution modulo p^{i+1}.

2.2 The Attack

Let $\bar{E}$ be a non-singular elliptic curve of trace one defined over a finite field $\mathbf{F}_p$ with p prime, i.e., $\#\bar{E}(\mathbf{F}_p) = p$.

We provide now the algorithm proposed by Nigel Smart (see [9]) which allows to solve the discrete logarithm problem on such curves very rapidly. This problem can be described as following: Given two points $\bar{P}$, $\bar{Q} \in \bar{E}(\mathbf{F}_p)$ with $\bar{Q} \in \{\, [k]\,\bar{P} \mid k \in \mathbf{N}\}$ find m such that

$$\bar{Q} = [m]\,\bar{P}. \tag{1}$$

At first, we compute the lifts P, $Q \in E(\mathbf{Q}_p)$ of the points $\bar{P}$, $\bar{Q}$, using the method explained in Subsection 2.1. Since the reduction modulo p is a homomorphism and from (1), we have

$$Q - [m]\,P = R \in E_1(Q_p). \tag{2}$$

We recall from Subsection 2.1, that $\bar{E}(\mathbf{F}_p) \simeq E(\mathbf{Q}_p)/E_1(\mathbf{Q}_p)$ and also that $E_1(\mathbf{Q}_p)/E_2(\mathbf{Q}_p) \simeq \mathbf{F}_p^+$. From this fact and since $\#\bar{E}(\mathbf{F}_p) = p$, we see that the multiplication by $[p]$ maps the elements of $E(\mathbf{Q}_p)$ to $E_1(\mathbf{Q}_p)$ respectively the elements of $E_1(\mathbf{Q}_p)$ to $E_2(\mathbf{Q}_p)$. Hence, multiplying the equation (2) by p leads to

$$[p]\,Q - [m]\,([p]\,P) = [p]\,R \in E_2(\mathbf{Q}_p).$$

Since $[p]\,P$ and $[p]\,Q$ lie in $E_1(\mathbf{Q}_p)$, we can apply the isomorphism ψ_p on these elements and get

$$\psi_p\,([p]\,Q) - m\psi_p\,([p]\,P) \in p^2\mathbf{Z}_p.$$

This relation can be written as

$$c_1 \cdot p + c_2 \cdot p^2 + \cdots - m(d_1 \cdot p + d_2 \cdot p^2 + \cdots) = b_2 \cdot p^2 + \cdots,$$

where c_i's are the coefficients of the p-adic expansion of $\psi_p\,([p]\,Q)$ and d_i's are the coefficients of the p-adic expansion of $\psi_p\,([p]\,P)$. Thus, we finally obtain

$$m = \frac{\psi_p\,([p]\,Q)}{\psi_p\,([p]\,P)} \bmod p = \frac{c_1}{d_1} \bmod p.$$

In order to find m, we only need to describe how to compute $\psi_p(S)$ modulo p^2 for a point $S \in E_1(\mathbf{Q}_p)$, and apply this method to $S = [p]P$, and $S = [p]Q$. According to the definition of ϑ_p, we have

$$\vartheta_p^{-1}(S) = -\frac{x(S)}{y(S)} \in p\mathbf{Z}_p,$$

where $x(S)$, $y(S)$ denote the x-, y-coordinates of S. Hence, by definition of the formal logarithm and the definition of ψ_p, we get

$$\psi_p(S) \equiv -\frac{x(S)}{y(S)} \pmod{p^2}.$$

3 Complex Multiplication

In this section, we briefly recall the complex multiplication method (see [2] and [8]) for constructing elliptic curves with some properties.

Given a non supersingular elliptic curve E defined over a field L, its ring of endomorphisms $\mathrm{End}(E)$ is either $\mathbf{Z}$ or an order in an imaginary quadratic field. In the latter case, such an elliptic curve is said to have complex multiplication by this order.

Let τ be an element of Poincaré's upper-half plane $\mathfrak{H} = \{z = x + iy,\ x, y \in \mathbf{R},\ y > 0\}$, and $q = \exp(2i\pi\tau)$. The quantities $\Delta(\tau)$ and $j(\tau)$ are defined by:

$$\Delta(\tau) = q\prod_{n\geq 1}(1-q^n)^{24}, \qquad j(\tau) = \frac{(256\Delta(2\tau)+\Delta(\tau))^3}{\Delta^2(\tau)\Delta(2\tau)}.$$

Actually, as long as $j(\tau) \neq 0, 1728$, $j = j(\tau)$ may be seen as the modular invariant of the elliptic curve E with equation:

$$y^2 = x^3 - \frac{3j}{j-1728}x + \frac{2j}{j-1728}. \tag{3}$$

Similar formulae arise in the cases $j = 0, 1728$, cases that will not be considered here. Indeed, the above formula applies over the field of definition of $j(\tau)$. In particular, given an element j of a finite field $\mathbf{F}_p$, one can construct in this way an elliptic curve E defined over $\mathbf{F}_p$, such that its modular invariant $j_E = j$.

On the other hand, let $D > 0$ be an integer such that $-D$ is a fundamental discriminant of the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-D})$, and let d be the square-free positive integer such that $K = \mathbf{Q}(\sqrt{-d})$; in other words, if $d \equiv 3 \pmod 4$, then $D = d$, and $D = 4d$ otherwise. Let H/K be the Hilbert class

field of K, namely the maximal unramified Abelian extension of K. Its Galois group is isomorphic to the class group of K:

$$\mathrm{Gal}(H/K) \simeq \mathrm{Cl}_K.$$

Let h_D denote the class number of the field K. It turns out, that H is the decomposition field of the monic polynomial $H_D(x) \in \mathbf{Z}[x]$ of degree h_D defined by:

$$H_D(x) = \prod_{\tau \in S_D} (x - j(\tau)),$$

where

$$S_D = \Big\{ \tau = \frac{-b + \sqrt{-D}}{2a};\ b^2 - 4ac = -D,\ |b| \leq a \leq \sqrt{|D|/3},$$
$$a \leq c,\ \gcd(a,b,c) = 1 \text{ and if } |b| = a \text{ or } a = c \text{ then } b \geq 0 \Big\}.$$

The roots $j(\tau)$ of the Hilbert polynomial $H_D(x)$ are the j-invariants of elliptic curves E_τ with complex multiplication by an order in $\mathbf{Q}(\tau) = \mathbf{Q}(\sqrt{-D})$. Because $H_D(x) \in \mathbf{Z}[x]$, we show in the next section how to use most of these results also modulo p.

4 Construction of Anomalous Elliptic Curves

Now, let p be a prime number, and let E be an elliptic curve defined over $\mathbf{F}_p$. Its number of $\mathbf{F}_p$-rational points is:

$$\#E(\mathbf{F}_p) = p + 1 - t,$$

where $t = \alpha + \overline{\alpha}$ is the trace of the Frobenius endomorphism, and α is an element of K of norm p. If E is defined by the equation $y^2 = x^3 + ax + b$, and if u is any non-quadratic residue modulo p, then the quadratic twist $\tilde{E}$ of the elliptic curve E is defined by the equation (independant of the choice of u)

$$uy^2 = x^3 + ax + b. \tag{4}$$

The j-invariant of E equals the j-invariant of $\tilde{E}$. Moreover, the number of $\mathbf{F}_p$-rational points of E and of $\tilde{E}$ are related by

$$\#E(\mathbf{F}_p) + \#\tilde{E}(\mathbf{F}_p) = 2p + 2.$$

If furthermore the prime number p satisfies the condition:

$$4p = x^2 + Dy^2,$$

for some integers x, y, and if E has furthermore complex multiplication by an order of discriminant $-D$, then $\alpha = \pm(x + y\sqrt{-D})/2$, and $t = \pm x$. Therefore, the numbers $p + 1 \pm x$ will be the orders of E, and of its quadratic twist $\tilde{E}$ over $\mathbf{F}_p$. In particular, if $x = 1$, then the order of E (resp. of $\tilde{E}$) over $\mathbf{F}_p$ is equal to p or $p + 2$ (resp. $p + 2$ or p).

Case $h_D = 1$. So, our strategy to construct elliptic curves E defined over $\mathbf{F}_p$ such that $\#E(\mathbf{F}_p) = p$ will be first to look for values of D such that the degree h_D of the Hilbert polynomial $H_D(x)$ is equal to 1. If p is a prime number such that $4p = 1 + Dy^2$, then the root of $H_D(x) = x - j_D$, obviously rational over $\mathbf{F}_p$, is the j-invariant of an elliptic curve E defined over $\mathbf{F}_p$, and of its quadratic twist $\tilde{E}$. The equations of these curves are obtained, thanks to the equations (3) and (4), and one of these two elliptic curves is anomalous over $\mathbf{F}_p$. We further focus here on elliptic curves with complex multiplication by the principal order of an imaginary quadratic number field. These conditions lead to the values of d, D and of j_D stated in the following table (see *e.g.* [7]):

d	D	j_D
1	4	$2^6.3^3$
2	8	$2^6.5^3$
3	3	0
7	7	$-3^3.5^3$
11	11	-2^{15}
19	19	$-2^{15}.3^3$
43	43	$-2^{18}.3^3.5^3$
67	67	$-2^{15}.3^3.5^3.11^3$
163	163	$-2^{18}.3^3.5^3.23^3.29^3$

We then look for prime numbers of fixed length k (say $k = 160$ bits) satisfying

$$4p = 1 + Dy^2.$$

Some values of D listed in the table are not convenient for our purpose. Indeed, we want to construct elliptic curves with coefficients of length k. This means that the values $d = 1, 2$, and 3, corresponding to small values $j_D \geq 0$ have to be excluded. Moreover, one easily checks that the conditions on p require that $D \equiv 3 \mod 8$, and the value $D = 7$ is also excluded. In other words, one looks for prime numbers p of the form given in the following table, where m is an integer such that p is of length k:

$D = 11$	$p = 11m(m+1) + 3$
$D = 19$	$p = 19m(m+1) + 5$
$D = 43$	$p = 43m(m+1) + 11$
$D = 67$	$p = 67m(m+1) + 17$
$D = 163$	$p = 163m(m+1) + 41$

Computation shows that there are many such prime numbers of length k of this form. Then, using Section 3, we compute a curve E over $\mathbf{F}_p$ with modular invariant j_D. This curve is provided by the reduction modulo p of the equation (3), with $j = j_D$. To decide which one between the two curves E or $\tilde{E}$ is anomalous, one simply takes a point $P \in E(\mathbf{F}_p) - \{\mathcal{O}\}$ at random, and checks if $[p]P = \mathcal{O}$. If this is the case, E is anomalous, and $\#\tilde{E}(\mathbf{F}_p) = p + 2$. Otherwise, we change E into its quadratic twist $\tilde{E}$. To illustrate the first issue over $\mathbf{F}_p$, where p is a prime number of length 160 bits, we outline an example (obtained using the Magma package) in the case $D = 11$, and $j_{11} = -2^{15}$.

Example 1. For $m = 257743850762632419871495$, $p = 11m(m+1) + 3$ is a prime number of length 160 bits. Then, the elliptic curve E over $\mathbf{F}_p$ is defined by the equation $y^2 = x^3 + \mu x + \nu$, where

$$\mu = 257064138422110541027002381641335383021691764 74,$$

and

$$\nu = 203362936548826936673264444982866339953265530166,$$

and one checks that $E(\mathbf{F}_p) = p$, and the curve E is anomalous over $\mathbf{F}_p$. Now, if

$$P = (25, 373046486843468839388624733545540314758667830 37) \in E(\mathbf{F}_p)$$

and

$$Q = (20, 157931136836524102701922129702410179003466984543) \in E(\mathbf{F}_p),$$

the method shows that $Q = nP$, with

$$n = 210393287966660756596132643172172640405085536179.$$

In this example, it was enough to use a routine written in Maple in order to recover the discrete logarithm in a few seconds on a 1.5 GHz Pentium 4.

Case $h_D \geq 2$. It is of course possible to consider other values of D for which the degree h_D of the Hilbert polynomial is ≥ 2. However, the equations of the curves E and $\tilde{E}$ we are looking for are obtained by (3) and (4); in particular,

they are defined over $\mathbf{F}_p(j)$, where j is a root of $H_D(x)$. It turns out, that such a root is defined over $\mathbf{F}_p$: Let $D > 0$ a square-free integer such that $D \equiv 3 \mod 8$. Let p be a prime number such that $4p = 1 + Dy^2$ for an integer y. Then the Hilbert polynomial $H_D(x)$ is completely split over $\mathbf{F}_p$:

$$H_D(x) \equiv \prod_{i=1}^{h_D}(x - j_i) \mod p, \text{ with } j_i \in \mathbf{F}_p.$$

This is a consequence of class field theory. We provide here a simple proof in the case $h_D = 2$ (the case $h_D = 1$ is obvious). The condition $D \equiv 3 \mod 8$ requires that D and $H_D(x)$ are as in the following table (see [3] and [5]) :

D	$H_D(x)$
35	$x^2 + 117964800x - 134217728000$
51	$x^2 + 5541101568x + 6262062317568$
91	$x^2 + 10359073013760x - 3845689020776448$
115	$x^2 + 427864611225600x + 130231327260672000$
123	$x^2 + 1354146840576000x + 148809594175488000000$
187	$x^2 + 4545336381788160000x - 3845689020776448000000$
235	$x^2 + 823177419449425920000x + 1194662117046272340787200$
267	$x^2 + 19683091854079488000000x + 5314296626726213768970240000000$
403	$x^2 + 24528113892293313919795200000x - 10884420340249105583308800000$
427	$x^2 + 15611455512523783919812608000x + 1550417562226189165469368320000000$

In case $D = 35$, the discriminant of $H_D(x)$ is $\Delta = 2^{32}.5^3.7^2.23^2$. On the other hand, if p is a prime number not dividing Δ, and such that $4p = 1 + 35y^2$, then, if $y = 2m+1$, one has $p = 9+35m(m+1)$. Finally, thanks the quadratic reciprocity law, one shows that 5 is a square mod p, and hence that Δ is also a square mod p. Thus, $H_D(x)$ is completely split over $\mathbf{F}_p$. The proof for the other values of D in the table is straightforward.

Finally, each odd prime p is such that $4p = 1 + Dy^2$ for an integer y, and a non-negative integer $D \equiv 3 \mod 8$. One recovers h_D j-invariant values defined over $\mathbf{F}_p$, to which one can associate anomalous elliptic curves over $\mathbf{F}_p$ with the formulae (3) and (4), in a similar way as we did in the case $h_D = 1$.

References

[1] ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), American National Standard Institute, American Bankers Association, 1998.

[2] I. Blake, G. Seroussi, N. Smart, *Elliptic curves in cryptography*, London Mathematical Society, LNS **265**, Cambridge University Press, 1999.

[3] Kant web page: http://www.math.tu-berlin.de/~kant

[4] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, 1984.

[5] Magma web page: http://magma.maths.usyd.edu.au

[6] J. Monnerat, *Computation of the discrete logarithm on elliptic curves of trace one - Tutorial*, Technical report IC 200249, EPFL, 2002. `http://lasecwww.epfl.ch`

[7] J.-P. Serre *Complex Multiplication*, in *Algebraic Number Theory*, Academic Press, 1967.

[8] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer GTM **106**, 1992.

[9] N. P. Smart, *The Discrete Logarithm Problem on Elliptic Curves of Trace One*, Journal of Cryptology (**1999**) 12: 193-196.