SCIS92 The 1992 Symposium on
Cryptography and Information Security
Tateshina, Japan, April 2-4, 1992
The Institute of Electronics,
Information and Communication Engineers

暗号に適した楕円曲線の実現
On the Implementation of Ordinary Elliptic Curve Cryptosystems

宮地 充子
Atsuko Miyaji

April 1, 1992

松下電器産業株式会社
Matsushita Electric Industrial Co. , LTD.
miyaji@isl.mei.co.jp

Abstract

A method, proposed by [MOV], gave an impact on the security of cryptosystems based on the elliptic curve discrete logarithm problem(EDLP). The author showed the method is valid only when Weil pairing can be defined over the m-torsion group which includes the base point of EDLP([Miy]). If an elliptic curve is ordinary, there exists EDLP which makes the reducing inapplicable. In this paper, we explore the feasibility of constructing such ordinary elliptic curves E defined over F_p. We show the next main results.

- We present a revised algorithm for constructing ordinary elliptic curves E defined over F_p that make reducing EDLP on E to DLP by embedding impossible.
- With the algorithm we can construct a 30 digits's elliptic curve in 70.8 seconds on a 32 bit personal computer(20MHz).
- We are able to construct 30 digits's elliptic curves of theorem2 in 70.8 seconds on 32bit personal computer(20 MHz).

あらまし：著者は、以前に楕円曲線の離散対数問題にはどんな埋め込みによっても有限体上の離散対数問題に帰着して解法することができないものが存在することを示した。本報告書では上記の性質を持ち十分安全な素数位数の楕円曲線が３２ビットパソコンを用いて実用的な速度で構成できることを示した。

Section 5 shows the experiment results for constructing elliptic curves with elements of a 30 digit prime.

Notation

p : a prime
r : a positive integer
q : a power of p
F_q : a finite field with q elements
K : a field (including a finite field)
$ch(K)$: the characteristic of a field K
K^* : the multiplicative group of a field K
$\overline{K}$: a fixed algebraic closure of K
E : an elliptic curve
If we remark a field of definition K of E , we write E/K.
$\#$A : the cardinality of a set A
$o(t)$: the order of an element t of a group
Z : the ring of integers

2 What makes the reduction inapplicable?

In this section, we outline the condition that makes the MOV reduction of EDLP inapplicable. For more information, see [Miy]. First we give the definition of EDLP .

Definition 1 ([Ko2]) *Let E/F_q be an elliptic curve and P be a point of $E(F_q)$. Given a point $R \in E(F_q)$, EDLP on E to the base P is the problem of finding an integer $x \in Z$ such that $xP = R$ if such an integer x exists.*

The MOV reduction is constructed by Weil pairing defined over an m-torsion subgroup containing $< P > \subset E(F_q)$, generated by a point P. If $o(P)$ is divisible by $ch(F_q)$, the Weil pairing can't be defined over any m-torsion subgroup containing $< P >$. So in this case, the MOV reduction is invalid. Though it is the special case, it happens in the case of ordinary elliptic curves. Next we give the definition of ordinary elliptic curves.

Definition 2 *Let E/F_q be an elliptic curve. If E has the properties $E[p^t] = \mathcal{O}$ for all integer $t \geq 1$, then we say that E is supersingular. Otherwise we say that E is ordinary.*

3.2 Good d and good p

For a given large prime p, we can construct an elliptic curve E/F_p as we mentioned above. What prime p and integer d such that $4p - 1 = b^2 d$ (b is an integer) are good for constructing such an elliptic curve? We will find a prime p and an integer d such that the order O_d has a small class number. Because if the order O_d has a large class number, the degree of $P_d(x)$ is large and it is cumbersome to construct $P_d(x)$.

3.3 Procedure for constructing an elliptic curve

We can construct an elliptic curve by the following algorithm.

Procedure

(p-1) Choose an integer d such that the order O_d has a small class number from a list ([Ta]).

(p-2) Find a large prime p such that $4p - 1 = b^2 d$ for an integer b.

(p-3) Calculate a class polynomial $P_d(x)$.

(p-4) Let $j_0 \in F_p$ be one root of $P_d(x) = 0 \pmod{p}$.

(p-5) Construct an elliptic curve E/F_p with j-invariant j_0.

(p-6) Construct all twists of E/F_p.

(p-7) For any twist E_t of E/F_p, fix any point $X_t \neq \mathcal{O}$ of $E_t(F_p)$ and calculate pX_t. If $pX_t = \mathcal{O}$, then $E_t(F_p)$ has exactly p elements.

For the purpose of making EDLP on E/F_p complexity, we must construct E/F_p with p, more than 30 digits, elements. This procedure is too general, so we can't know feasibility of making such an elliptic curve. In order to estimate the running time for the construction of elliptic curves with the necessary figure, we also need what the running time of it depends on. The next section investigates these.

Problem2: For a given prime p, make E/F_p with p elements.

First we discuss problem1 in the next section.

4.2 Finding p

First we discuss the case of $d = 11$. As we mentioned section 3, the prime p must be more than 30 digits. A simple algorithm would be as follows.
Algorithm

1. Let $b = \lceil\sqrt{\frac{4*10^{29}-1}{11}}\rceil$.
2. Test the primality of $p = \frac{1+11*b^2}{4}$. If p isn't prime, then increase b by 1 and repeat 2. If p is prime, then stop.

This algorithm requires testing primality of p one by one for all b. We can reduce the number of tests to $\frac{1}{10}$ by the algorithm 1.

Algorithm 1 .

1. *Let b be the minimal integer satisfying the next two conditions:*

   Condition1: $b \geq \lceil\sqrt{\frac{4*10^{29}-1}{11}}\rceil$;
   Condition2: $b \equiv 9, 15, 21 \pmod{30}$.

   Then $b = 190692517849119 \equiv 9 \pmod{30}$ *and goto 2.*

2. *Test the primality of* $p = \frac{1+11*b^2}{4}$. *If p isn't prime, then* $b = b + 6$ *and goto 3. If p is prime, then stop.*

3. *Test the primality of* $p = \frac{1+11*b^2}{4}$. *If p isn't prime, then* $b = b + 6$ *and goto 4. If p is prime, then stop.*

4. *Test the primality of* $p = \frac{1+11*b^2}{4}$. *If p isn't prime, then* $b = b + 18$ *and goto 2. If p is a prime, then stop.*

The validity of the algorithm 1 follows the next discussion.
From $4p = 11 * b^2 + 1$, $b \equiv 1 \pmod{2}$. In order for p to be prime more than 30 digits, $4p = 11 * b^2 + 1 \not\equiv 0 \pmod{3}$. So we get $b \equiv 0 \pmod{3}$. In the same way, we get $b \equiv 0, 1, 4 \pmod{5}$. Therefore the integer b requires that

$$\left(\frac{c}{p}\right) = \begin{cases} 1 & \text{if } c \text{ is a quadratic residue} \pmod p \\ -1 & \text{if } c \text{ is a non-quadratic residue} \pmod p . \end{cases}$$

Then the one group gives the elliptic curves with p elements and the other doesn't.

First we discuss how to choose an elliptic curve and its point for each group. We deal with the group $\mathcal{E}'$. First we choose t such that $\left(\frac{t}{p}\right) = -1$. We apply the fact that

$$\text{for any } c \text{ such that } \left(\frac{c}{p}\right) = 1,\ \mathcal{E}' \ni E_{ct}.$$

Let

$$y_0 = x_0^3 + t^2 \frac{j}{1728-j} x_0 + t^3 \frac{j}{1728-j} \quad \text{for } x_0 \in F_p.$$

If $\left(\frac{y_0}{p}\right) = 1$, we understand $E_{y_0 t} \in \mathcal{E}'$ from the above fact. We further see $E_{y_0 t} \ni (y_0 x_0, y_0^2)$ easily. So we get $\mathcal{E}' \ni E_{y_0 t}$ and $E_{y_0 t}(F_p) \ni (y_0 x_0, y_0^2)$.

Concerning $\mathcal{E}$, we may use E_1 instead of E_t. We combine this and procedure (p-7) into the next algorithm 2.

Algorithm 2 .

1. *Find $x_0 \in F_p$ such that $y_0 = x_0^3 + \frac{j}{1728-j} x_0 + \frac{j}{1728-j}$ is a quadratic residue. Then $X_{y_0} = (y_0 x_0, y_0^2) \in E_{y_0}(F_p)$.*

2. *Calculate pX_{y_0}. If $pX_{y_0} = \mathcal{O}$, then $E_{y_0}(F_p)$ has exactly p elements. If not, we choose t such that $\left(\frac{t}{p}\right) = -1$ and find $x_1 \in F_p$ such that $y_1 = x_1^3 + t^2 \frac{j}{1728-j} x_1 + t^3 \frac{j}{1728-j}$ is a quadratic residue. Then $E_{y_1 t}(F_p) \ni (y_1 x_1, y_1^2)$ and $E_{y_1 t}(F_p)$ has just p elements over F_p.*

We can easily determine whether an element is a quadratic residue or not. So the running time of this algorithm is insignificant compared to the time of algorithm 1. Thus the time to construct elliptic curves (theorem 2) should mainly depend on the time to implement the algorithm 1. Experimental results in section 5 show this actually happens.

the distribution of b that makes $\frac{1+d*b^2}{4}$ prime in a ranged of $\{b|Low \leq b \leq Low + 10^4\}$. Table 5 shows the minimal and maximal primes obtained.

We construct $E/F_p, E(F_p) \ni X$ for all primes p given by the previous experiment with algorithm 2. Table 6 presents the running time for the algorithm 2.

5.2 Consideration of experimental results

From the experimental results we obtained, Table 7 lists the time necessary to construct one elliptic curve good for cryptosystems. We see that we can make an elliptic curve with p elements, where p is prime, in 70.6 seconds on a 32bit personal computer(20 MHz) on the average. We further see if a prime p is given, we can make E/F_p with p elements in a few seconds (Table 6). So we can easily construct many elliptic curves as the source of cryptosystems for a given p.

The conjecture 1 of existence of a prime p satisfying $4p - 1 = b^2 d$ says nothing about the distribution of p for b. We know it may be very important for the running time to find such p. Table 3 and 4 say that the higher the distribution is, the faster the time to find p is.

6 Conclusion

The construction of E/F_p with p elements consists of two phases. One is to find a prime p such that $4p = 1 + db^2$ for a given d. We analyzed the condition of b and reduced the number of primality tests. We reduced the number of primality tests to $\frac{1}{10}$ in the case of $d = 11$. Second is to construct an elliptic curves E/F_p with p elements for a given p. We showed that we can construct E/F_p in a polynomial time of the element size. We also showed that we can construct E/F_p with p elements in a practical time on a 32 bit personal computer.

7 Acknowledgements

I wish to thank Makoto Tatebayashi for his helpful advice. I am grateful to all other members of my group for their kind help. I express my gratitude to Yoshihiko Yamamoto for his teaching me about the class polynomial.

References

[Be-Ca] A. Bender and G. Castagnoli *"On the implementation of elliptic curve cryptosystems", Advances in Cryptology - Proceedings of Crypto '89, Lecture Notes in Computer Science, 435 (1990), Springer-Verlag, 186-192.*

[Be-Sc] T. Beth and F. Schaefer *"Non supersingular elliptic curves for public key cryptosystems", Abstracts for Eurocrypto 91 , Brighton, U.K. 155-159.*

[Co-Le] H. Cohen and H. W. Lenstra Jr. *"Primality Testing and Jacobi Sums ", Mathematics of computation 42(1984), 297-330*

[Deu] M. Deuring *"Die Typen der Multiplikatorenringe elliptischer Funktionenkorper", Abh. Math. Sem. Hamburg 14 (1941), 197-272.*

[HW] G. Hardy and E. Wright *"An Introduction to the Theory of Numbers", Oxford Univ. Press, 1960.*

[Ko1] N. Koblitz *"Elliptic curve cryptosystems", Math. Comp. 48(1987), 203-209.*

[Ko2] N. Koblitz *"A course in Number Theory and Cryptography", GTM114, Springer-Verlag, New York(1987).*

[Ko3] N. Koblitz *"CM-curves with good cryptographic properties", Proceedings of CRYPTO'91, to appear*

[La] S. Lang *"Elliptic Functions", Addison-Wesley, 1973.*

[Mil] V. S. Miller *"Use of elliptic curves in cryptography", Advances in Cryptology-Proceedings of Crypto'85, Lecture Notes in Computer Science, 218 (1986), Springer-Verlag, 417-426.*

[Miy] A. Miyaji *"On ordinary elliptic curves", Abstract of proceedings of ASIACRYPTO'91, 1991*

[Me-Va] A. Menezes and S. Vanstone *"The implementaion of elliptic curve cryptosystems", Advances in Cryptology - Proceedings of Auscrypt'90, Lecture Notes in Computer Science, 453(1990), Springer-Verlag, 2-13.*