Design of Elliptic Curves with Controllable Lower Boundary of Extension Degree for Reduction Attacks

Jinhui Chao[1], Kazuo Tanada[2] and Shigeo Tsujii[1]

[1] Chuo University, 1-13-27, Kasuga, Bunkyo-ku, Tokyo, 112, Japan
[2] Tokyo Institute of Technology, 2-12-1, Ookayama, Meguro-ku, Tokyo, 152, Japan

Abstract. In this paper, we present a design strategy of elliptic curves whose extension degrees needed for reduction attacks have a controllable lower boundary, based on the complex multiplication fields method of Atkin and Morain over prime fields.

1 Introduction

In recent years, elliptic curves have been used to define a new category of discrete logarithm problems, in hope to build new one-way functions instead of the existing cryptographic functions [1][2] [3].

An elliptic curve over a field K, E/K is defined by the Weierstrass canonical form

$$E/K \ : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_1, a_3, a_2, a_4, a_6 \in K). \quad (1)$$

When $\mathrm{char}(K) \neq 2, 3$, E/K can be transformed by an isomorphism to a form of

$$E/K \ : y^2 = x^3 + ax + b \quad (a, b \in K). \quad (2)$$

The discrete logarithm problem over an elliptic curve E/K is to find $x \in \boldsymbol{Z}$ such that for P, $Q \in E/K$, $Q = xP$. Hereafter we will assume that $\mathrm{char}(K) = p$.

The above problems are expected to provide a new cryptographic function with stronger integrity and have been applied to build cryptosystems. Until now, two algorithms are known as attacks on the problems: the Baby-step-Giant-step algorithm[4] and the MOV reduction [5].

The first method by Shanks costs $O(\sqrt{\#E(K)}\log \#E(K))$ of fully exponential time. Its fast versions, e.g. Pohligh-Hellman's algorithm[6] reduced the computation to order of the root of the maximum prime factor of $\#E(K)$. If the maximum prime factor is smaller than $\log \#E(K)$, it costs $O((\log \#E(K))^2)$ and becomes a very powerful method.

The second algorithm by Menezes, Okamoto and Vanstone uses the Weil pairing to embed the discrete logarithm problems over $E(\boldsymbol{F}_q)$ into the classic discrete logarithm problems over certain extension of the ground field $\boldsymbol{F}_{q^k}$, which then can be solved by efficient algorithms such as Adleman's index algorithm[7] of subexponential time. This approach works when the extension degree of the ground field required for a well-defined embedding is very low.

Y.G. Desmedt (Ed.): Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 50-55, 1994.

To defend the elliptic-curves-based cryptosystems against the first attack, the order of elliptic curves $\#E(K)$ has to contain a large prime factor. As to the second attack, it is known that for a class of elliptic curves called super-singular curves, the reduction can be fulfilled with extension of 6 degree of the ground field[5]. The super-singular curves however are in fact very few. For the ordinary or non-super-singular curves, it is shown in [8] that with high probability, the extension degrees of the ground field needed for reduction attack on random curves are an exponential function of $char(\boldsymbol{F}) = p$. However, this is an asymptotic conclusion and not directly applicable to a fixed prime p [8]. In cryptosystem design practice, it would be desirable to find some strategy to control the lower bound of the extension degree for particular curves defined over fixed fields.

In this paper, we consider about the extension degree of ground fields which is needed to reduce discrete logarithm problems over elliptic curves to discrete logarithm problems over finite fields. Then we show an algorithm to design elliptic curves over primary fields which can control the extension degree for the reduction attack. This algorithm is based on the complex multiplication field method by Atkin and Morain[9][10]. (Both the algorithms can also be generalized over extension fields[11].)

2 Current Design Methods of Curves

Below we review popular design methods of elliptic curves.

(1) Method using Schoof's algorithm[12] : This method selects randomly curves until a desired group structure is found. The order of the curve is calculated by Schoof's algorithm. Koblitz used the following algorithm to design curves of prime orders and the extension degree for the reduction attack to be larger than $(\log p)^2$[8].

[Koblitz's algorithm]

1. Choose a curve $E/\boldsymbol{F}_p$ randomly;
2. Calculate $N = \#E(\boldsymbol{F}_p)$ by Schoof's algorithm;
3. Check that if N is a prime, if not, go back to 1;
4. Check that if $p^j \not\equiv 1 \bmod N (1 \leq j \leq (\log p)^2)$ if not, go back to 1.

In this algorithm, the order calculation part is of most costly, which requires $O((\log p)^8)$ computations by Schoof's algorithm. This becomes awkward when p is large. Recently, progresses have appeared in development of fast order calculation algorithms. However, the order-counting problem seems to be difficult for curves with arbitrary orders. One way to avoid this difficulty is to choose an order first which is "easy" in certain sense and with desired cryptographic property, then build a curve with such order. This is the method by Atkin and Morain.

(2) Method using complex multiplication field : It is implemented by Atkin and Morain to build curves of assigned order with complex multiplication[9] [10].

[Atkin, Morain's algorithm]

1. Determine an order $\#E(\boldsymbol{F}_p) = m$ such that $t = p+1-m$ satisfies $|t| < 2\sqrt{p}$;
2. Calculate d such that $t^2 - 4p = c^2 d$;
3. Calculate the class equation $H_d(x)$;
4. Solve $H_d(x) \equiv 0 \bmod p$ to find a root j_0;
5. Build a curve with j_0 as its j-invariant.

Theoretically, one can produce curves over the prime field with arbitrary order with this algorithm. The most demanding part of the algorithm is the step 3, 4. Since the degree of $H_d(x)$ equals the class number of d, $h(d)$ which is of $O(\sqrt[4]{p})$, the calculation of $H_d(x)$ and the solution of it over $\boldsymbol{F}_p$ by Berlekamp's[13] or Rabin's[14] algorithms require computations of exponential time.

Thus, this algorithm can only be used for small class number cases. Under this condition, curves with the order equals to the characteristic or contains a large prime factor are built in [15][16]. The curve used in [15] is interesting because it can resist any reduction attacks. However, there is only one isogeny class of such curves over a prime field. (Although much richer isogeny classes of p-divisible curves exist over extension fields [17]). Besides, in order to make the class number small, one has to restrict the prime p to meet certain conditions. For the same reason, isogeny classes of curves are also restricted. On the other hand, it seems that to build curves without using Schoof's algorithm could be computationally attractive.

3 Design of Curves with Controlled Lower Boundary of Extension Degree against Reduction Attack

To control the extension degree for the reduction attack, we choose the following strategy, i.e., to specify a lower boundary B of the extension degree for the reduction attack, then design a curve with the order satisfies this lower boundary.

First we consider the extension degree for the reduction attack on non-p-divisible curves.

The condition for any well-defined reduction to $\boldsymbol{F}_{q^k}$ with $m = \#E(\boldsymbol{F}_q)$ is that

$$m \mid q^k - 1 \tag{3}$$

or

$$q^k \equiv 1 \bmod m \tag{4}$$

By Euler's theorem, the minimum k satisfies (4) must a factor of $\varphi(m)$. Thus, take the primary factorization of $\varphi(m)$, one can find the minimum factor satisfy (4), then find the minimum k. However, the primary factorization of $\varphi(m)$ is then necessary, which could become a new computational burden.

Now we give a condition of order m for the extension degree to be larger than B.

Theorem 1. *Assume an elliptic curve over $\boldsymbol{F}_q$ has order m. Denote the extension degree for arbitrary reduction as k. If $\varphi(m)/2$ is B-nonsmooth and $q^2 \not\equiv 1 \bmod m$ then*

$$k \geq B.$$

Here n is B-nonsmooth means that n has not primary factors less than B.

Proof : As before, by Euler's theorem, k divides $\varphi(m)$. If $\varphi(m)/2$ is B-nonsmooth, then $k = 2$ or $k \geq B$. Thus, if $q^2 \not\equiv 1 \bmod m$, then $k \geq B$. QED

Corollary 2. *Let $\#E(\boldsymbol{F}_q) = m$, $l \,|\, m$ (l : a prime), and the extension degree for any reduction as k. If $(l-1)/2$ is B-nonsmooth and $q^2 \not\equiv 1 \bmod l$ then*

$$k \geq B$$

QED

Therefore, curves are to be designed to satisfy the following condition.

zh

Condition : $l \mid \#E(\boldsymbol{F}_p)$ and $(l-1)/2$ is B-nonsmooth.

zh

We need then a method to assign order of a curve. There is currently only one method for this purpose, the one with complex multiplication fields, or Atkin and Morain's algorithm.

Below, we show an algorithm over primary fields to build the curves satisfy the above condition based on the Atkin and Morain's algorithm.

[Algorithm]

1. Choose a large prime l such that $(l-1)/2$ to be B-nonsmooth and $(\frac{d}{l}) = 1$, choose also $d < 0$ with small $h(d)$;
2. Choose t, c, s such that $(t-2)^2 = 4sl + c^2 d$, $(t \not\equiv 0, 2 \bmod l)$;
3. Check if $p = sl + t - 1$ is a prime , if not, go back to 2. ;
4. Calculate the class equation $H_d(x)$ and solve $H_d(x) \equiv 0 \bmod p$ to find a root j_0 ;
5. Define a curve with j-invariant as j_0.

In this way, curves of order sl are derived.

In Step1, to search for B-nonsmooth l need about $(\log l)(\log B)$ primality tests. $(\frac{d}{l}) = 1$ holds in probability of $1/2$. Once $(\frac{d}{l}) = 1$ is true, there are plenty of solutions for Step2. Assuming p is random, Step 3 will repeat about $\log p$ times to pass the check. (In simulation it seems quite easy.)

[Example]

1. Choose prime $l = 21838143759917965991093122527538325 03$ and $d = -43$; where $l - 1 = 2 * 10\,91907\,18799\,58982\,99554\,65612\,63769\,16251$
2. Choose $t = 5472\,72782\,79345\,38832$, $s = 4$;
3. Obtain $p = 87\,35257\,50396\,71864\,01909\,97683\,89498\,68843$;
4. From $H_d(x) = x + 960^3$, we have $j_0 = -960^3$, which defines a curve as

zh

$$y^2 = x^3 + ax + b \bmod p \tag{5}$$
$$a = 29\,71431\,93700\,48984\,66387\,07954\,89768\,65095$$
$$b = 9\,30797\,87665\,24631\,56378\,60591\,36653\,79551$$
$$p = 87\,35257\,50396\,71864\,01909\,97683\,89498\,68843$$

This curve has its order and the extension degree for any reduction as

$$\#E(\boldsymbol{F}_p) = 4 * 21\,83814\,37599\,17965\,99109\,31225\,27538\,32503$$
$$B = 10\,91907\,18799\,58982\,99554\,65612\,63769\,16251$$

References

1. Miller, V. S.: Use of elliptic curves in cryptography. Advances in Cryptology-CRYPTO'85, Lecture Notes in Computer Science, **218** (1986) 417-426
2. Koblitz, N. : Elliptic Curve Cryptosystems. Math. Comp. **48** (1987) 203-209
3. Menezes, A. J.: *Elliptic Curve Public Key Cryptosystems* Kluwer Academic Publishers (1993)
4. Knuth, D. E.: *The art of computer programming*, Sorting and searching. vol. 3, Addison Wesley (1973)
5. Menezes, A. J., Vanstone, S., Okamoto T.: Reducing elliptic curve logarithms to logarithms in a finite field. Proc. of STOC'91 (1991) 80-89
6. Pohlig, S. C., Hellman, M. E.: An improved algorithm for computing logarithm over $GF(p)$ and its cryptographic significance. IEEE Trans. Information Theory, **IT-24**, 1 (1978) 106-110,
7. Adleman, L. M.: A subexponential algorithm for the discrete logarithm problem with applications to cryptography. Proc. of IEEE 20th Symp. on Foundations of Comp. Sci. (1979) 55-60
8. Koblitz, N.: Elliptic curve implementation of zero-knowledge blobs. Journal of Cryptology, vol. 4, No. 3 (1991) 207-213,
9. Atkin, A. O. L., Morain F.: Elliptic curves and primality proving. Research Report 1256, INRIA, June (1990)
10. Morain, F., Building cyclic elliptic curves modulo large primes. Advances in Cryptology -EUROCRYPT'91, Lecture Notes in Computer Science, **547** (1991) 328-336
11. Chao, J., Tanada, K., Tsujii S.: On secure elliptic curves against the "reduction attack" and their design strategy. Proc. of SCIS'94 (1994) 10A, IEICE Tech. Report, ISEC93-100, 29-37

12. Schoof, R.: Elliptic curves over finite fields and the computation of square roots mod p. Math. Comp. **44** (1985) 483-494
13. Berlekamp, E. R.: *Algebraic coding theory.* MacGraw–Hill (1968)
14. Rabin, M. O.: Probabilistic algorithm in finite fields. SIAM J. on Comput., Vol.9, No.2 (1980) 273-280
15. Miyaji, A.: On ordinary elliptic curve cryptosystems. Advances in Cryptology-ASIACRYPT'91, Lecture Notes on Computer Science **739** (1991) 460-469
16. Miyaji, A.: Fast elliptic curve cryptosystems, Technical Report of IEICE (1993) COMP93-25
17. Chao, J., Ikemoto, H., Tanada, K., Tsujii, S.: On Discrete Logarithm Problems over elliptic curves with p-divisible groups. Proc. of Joint Workshop on Information Security and Cryptography, JW-ISC93 (1993) 99-104
18. Koblitz, N.: Constructing elliptic curve cryptosystems in characteristic 2. Advances in Cryptology - CRYPTO'90, Lecture Notes in Computer Science, **537** (1990) 156-167