In W. Fumy, editor, *Advances in Cryptology - EUROCRYPT '97: International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, May 1997. Proceedings*, volume 1233 of *Lecture Notes in Computer Science*, pages 379–392. Springer Berlin / Heidelberg, May 1997.

Finding Good Random Elliptic Curves for Cryptosystems Defined over $\mathbb{F}_{2^n}$

Reynald Lercier

CELAR/CASSI, Route de Laillé, F-35170 Bruz, FRANCE
email: `lercier@lix.polytechnique.fr`

Abstract. One of the main difficulties for implementing cryptographic schemes based on elliptic curves defined over finite fields is the necessary computation of the cardinality of these curves. In the case of finite fields $\mathbb{F}_{2^n}$, recent theoretical breakthroughs yield a significant speed up of the computations. Once described some of these ideas in the first part of this paper, we show that our current implementation runs from 2 up to 10 times faster than what was done previously. In the second part, we exhibit a slight change of Schoof's algorithm to choose curves with a number of points "nearly" prime and so construct cryptosystems based on random elliptic curves instead of specific curves as it used to be.

1 Introduction

It is well known that the discrete logarithm problem is hard on elliptic curves defined over finite fields $\mathbb{F}_q$. This is due to the fact that the only known attacks (baby steps giant steps [39], Pollard ρ [35] and Pohlig-Hellman [34] methods) are still exponential in $\log q$. So, cryptosystems based on this problem can reach the same level of security as non elliptic versions with slightly higher computation rates and much smaller keys [38, 11].

The remaining difficulty to design elliptic cryptosystems is the computation of the cardinality of elliptic curves. Until recently, it was usually admitted that the cost needed to perform this task was too high for randomly chosen curves. To tackle this difficulty, one used to consider specific curves, for instance, supersingular curves [27, 14, 13, 1, 24] or curves with complex multiplication [31, 16, 28, 29, 17, 4]. Unfortunately, supersingular curves turned out to be disastrous and so, the use of specific curves seems to be quite compromised for cryptographical purposes [23].

Thanks to recent theoretical as well as practical developments, the cost of computing the number of points on a randomly chosen curve is no longer prohibitive. For finite fields of characteristic two (specially attractive for industrial applications), the improvements of Schoof's algorithm due to Atkin, Elkies, Morain, Couveignes, Müller, Dewaghe,... [36, 10, 33, 37, 9] were significantly speeded up by replacing the isogeny computation algorithm of Couveignes [6] with a recent heuristic algorithm of the author [19].

In this article, once briefly recalled some basic facts about elliptic curves in Section 2, we describe in Section 3 our current implementation of these ideas and we explain in Section 4 how we can take advantage of Schoof's algorithm for speeding up the search of an elliptic curve with a nearly prime number of points. Among others, it turns out that we are now able to compute the cardinality of any elliptic curve for sizes of finite fields recommended for cryptographical schemes in only a few seconds, that is to say a speed up factor from 2 up to 10 compared to our previous implementation [21].

2 Elliptic Curves over $\mathbb{F}_{2^n}$

Following [25], we consider for our purposes elliptic curves over $\mathbb{F}_{2^n}$ defined by

$$E_a : y^2 + xy = x^3 + a,\ a \in \mathbb{F}_{2^n}^*. \tag{1}$$

Any non supersingular elliptic curve is isomorphic to a curve or the twist of a curve defined by this equation. Invariant J_a and discriminant Δ_a of E_a are equal to

$$J_a = 1/a \text{ and } \Delta_a = a.$$

Let us note that E_a can not be supersingular because, in $\mathbb{F}_{2^n}$, an elliptic curve is supersingular if and only if its invariant is equal to 0 (on the explicit determination of supersingular curves in finite fields of odd characteristic, see [32]).

The set of points of E_a over $\mathbb{F}_{2^n}$ is

$$E_a(\mathbb{F}_{2^n}) = \{O_{E_a}\} \cup \left\{(x,y) \in \mathbb{F}_{2^n}^2, y^2 + xy = x^3 + a\right\}.$$

This set is a finite group and the formulae of the abelian group law are:

- $\forall P = (x_P, y_P) \in E_a(\mathbb{F}_{2^n})$, $P + O_{E_a} = O_{E_a} + P = P$, $-P = (x_P, y_P + x_P)$;
- if $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, $P \neq -Q$, then, if $P = Q$, let $\lambda = x_P + y_P/x_P$, otherwise let $\lambda = (y_Q + y_P)/(x_Q + x_P)$, and $R = P + Q = (x_{P+Q}, y_{P+Q})$ is obtained by

$$\begin{cases} x_{P+Q} = \lambda^2 + \lambda + x_P + x_Q, \\ y_{P+Q} = \lambda(x_P + x_{P+Q}) + x_{P+Q} + y_P. \end{cases}$$

Some endomorphisms will be of special interest in Section 3, namely $[m]_a$, multiplication by any integer m on E_a and ϕ_a, the Frobenius map. These endomorphisms are defined as follows.

$$[m]_a : \begin{array}{rcl} E_a(\overline{\mathbb{F}}_{2^n}) & \longrightarrow & E_a(\overline{\mathbb{F}}_{2^n}), \\ (x,y) & \longmapsto & m(x,y), \end{array} \text{ and } \phi_a : \begin{array}{rcl} E_a(\overline{\mathbb{F}}_{2^n}) & \longrightarrow & E_a(\overline{\mathbb{F}}_{2^n}), \\ (x,y) & \longmapsto & (x^{2^n}, y^{2^n}). \end{array}$$

In particular, multiplication by 2 is given by

$$[2]_a : \begin{array}{rcl} E_a(\overline{\mathbb{F}}_{2^n}) & \longrightarrow & E_a(\overline{\mathbb{F}}_{2^n}), \\ (x,y) & \longmapsto & \left(x^2 + \dfrac{a}{x^2}, \left(x + \dfrac{y}{x}\right)\left(x^2 + \dfrac{a}{x^2}\right) + \dfrac{a}{x^2}\right). \end{array} \tag{2}$$

Equation (2) shows that there exists a single point $P_a = (0, \sqrt{a})$ of order 2 on these curves and the formulae of the translation by P_a are

$$T_a : \begin{array}{rcl} E_a(\overline{\mathbb{F}}_{2^n}) & \longrightarrow & E_a(\overline{\mathbb{F}}_{2^n}), \\ P = (x,y) & \longmapsto & P + P_a = \left(\dfrac{\sqrt{a}}{x}, \sqrt{a} + \dfrac{\sqrt{a}}{x} + \dfrac{a}{x^2} + \sqrt{a}\dfrac{y}{x^2}\right). \end{array}$$

3 Counting Points on Elliptic Curves

The number of points of a *non supersingular* elliptic curve E_a defined over $\mathbb{F}_{2^n}$ satisfies Hasse's inequality [40],

$$\#E_a(\mathbb{F}_{2^n}) = 2^n + 1 - t, \text{ with } |t| < 2\sqrt{2^n}. \tag{3}$$

Before 1985, the only known methods to compute this number consisted in testing all the possible integers t in Equation (3) with baby steps giant steps variants [39]. The complexity of these algorithms is asymptotically $O(2^{n/4})$. With the work by Schoof [36] and the numerous improvements that followed, it is now possible to compute this cardinality with a probabilistic complexity asymptotically equal to $O(n^6)$. We briefly describe this method in Section 3.1.

The heart of these algorithms is the computation of isogenies. In practice, the most efficient method to do that in $\mathbb{F}_{2^n}$ seems to be a heuristic algorithm due to the author [19] and we overview it in Section 3.2. Thanks to this algorithm, first, we were able to speed up our previous implementation [21] by a significant factor and secondly, compute the cardinality of an elliptic curve defined over $\mathbb{F}_{2^{1301}}$.

3.1 The Schoof-Elkies-Atkin Algorithm

The characteristic equation satisfied by the Frobenius map ϕ_a is

$$\phi_a^2 - [t]_a \circ \phi_a + [2^n]_a = 0, \tag{4}$$

where $2^n + 1 - t$ is the cardinality of $E_a(\mathbb{F}_{2^n})$. First, Schoof remarked, that once restricted to the ℓ^2 points of the kernel $E_a[\ell]$ of the multiplication $[\ell]_a$ (ℓ an odd prime), Equation (4) yields

$$\phi^2_{E_a[\ell]} + [2^n \bmod \ell]_{E_a[\ell]} = [t \bmod \ell]_{E_a[\ell]} \circ \phi_{E_a[\ell]}. \tag{5}$$

Schoof's algorithm simply consists in computing left hand side of Equation (5) for a point P of $E_a[\ell]$ and then in computing $[k]_a\phi_a(P)$ for k in $0, \ldots, \ell - 1$. When Equation (5) is satisfied for such an integer k, we have $t \bmod \ell = k$ and when $t \bmod \ell$ is known for enough primes ℓ, that is to say

$$\prod \ell \geq 4\sqrt{2^n},$$

we deduce t by using the Chinese Remainder Theorem.

The main drawback of this method is that we are virtually forced to work not only with one point P of $E_a[\ell]$, but with all the points of $E_a[\ell]$ because the x-coordinates of these points are basically defined in an extension of degree $(\ell^2 - 1)/2$ of $\mathbb{F}_{2^n}$.

Works by Atkin and Elkies improved largely this situation by noticing that, for half the primes ℓ (called Elkies primes), $E_a[\ell]$ contains at least one subgroup of ℓ points. Thus, x-coordinates of these points are defined in an extension of degree $(\ell - 1)/2$ of $\mathbb{F}_{2^n}$. Indeed, this subgroup is the kernel of an isogeny (morphism) I between the curve E_a and an isogenous curve E_b and, when such an isogeny exists, there exists another isogeny $\hat{I}$ from E_b to E_a (called the dual isogeny) such that $\hat{I} \circ I = [\ell]_a$. Therefore, $\mathrm{Ker} I \subset \mathrm{Ker}[\ell]_a$.

Elkies and Atkin gave a construction based on modular equations to obtain E_b for Elkies primes ℓ. This works in any finite field. Unfortunately, the nice analytical method that they proposed for computing explicitly the isogeny between E_a and E_b is only valid in finite fields of large characteristic [37].

3.2 Isogenies between Elliptic Curves in $\mathbb{F}_{2^n}$.

Since the original method by Atkin and Elkies for computing isogenies between two elliptic curves E_a and E_b does not work in finite fields of small characteristic p [37], only Schoof's algorithm was available during a while to count points [26]. Fortunately, the situation evolved quickly.

Known Algorithms. The first attempt to fill this gap is due to Couveignes [6]. The computations take place in the formal group defined by E_a. The algorithm was successfully implemented by Morain and the author [22] and we do not describe it here.

But the time needed to compute isogenies with this method turned out to be the major cost while counting points. We recently proposed another algorithm which performs much better in practice. It is specially designed for the characteristic two case and is only based on algebraic properties [19].

Let us note that Couveignes proposed a third algorithm for finite fields of small characteristic p based on algebraic properties too. It consists in computing $E_a[p^k]$ and $E_b[p^k]$ and then, uses the fact that $I(E_a[p^k]) = E_b[p^k]$. But since the computations take place in extension of degree $p^i(p-1)/2 \simeq 2\ell$, it does not seem obvious to implement it efficiently in practice even if its asymptotical complexity is attractive [7, 8].

Lercier's Approach. In finite fields of characteristic two, we exploited that there exists a unique point P_a of order 2 on E_a. Thus, an isogeny I must satisfy

$$I \circ T_a = T_b \circ I.$$

From this, we deduced the following characterization.

Theorem 1. *Let E_a and E_b be two elliptic curves defined over $\mathbb{F}_{2^n}$. Let ℓ be an odd integer, and $d = (\ell - 1)/2$. Let $\mathcal{I}$ be an isogeny of degree ℓ between E_a and E_b given by $(X, Y) \mapsto \left(\frac{G(X)}{Q^2(X)}, \frac{H(X)+YK(X)}{Q^3(X)}\right)$*

where $Q(X), G(X), H(X), K(X)$ in $\mathbb{F}_{2^n}[X]$ with degrees at most d, ℓ, $3d$ and $2d$. Then $G(X) = XP^2(X)$ where $P(X)$ is a polynomial of degree d such that $\gcd(P(X), Q(X)) = 1$ and

$$X^d Q(\sqrt{a}/X) = \frac{\sqrt[8]{a}}{\sqrt[8]{b}} \left(\sqrt[4]{a}\right)^d P(X),$$

or equivalently via $X \to \sqrt{a}/X$,

$$X^d P(\sqrt{a}/X) = \frac{\sqrt[8]{b}}{\sqrt[8]{a}} \left(\sqrt[4]{a}\right)^d Q(X). \tag{6}$$

In order to explicitly compute the isogeny I, it turns out that we have to find conditions satisfied by the polynomial $Q(X)$. This is achieved from the fact that $I \circ [2]_a = [2]_b \circ I$.

Corollary 1. *With the notations of theorem 1, polynomials $P(X)$ and $Q(X)$ must satisfy*

$$X^d \widehat{Q}(X + \sqrt{a}/X) = Q(X)P(X), \tag{7}$$

and

$$\left(X + \sqrt[4]{a}\right) X^d \widehat{P}\left(X + \sqrt{a}/X\right) = XP^2(X) + \sqrt[4]{b}Q^2(X), \tag{8}$$

where $\widehat{P}(X) = \sqrt{P(X^2)}$ and $\widehat{Q}(X) = \sqrt{Q(X^2)}$ (polynomials whose coefficients are square roots of coefficients of $P(X)$ and $Q(X)$).

Even if Equation (8) is a linear equation satisfied by $Q(X)$ over $\mathbb{F}_2$, asymptotic complexity to inverse this system is $O(\ell^3 n)$. This is too high in practice.

To decrease this complexity, we considered Equation (7) and replaced the resolution of this linear system over $\mathbb{F}_{2^n}$ by a quadratic system over $\mathbb{F}_2$. This yields an algorithm (we do not describe here) whose heuristic complexity is $O(\ell^3)$.

3.3 Results

We had an old implementation of the `SEA` (Schoof, Elkies, Atkin) algorithm including Couveignes's first algorithm to compute isogenies and using an "ad hoc" C arithmetic of $\mathbb{F}_{2^n}$ [21]. We completely rewrote it with our approach and the formalism of `ZEN` library [2, 3] which enables us to handle any finite field given recursively by a polynomial basis over a subfield (for instance, $\mathbb{F}_2$). Since we restrict ourselves to the case of the characteristic two in this article, we only give accurate timings for finite fields $\mathbb{F}_{2^n}$, even if this implementation allows us to compute the number of points of an elliptic curve defined over other finite fields [20].

$\mathbb{F}_{2^{65}}$	min	max	avg	$\mathbb{F}_{2^{89}}$	min	max	avg	$\mathbb{F}_{2^{105}}$	min	max	avg
$\ell_{\max}$	31	31	31	$\ell_{\max}$	41	43	41	$\ell_{\max}$	47	47	47
$\#U$	1	3	2	$\#U$	1	5	2	$\#U$	1	5	2
$\#L$	8	10	9	$\#L$	8	12	10	$\#L$	10	14	12
$\#M$	10^3	10^6	$3{\cdot}10^5$	$\#M$	$3{\cdot}10^3$	$3{\cdot}10^8$	$3{\cdot}10^7$	$\#M$	$6{\cdot}10^5$	$6{\cdot}10^9$	$5{\cdot}10^8$
X^{2^n}	2.8	2.9	2.9	X^{2^n}	7.3	9.5	7.5	X^{2^n}	15	16.5	15.7
$X^{2^{nr}}$	0.7	2.4	1.8	$X^{2^{nr}}$	3.5	6.8	5.1	$X^{2^{nr}}$	6.4	12.2	8.9
Schoof	0	0	0	Schoof	0	0	0	Schoof	0	0	0
g	0	0	0	g	0	0	0	g	0	0	0
k	0	0	0	k	0	0	0	k	0	0	0
M − S	0.3	1.1	0.7	M − S	0.4	5.8	2.2	M − S	1.5	30.1	6.5
Total	4.2	6.1	5.4	Total	11.4	18.9	14.9	Total	24.9	53.3	31.1

Table 1. Statistics obtained with our first implementation for small finite fields $\mathbb{F}_{2^n}$.

All the timings (in seconds) are obtained on a DEC Alpha workstation 250 (266 MHz, 4th generation). First, we did the same benchmarks as in [21]. That is to say, we measured the running times for 50 random curves $y^2 + xy = x^3 + a$ where $a \in \mathbb{F}_2[T]$ defined over $\mathbb{F}_{2^{65}} \simeq \mathbb{F}_2[T]/(T^{65} + T^4 + T^3 + T + 1)$, $\mathbb{F}_{2^{89}} \simeq \mathbb{F}_2[T]/(T^{89} + T^6 + T^5 + T^3 + 1)$ and $\mathbb{F}_{2^{105}} \simeq \mathbb{F}_2[T]/(T^{105} + T^4 + 1)$ with the so-called "dynamic strategy". Results are given in Table 2. For the sake of comparison, we also give statistics obtained with our previous implementation on this machine in Table 1.

$\mathbb{F}_{2^{65}}$	min	max	avg	$\mathbb{F}_{2^{89}}$	min	max	avg	$\mathbb{F}_{2^{105}}$	min	max	avg
$\ell_{\max}$	31	31	31	$\ell_{\max}$	41	41	41	$\ell_{\max}$	41	47	42
$\#U$	0	5	1	$\#U$	0	4	2	$\#U$	1	6	3
$\#L$	6	11	10	$\#L$	9	13	11	$\#L$	8	13	10
$\#M$	10^3	$3{\cdot}10^6$	$2{\cdot}10^5$	$\#M$	$6{\cdot}10^3$	$8{\cdot}10^7$	$6{\cdot}10^6$	$\#M$	$5{\cdot}10^3$	$2{\cdot}10^8$	10^7
X^{2^n}	2.2	4.2	3.3	X^{2^n}	5.1	7.8	6.4	X^{2^n}	6.6	11.5	8.8
$X^{2^{nr}}$	$0,3$	0.9	0.6	$X^{2^{nr}}$	0.8	2.6	1.9	$X^{2^{nr}}$	1.0	3.8	2.6
Schoof	0	0	0	Schoof	0	0.4	0	Schoof	0	3.8	0.3
g	0	0	0	g	0	0.2	0	g	0	1.7	0.5
k	0	0	0	k	0.2	0.8	0.6	k	0.8	3.8	2.4
M − S	0.6	1.5	1.0	M − S	1.1	5.2	2.2	M − S	1.1	9.8	2.9
Total	3.8	5.9	4.9	Total	9.2	14.6	11.2	Total	13.4	24.5	17.3

Table 2. Statistics for small finite fields $\mathbb{F}_{2^n}$.

We give: ℓ_{max}, the maximal prime used; the number of U (resp. L) primes; $\#M$, the number of combinations; the cumulated time for X^{2^n}, $X^{2^{nr}}$, Schoof's algorithm; computing isogenies (g_ℓ) and $t \bmod \ell$ when ℓ is Elkies (k); the time for the match and sort program; the total time. For each category, minimal, maximal and average values are given.

Since for these "small" finite fields, the time needed to compute isogenies is negligible, we only gain a speed up factor from 1.1 up to 1.8 thanks in part to the arithmetic of ZEN which is faster than the arithmetic of our old implementation. We did the same experiments for three larger finite fields, $\mathbb{F}_{2^{155}} \simeq \mathbb{F}_2[T]/(T^{155}+T^7+T^5+T^4+1)$, $\mathbb{F}_{2^{196}} \simeq \mathbb{F}_2[T]/(T^{196}+T^3+1)$ and $\mathbb{F}_{2^{300}} \simeq \mathbb{F}_2[T]/(T^{300}+T^5+1)$ (note that our previous implementation is really too slow to provide similar statistics). Results are given in Table 3.

$\mathbb{F}_{2^{155}}$	min	max	avg	$\mathbb{F}_{2^{196}}$	min	max	avg	$\mathbb{F}_{2^{300}}$	min	max	avg
$\ell_{\max}$	59	71	60	$\ell_{\max}$	73	79	74	$\ell_{\max}$	97	157	113
$\#U$	4	11	7	$\#U$	7	13	10	$\#U$	11	19	16
$\#L$	7	15	10	$\#L$	8	15	11	$\#L$	9	20	14
$\#M$	$3{\cdot}10^4$	$7{\cdot}10^8$	$7{\cdot}10^7$	$\#M$	10^5	$7{\cdot}10^9$	$8{\cdot}10^8$	$\#M$	$5{\cdot}10^6$	$5{\cdot}10^{11}$	$5{\cdot}10^{10}$
X^{2^n}	30.4	56.1	40.6	X^{2^n}	113	475	147	X^{2^n}	744	1761	996
$X^{2^{nr}}$	4.4	13.9	7.8	$X^{2^{nr}}$	8.8	31.8	21.6	$X^{2^{nr}}$	46	387	119
Schoof	0	14.8	4.3	Schoof	0	55.5	17.9	Schoof	0	551	199
g	1.5	21.6	7.1	g	9.9	419	40.6	g	76	568	287
k	7.4	31.9	20.1	k	29.2	90.1	58.9	k	354	961	601
M − S	2.9	20.4	6.5	M − S	5	86.9	22.9	M − S	14	1510	230
Total	58.8	132	86.5	Total	212	1029	308	Total	1519	3686	2434

Table 3. Statistics for larger finite fields $\mathbb{F}_{2^n}$.

At this point, the advantage of our approach clearly appears. The time needed to compute isogenies is (completely) negligible while it used to be the main cost in [21] and we gain a speed up factor from 4 up to 10 on the whole computation.

To compare Couveignes's and Lercier's approaches for two huge finite fields, we collected the same data in Table 4 for the curve

$$E_X : y^2 + xy = x^3 + T^{16} + T^{14} + T^{13} + T^9 + T^8 + T^7 + T^6 + T^5 + T^4 + T^3.$$

For the first finite field, $\mathbb{F}_{2^{1009}} \simeq \mathbb{F}_2[T]/(T^{1009} + T^{11} + T^4 + T^2 + 1)$, we first used Couveignes's and Lercier's algorithms (respectively noted JMC and RL). For the second field, $\mathbb{F}_{2^{1301}} \simeq \mathbb{F}_2[T]/(T^{1301} + T^{11} + T^{10} + T + 1)$, we could only use Lercier's (the current record, as of February 1997). The results are striking, the time needed to compute isogenies is completely negligible in the case of $\mathbb{F}_{2^{1301}}$ (3 days) while it was the main cost for $\mathbb{F}_{2^{1009}}$ (77 days).

	X^{2^n}	$X^{2^{nr}}$	Schoof	g	k	M − S	Total
$\mathbb{F}_{2^{1009}}$ (JMC)	15d 3h	2d 21h	10d 14h	77d 21h	23d 3h	1h	121d 15h
$\mathbb{F}_{2^{1009}}$ (RL)	9d 16h	1d 9h	2h	1d 2h	7d 7h	2h	19d 11h
$\mathbb{F}_{2^{1301}}$ (RL)	51d 7h	8d 12h	2d 8h	3d 17h	36d 14h	2h	103d 5h

	$\ell_{\max}$	$\#U$	$\#L$	$\#M$
$\mathbb{F}_{2^{1009}}$ (JMC)	577	57	46	$4{\cdot}10^9$
$\mathbb{F}_{2^{1009}}$ (RL)	547	48	47	$2{\cdot}10^{10}$
$\mathbb{F}_{2^{1301}}$ (RL)	673	88	50	$9{\cdot}10^{10}$

Table 4. Timings for huge finite fields (days/hours).

To improve the `SEA` algorithm, future implementation should now optimize computations of $X^{2^n} \bmod \Phi$.

4 Finding Random Elliptic Curves with Nearly Prime Cardinality Efficiently.

Since the best known attacks against the discrete logarithm problem on elliptic curves are

1. the Weil pairing reduction for supersingular curves,
2. the baby steps giant steps, Pollard-ρ and Pohlig Helman algorithms for other curves,

"good curves" for cryptographical purposes only have to be defined in a not too small finite field and to be of "nearly prime" cardinality (to avoid point 2.) different from 2^n, $2^n + 1 \pm \sqrt{2^n}$, $2^n + 1 \pm \sqrt{2^{n+1}}$ and $2^n + 1 \pm 2\sqrt{2^n}$ (to avoid point 1.) if defined over $\mathbb{F}_{2^n}$.

In Section 4.1, we describe an early abort strategy suggested by Morain that takes advantage of the `SEA` algorithm to quickly throw away most of the curves which do not meet this condition. For convenience, we explain it only in the case of elliptic curves E_a defined over $\mathbb{F}_{2^n}$. But this strategy obviously works in any finite field. Then we give timing and examples of "good curves" provided by this strategy.

4.1 Early Abort Strategy

The Algorithm. An elliptic curve E_a given by Equation (1) is non supersingular and has a point $Q_a = (\sqrt[4]{a}, \sqrt{a})$ of order 4. Thus, the previous condition can be reformulated as follows : "A good curve E_a is a curve defined over $\mathbb{F}_{2^n}$ with $n \geq 60$ whose cardinality is 4 times a prime".

To find such "good curves", we proceed as follows:

1. Choose an element $a \in \mathbb{F}_{2^n}^*$ at random.
2. As explained in Section 3, compute $t \bmod \ell$ with the `SEA` algorithm checking during the computation that, for each Elkies prime $\ell \neq 2$,
$$2^n + 1 - t \bmod \ell \neq 0.$$
Otherwise, this means that the number of points of the curve is divisible by ℓ. In this case, go to step 1.
3. Check that the cardinality of the curve is 4 times a prime, otherwise go to step 1.

First of all, let us note that when $2^n + 1 - t \bmod \ell = 0$ for a prime ℓ, this means there is a point of order ℓ in E_a. Therefore, there exists an isogeny of degree ℓ defined from E_a, and ℓ is necessarily an Elkies prime.

Let us observe too that it is better to test the primality of the cardinality at step 3., first, by a pseudo primality test, and then by an exact primality prover (for instance ECPP [30]). But for practical reasons, we used MAPLE system [5].

In practice, this algorithm works well because most of the time a curve does not have a prime cardinality, we will see in Section 4.1 that this cardinality is divided by a small integer. Since we choose primes ℓ as small as possible in the `SEA` algorithm, we detect such a curve quickly.

Analysis. A theorem by Howe [12], which extends works by Lenstra [18] (see also [15]), gives the asymptotic behavior of the probability that a random elliptic curve over a finite field $\mathbb{F}_q$ has ℓ^k $(k \in \mathbb{N}^*)$ dividing the number M of its points when $q \to \infty$.

Theorem 2. *There is a constant $C \leq 1/12 + 5\sqrt{2}/6 \simeq 1.262$ such that the following statement is true. Given a prime power q, let r be the multiplicative arithmetic function such that for all primes ℓ and positive integers k*

$$r_q(\ell^k) = \begin{cases} \dfrac{1}{\ell^{k-1}(\ell-1)} & \textit{if } q \neq 1 \bmod \ell^\mu, \\ \dfrac{\ell^{\nu+1} + \ell^\nu - 1}{\ell^{\nu+\mu-1}(\ell^2-1)} & \textit{if } q = 1 \bmod \ell^\mu, \end{cases}$$

where $\mu = \lceil k/2 \rceil$ and $\nu = \lfloor k/2 \rfloor$. Then for all positive integers N, the probability $\pi_{q,N}$ that a random elliptic curve over $\mathbb{F}_q$ has N dividing the number of its $\mathbb{F}_q$-defined points satisfies

$$|\pi_{q,N} - r_q(N)| \leq \frac{CN\chi(N)2^{\sigma(N)}}{\sqrt{q}},$$

where $\chi(N) = \prod_{\lambda|N} (\lambda+1)/(\lambda-1)$ and $\sigma(N)$ denotes the number of prime divisors of N.

Let $g_q(\ell)$ be the probability that the smallest prime factor of M is ℓ. This probability is equal to

$$g_q(\ell) = r_q(\ell) \prod_{\text{primes } \lambda < \ell} (1 - r_q(\lambda)).$$

In our particular case, we test random curves E_a defined over $\mathbb{F}_{2^n}$ with cardinalities always divisible by 4, so, we make the strong assumption that Howe's theorem applies, except for $\ell = 2$, and the probabilities $r_{2^n}(\ell^k)$ become

$$\rho_n(\ell^k) = \begin{cases} 1 & \text{for } \ell = 2 \text{ and } k = 1, \\ \frac{1}{2^{k-2}} & \text{for } \ell = 2 \text{ and } k > 1, \\ r_{2^n}(\ell^k) & \text{for } \ell > 2. \end{cases}$$

Consequently, the probability $\gamma_n(\ell)$ we detect at step 2. of the algorithm that an odd prime ℓ divides the cardinality of E_a is equal to

$$\gamma_n(\ell) = \rho_n(\ell)(1 - \rho_n(2^3)) \prod_{\text{odd primes } \lambda < \ell} (1 - \rho_n(\lambda)).$$

This quantity can be easily computed for n fixed but for any n, one can only state that

$$\rho_n(2^3) = \frac{1}{2} \text{ and } \frac{\ell}{\ell^2-1} \leq \rho_n(\ell) \leq \frac{1}{\ell-1},$$

and therefore, $3/16 \leq \gamma_n(3) \leq 1/4$, $5/96 \leq \gamma_n(5) \leq 5/64$, $7/256 \leq \gamma_n(7) \leq 95/2304\ldots$

4.2 Results

The implementation described in Section 3.3 allows to compute a lot of such "good curves" defined over $\mathbb{F}_{2^{65}}$, $\mathbb{F}_{2^{89}}$, $\mathbb{F}_{2^{105}}$, $\mathbb{F}_{2^{155}}$ and $\mathbb{F}_{2^{196}}$ in a reasonable amount of time. Accurate statistics are given in Table 5.

	$\mathbb{F}_{2^{65}}$	$\mathbb{F}_{2^{89}}$	$\mathbb{F}_{2^{105}}$	$\mathbb{F}_{2^{155}}$	$\mathbb{F}_{2^{196}}$
# curves tested	1000	1000	1000	1000	1000
$1000\gamma_n(8)$	500	500	500	500	500
# cardinalities divisible by 8	491	507	500	509	490
$1000\gamma_n(3)$	250	250	250	250	187.5
# cardinalities divisible by 3	255	253	256	236	177
$1000\gamma_n(5)$	62.5	62.5	62.5	62.5	65.1
# cardinalities divisible by 5	63	73	74	68	150
$1000\gamma_n(7)$	31.2	31.2	27.4	31.2	41.2
# cardinalities divisible by 7	28	28	59	25	34
# cardinalities divisible by $\ell \geq 11$ and detected at step 2. of the algorithm	29	52	43	61	57
# cardinalities divisible by $\ell \geq 11$ and detected at step 3. of the algorithm	116	77	62	96	90
Number of "good curves"	18	10	6	5	2
Total time needed (s)	1277	1733	2231	14112	30254

Table 5. Statistics of the "early abort strategy".

In this table, it turns out that the theoretical estimations of Section 4.1 are in practice satisfied most of the time, except maybe for the number of cardinalities divisible by 5 in $\mathbb{F}_{2^{196}}$ (150 instead of $1000 \cdot 25/394 \simeq 65$). In any case, the probability that an elliptic curve has its number of points divisible by a small prime ℓ is quite high and thus we need to compute the cardinality of a curve completely in only a few case. Some of these "good curves" are given in Table 6 with the notation $a_0 + a_1 2 + \cdots + a_{n-1}2^{n-1} = a_0 + a_1 T + \cdots + a_{n-1}T^{n-1}$.

5 Conclusion

Thanks to the contribution of many people in this field of research, computing the number of points of an elliptic curve defined over $\mathbb{F}_{2^n}$ can be performed quickly in practice. From this, we derived an efficient way for finding elliptic curves with nearly prime cardinality. Even if it is harder to obtain such curves when n increases (only 2 among 1000 for $n = 196$), we think this method is of special interest for cryptographic purposes.

Performances we obtained for $\mathbb{F}_{2^n}$ are now similar to the performances we already had for the case $\mathbb{F}_p$ with p, a large prime, and this, even when the size of the finite field increases. The only problem which remains in practice is the case p odd and small. But, as what was foreseen at the end of [21] for $p = 2$, we hope that the situation might evolve very soon for these fields too.

Acknowledgments. I would like to thank François Morain for fruitful discussions. I also thank the referees for careful comments and for suggesting a title corresponding closer to the content of this article.

	a	Cardinality
$\mathbb{F}_{2^{65}}$	$\overline{2108463510029530717}$	$2^2 \cdot 9223372038308612213$
$\mathbb{F}_{2^{65}}$	$\overline{15004298573160993787}$	$2^2 \cdot 9223372035176356667$
$\mathbb{F}_{2^{89}}$	$\overline{362244896591784868971148794}$	$2^2 \cdot 154742504910673945144969913$
$\mathbb{F}_{2^{89}}$	$\overline{57852959336296070429241468}$	$2^2 \cdot 154742504910669983358163303$
$\mathbb{F}_{2^{105}}$	$\overline{6543935405400478025717290432415}$	$2^2 \cdot 10141204801825837522175841 2\backslash$ 06867
$\mathbb{F}_{2^{105}}$	$\overline{22959897163766013073560510 3979}\backslash$ $\overline{54}$	$2^2 \cdot 101412048018258342875266703\backslash$ 03267
$\mathbb{F}_{2^{155}}$	$\overline{838795043588789173323661086541}\backslash$ $\overline{2790131341725747}$	$2^2 \cdot 114179815416476790484662819\backslash$ 27805319915233345669
$\mathbb{F}_{2^{155}}$	$\overline{110027220687791685841747180597}\backslash$ $\overline{77371906785324958}$	$2^2 \cdot 114179815416476790484662992\backslash$ 30130487707830550127
$\mathbb{F}_{2^{196}}$	$\overline{250334701759594235393108283794}\backslash$ $\overline{64907961567696239688511281965}$	$2^2 \cdot 251084069415467230553431576\backslash$ $92759220570140916154347737377983$
$\mathbb{F}_{2^{196}}$	$\overline{404284818812143036331788043458}\backslash$ $\overline{37154824320382480200588296980}$	$2^2 \cdot 251084069415467230553431576\backslash$ $92813473113492187155697729606263$

Table 6. Curves with a nearly prime cardinality.

References

[1] A. Bender and G. Castagnoli. On the implementation of elliptic curve cryptosystems. In G. Brassard, editor, *Advances in Cryptology*, volume 435 of *Lecture Notes in Comput. Sci.*, pages 186–192. Springer-Verlag, 1989. Proc. Crypto '89, Santa Barbara, August 20–24.

[2] F. Chabaud and R. Lercier. A new toolbox for finite extensions of finite fields. Technical report, Laboratoire d'Informatique de l'École Polytechnique (LIX), 1996. In preparation.

[3] F. Chabaud and R. Lercier. *ZEN, User Manual.* Laboratoire d'informatique de l'École polytechnique (LIX), 1996. Available at `http://lix.polytechnique.fr/~zen/`.

[4] J. Chao, K. Tanada, and S. Tsujii. Design of elliptic curves with controllable lower boundary of extension degree for reduction attacks. In Y. Desmedt, editor, *Advances in Cryptology – CRYPTO '94*, volume 839 of *Lecture Notes in Comput. Sci.*, pages 50–55. Springer-Verlag, 1994. Proc. 14th Annual International Cryptology Conference, Santa Barbara, Ca, USA, August 21–25.

[5] B. W. Char, K. O. Geddes, G. H. Gonnet, and S. M. Watt. *Maple Reference Manual, Fourth Edition.* Symbolic Computation Group, Department of Computer Science, University of Waterloo, 1985.

[6] J. M. Couveignes. *Quelques calculs en théorie des nombres.* thèse, Université de Bordeaux I, July 1994.

[7] J. M. Couveignes. Computing l-isogenies with the p-torsion. In H. Cohen, editor, *ANTS-II*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 59–65. Springer-Verlag, 1996.

[8] J. M. Couveignes. Isomorphisms between towers of artin-schreier exetensions over a finite fields. Draft, 1997.

[9] J.-M. Couveignes, L. Dewaghe, and F. Morain. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Research Report LIX/RR/96/03, LIX, April 1996.

[10] J.M. Couveignes and F. Morain. Schoof's algorithm and isogeny cycles. In L. Adleman and M. D. Huangs, editors, *ANTS-I*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 43–58. Springer-Verlag, May 1994.

[11] G. Harper, A. Menezes, and S. Vanstone. Public-key cryptosystems with very small key length. In R. A. Rueppel, editor, *Advances in Cryptoloy – EUROCRYPT '92*, volume 658 of *Lecture Notes in Comput. Sci.*, pages 163–173. Springer-Verlag, 1993. Workshop on the Theory and Application of Cryptographic Techniques, Balatonfüred, Hungary, May 24–28, 1992, Proceedings.

[12] E. W. Howe. On the group orders of elliptic curves over finite fields. *Compositio Mathematica*, 85:229–247, 1993.

[13] B. S. Kaliski, Jr. A pseudo-random bit generator based on elliptic logarithms. In *Proc. Crypto 86*, volume 263 of *Lecture Notes in Comput. Sci.*, 1986. Proceedings Crypto '86, Santa Barbara (USA), August 11–15, 1986.

[14] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, January 1987.

[15] N. Koblitz. Primality of the number of points on an elliptic curve over a finite field. *Pacific Journal of Mathematics*, 131(1):157–165, 1988.

[16] N. Koblitz. Elliptic curve implementation of zero-knowledge blobs. *Journal of Cryptology*, 4(3):207–213, 1991.

[17] G. J. Lay and H. G. Zimmer. Constructing elliptic curves with given group order over large finite fields. In L. Adleman and M.-D. Huang, editors, *ANTS-I*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 250–263. Springer-Verlag, 1994. 1st Algorithmic Number Theory Symposium - Cornell University, May 6-9, 1994.

[18] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Math.*, 126:649–673, 1987.

[19] R. Lercier. Computing isogenies in GF(2^n). In H. Cohen, editor, *ANTS-II*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 197–212. Springer-Verlag, 1996.

[20] R. Lercier. Finding good random elliptic curves for cryptosystems definied over $\mathbb{F}_{2^n}$. In *Advances in Cryptoloy – EUROCRYPT '97*, LNCS. Springer-Verlag, 1997. To appear.

[21] R. Lercier and F. Morain. Counting the number of points on elliptic curves over finite fields: strategies and performances. In L. C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology – EUROCRYPT '95*, number 921 in Lecture Notes in Comput. Sci., pages 79–94, 1995. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceedings.

[22] R. Lercier and F. Morain. Counting the number of points on elliptic curves over F_{p^n} using Couveignes's algorithm. Rapport de Recherche LIX/RR/95/09, Laboratoire d'Informatique de l'École polytechnique (LIX), 1995. Available at `http://lix.polytechnique.fr/~morain/Articles`.

[23] A. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curves logarithms to logarithms in a finite field. *IEEETIT*, 39(5):1639–1646, 1993.

[24] A. Menezes and S. A. Vanstone. The implementation of elliptic curve cryptosystems. In J. Seberry and J. Pieprzyk, editors, *Advances in Cryptology*, number 453 in Lecture Notes in Comput. Sci., pages 2–13. Springer–Verlag, 1990. Proceedings Auscrypt '90, Sysdney (Australia), January 1990.

[25] A. J. Menezes. *Elliptic curve public key cryptosystems.* Kluwer Academic Publishers, 1993.

[26] A. J. Menezes, S. A. Vanstone, and R. J. Zuccherato. Counting points on elliptic curves over F_{2^m}. *Math. Comp.*, 60(201):407–420, January 1993.

[27] V. Miller. Use of elliptic curves in cryptography. In A. M. Odlyzko, editor, *Advances in Cryptology*, volume 263 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer-Verlag, 1987. Proceedings Crypto '86, Santa Barbara (USA), August11–15, 1986.

[28] A. Miyaji. On ordinary elliptic curve cryptosystems. In *Advances in Cryptology – ASIACRYPT '91*, volume 739 of *Lecture Notes in Comput. Sci.*, pages 50–55. Springer-Verlag, 1991.

[29] A. Miyaji. Elliptic curves over F_p suitable for cryptosystems. In J. Seberry and Y. Zheng, editors, *Advances in cryptology - AUSCRYPT '92*, volume 718 of *Lecture Notes in Comput. Sci.*, pages 479–491. Springer-Verlag, 1993. Workshop on the theory and application of cryptographic techniques, Gold Coast, Queensland, Australia, December 13-16, 1992.

[30] F. Morain. *Courbes elliptiques et tests de primalité.* thèse, Université Claude Bernard–Lyon I, September 1990.

[31] F. Morain. Building cyclic elliptic curves modulo large primes. In D. Davies, editor, *Advances in Cryptology – EUROCRYPT '91*, volume 547 of *Lecture Notes in Comput. Sci.*, pages 328–336. Springer–Verlag, 1991. Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques, Brighton, United Kingdom, April 8–11, 1991.

[32] F. Morain. Classes d'isomorphismes des courbes elliptiques supersingulières en caractéristique ≥ 3. To appear in Utilitas Mathematica. Preprint, available at `http://lix.polytechnique.fr/~morain/`, March 1996.

[33] V. Müller. *Ein Algorithmus zur bestimmung der Punktanzahl elliptisher kurven über endlichen körpen der charakteristik größer drei.* PhD thesis, Technischen Fakultät der Universität des Saarlandes, February 1995.

[34] S. Pohlig and M. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. *IEEE Transactions on Information Theory*, 24:106–110, 1978.

[35] J. M. Pollard. Monte Carlo methods for index computation $\pmod p$. *Math. Comp.*, 32(143):918–924, July 1978.

[36] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.

[37] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7:219–254, 1995. Available at `http://www.emath.fr/Maths/Jtnb/jtnb1995-1.html`.

[38] R. Schroeppel, H. Orman, S. O'Malley, and O. Spatscheck. Fast key exchange with elliptic curve systems. In Don Coppersmith, editor, *Advances in Cryptology - Crypto '95*, pages 43–56, Berlin, 1995. Springer-Verlag. Lecture Notes in Computer Science Volume 963.

[39] D. Shanks. Class number, a theory of factorization, and genera. In *Proc. Symp. Pure Math. vol. 20*, pages 415–440. AMS, 1971.

[40] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.