On Ordinary Elliptic Curve Cryptosystems

Atsuko Miyaji

Matsushita Electric Industrial Co., LTD.
Information and Communications Research

Abstract

Recently, a method, reducing the elliptic curve discrete logarithm problem(EDLP) to the discrete logarithm problem(DLP) in a finite field, was proposed. But this reducing is valid only when Weil pairing can be defined over the m-torsion group which includes the base point of EDLP. If an elliptic curve is ordinary, there exists EDLP which we cannot apply the reducing to. In this paper, we investigate the condition for which this reducing is invalid. We show the next two main results. (1) For any elliptic curve E defined over F_{2^r} , we can reduce EDLP on E to DLP in an extension finite field of F_{2^r} by extending the above proposed method. (2) For an ordinary elliptic curve E defined over F_p (p is a large prime) , EDLP on E cannot be reduced to DLP in any extension field of F_p by any embedding. Furthermore we show an algorithm that constructs such ordinary elliptic curves E defined over F_p that makes reducing EDLP on E to DLP by embedding impossible.

1 Introduction

Koblitz and Miller described how the group of points on an elliptic curve over a finite field can be used to construct public key cryptosystems([Mil],[Ko1]). The security of these cryptosystems is based on the elliptic curve discrete logarithm problem(EDLP). The best algorithm that has been known for solving EDLP is only the method of Pohlig-Hellman([Ko2]). Since it doesn't work for the elliptic curve over a finite field whose order is divided by a large prime, some works on the implementation of elliptic curve cryptosystems have been done ([Me-Va],[Be-Ca]). Recently Menezes, Vanstone and Okamoto([MVO]) proposed a method to reduce EDLP on an elliptic curve E defined over a finite field F_q to the discrete logarithm problem(DLP) in a suitable extension field of F_q . Using their method, H.Shizuya, T.Itoh and K.Sakurai([SIS]) gave a characterization for the intractability of EDLP from a viewpoint of computational complexity theory. In this paper, we call their method ([MVO]) the reducing method.

The reducing method is constructed by a pairing defined over an m-torsion subgroup of an elliptic curve. It is called the Weil pairing. If an elliptic curve is supersingular, the Weil pairing is defined over any m-torsion subgroup of it. But if an elliptic curve is ordinary (non-supersingular), there exists an m-torsion subgroup of it which the Weil pairing can't be defined over. So we consider to extend the reducing method to EDLP on such m-torsion group of an ordinary elliptic curve.

Our result of this paper is following. For any elliptic curve E defined over F_{2^r} , we can reduce EDLP on E to DLP in a suitable extension field of F_{2^r} (Theorem 1). For an ordinary elliptic curve E defined over F_p (p is a large prime) , we cannot reduce EDLP on E to DLP in any extension field of F_p by any embedding (Theorem 2).

Section 2 contains a brief summary of the elliptic curves that we will need later. Section 3 explains the reducing method. Section 4 mentions the case that we cannot apply the reducing method and includes two subsection 4-1 and 4-2. Subsection 4-1 discusses how we can extend the reducing method to EDLP on any ordinary elliptic curve E defined over F_{2^r}. Subsection 4-2 shows why we cannot reduce EDLP on an ordinary elliptic curves E defined over F_p to DLP in any extension field of F_p by embedding. Section 5 constructs ordinary elliptic curves E defined over F_p that makes reducing EDLP on E to DLP by embedding impossible.

notation

p	: a prime
r	: a positive integer
q	: r powers of p
F_q	: a finite field with q elements
K	: a field (include 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 Background on Elliptic Curves

We briefly describe some properties of elliptic curves that we will use. For more information, see[Sil]. In the following, we denote a finite field F_q by K .

Basic Facts

Let E/K be an elliptic curve given by the equation, called Weierstrass equation,

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

The j-invariant of E is an element of K determined by a_1, a_3, a_2, a_4 and a_6. It has important properties as follows.

(j-1) Two elliptic curves are isomorphic (over $\overline{K}$) if and only if they have the same j-invariant.

(j-2) For any element $j_0 \in K$, there exists an elliptic curve defined over K with j-invariant equal to j_0. For example, if $j_0 \neq 0, 1728$, we let

$$E : y^2+xy = x^3 - 36/(j_0 -1728)x - 1/(j_0 - 1728).$$

Then j-invariant of E is j_0.

The Group Law

A group law is defined over the set of points of an elliptic curve (see Figure), and the set of points of an elliptic curve forms an abelian group. We denote the identity element ∞. After this, for $m \in Z$ and $P \in E$, we let

$mP = P+......+P$ (m terms) for $m > 0$,

$0P= \infty$,and

$mP= (-m)(-P)$ for $m < 0$.

The set of K-rational points on the elliptic curve E , denoted $E(K)$, is

$E(K)=\{(x,y)\in K^2 \mid y^2+ a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\infty\}$.

$E(K)$ is a subgroup of E and a finite abelian group. So we can define the descrete logarithm problem over it.

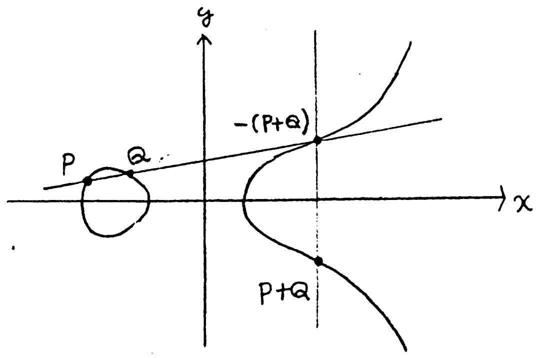

Figure: An elliptic curve over R.

Twist of *E/K*

A twist of *E/K* is an elliptic curve E'/K which is isomorphic to E over $\overline{K}$. We identify two twists if they are isomorphic over K.

Example Two elliptic curves *E/K* and E_1/K given below are twists each other.

$E : y^2 = x^3+ a_4x + a_6$

$E_1: y^2 = x^3+ a_4c^2x + a_6c^3$

($a_4,a_6 \in K$, c is any non-quadratic residue modulo p).

The Weil pairing

For an integer $m \geqq 0$, the m - torsion subgroup of E, denoted $E[m]$, is the set of points of order m in E,

$E[m]=\{ P\in E \mid mP = \infty \}$.

We fix an integer $m \geqq 2$, which is prime to $p=ch(K)$. Let μ_m be the subgroup of the mth roots of unity in $\overline{K}$.

The Weil e_m-Pairing is a pairing defined over $E[m]\times E[m]$

$e_m: E[m]\times E[m] \rightarrow \mu_m$.

For a definition of the Weil e_m-pairing, see [Sil]. We list some useful properties of Weil e_m-pairing.

For $E[m]\ni S, T, S_1, S_2, T_1, T_2$,

(e-1) Bilinear:

$e_m(S_1+S_2,T)=e_m(S_1,T)e_m(S_2,T)$

$e_m(S,T_1+T_2)=e_m(S,T_1)e_m(S,T_2)$;

(e-2) Alternating:

$e_m(S,T)=e_m(S,T)^{-1}$;

(e-3) Non-degenerate:

If $e_m(S,T)=1$ for all $S\in E[m]$,

then $T=\infty$;

(e-4) Identity

$e_m(S,S)=1$ for all $S \in E[m]$.

Number of Rational Points

We wish to estimate how many points there are in $E (K)$. The following Hasse's theorem gives a bound of the number of rational points of an elliptic curve.

Theorem ([Sil]) Let *E/K* be an elliptic curve . Then

$\mid \#E(K)-q-1 \mid \leqq 2q^{1/2}$.

Let $\#E(K)= q+1-a_q$. If $K=F_p$, we further have the next theorem by Deuring.

Theorem ([Deu]) Let a_p be any integer such that $\mid a_p \mid \leqq 2p^{1/2}$. Letting k(d) denote the Kronecker class number of d, there exist

$k(a_p^2\text{-}4p)$ elliptic curves over F_p with number of points $p+1-a_p$, up to isomorphisms.

3 Reducing EDLP to DLP in a finite field

In this section, we briefly describe the reducing method of EDLP via Weil pairing. For more information, see [MVO].

First we mention about EDLP.

EDLP([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.

Next we mention about embedding the subgroup $<P> \subset E(K)$ generated by a point P into the multiplicative group of a finite extension field of K. This embedding is constructed via Weil pairing. And it is the essence of the reducing method ([MVO]). In the following, we denote a finite field F_q by K and fix an elliptic curve E/K, a point $P \in E(K)$. We further assume that $o(P) = m$ is prime to $p=ch(K)$.

Embedding

Let Q be another point of order m such that $E[m]$ is generated by P, Q. Let K^r be an extension field of K containing μ_m. We can define a homomorphism

$$f : <P> \to K^{r*}$$

by setting

$$f(nP) = e_m(nP, Q).$$

From the definition of Weil pairing, it follows easily that f is an injective homomorphism from $<P>$ into K^{r*}. In fact, as $K^r \supset \mu_m$, the subgroup $<P>$ of E is a group isomorphism to the subgroup μ_m of K^{r*}.

Summary of the reducing method([MVO])

We summarize the reducing method of EDLP, which finds an integer x such that $R = xP$ for a given $R \in E(K)$, with th above embedding.

We can check in probablistic polynomia time whether $R \in <P>$ or not. So we assume that $R \in <P>$. Since m is prime to p, we can construct an injective homomorphism f from $<P>$ into K^{r*} as stated above. Then the problem is equal tc find an integer x such that $f(R) = x\,f(P)$ for a given $f(R), f(P) \in K^r$. In this way, we can reduce EDLP to DLP in an extension field K^r of K.

Note that this reducing is invalid if m is divisible by $p= ch(K)$ because the above injective homomorphism cannot be defined in the case. The next section investigates this case.

4 Inapplicable case

Definition Let E/F_q be an elliptic curve. If E has the properties

$$E[p^t]=\{\infty\} \quad \text{for all integer } t \geqq 1,$$

then we say that E is supersingular. Otherwise we say that E is ordinary.

Remark Let E be a supersingular elliptic curve. The definition of supersingular says that $o(T)$ is prime to $ch(K)=p$ for all $T \in E(K)$.

In the following, we denote a finite field F_q by K and fix an elliptic curve E/K, a point $P \in E(K)$. We further assume that $o(P) = m$ is divisible by $p= ch(K)$. From the above remark, it follows that E is ordinary. We will describe EDLP on such a point of an ordinary elliptic curve in the next two subsections.

4-1 Ordinary elliptic curves over F_{2^r}

In this subsection, we investigate the case of $q=2^r$. Let m be expressed by $m=2^tk$ (k is an integer prime to 2, t is a positive integer). And EDLP on E to the base P is finding an integer x such that R=xP for given $R \in E(K)$ (section 2).

As we assume that g.c.d(m,2)$\neq$ 1, we can't apply the reducing method ([MVO]) directly to this case. So we extend the reducing method [MVO] as follows.

The extended reducing method

If all of the prime factors of k are small, then we can solve this problem with Pohlig-Hellman's method ([Ko2]). So we assume that k has a large prime factor.

Let $P' = 2^tP$, $R' = 2^tR$. Then in probablistic polynomial time, we can check whether $R' \in < P' >$ or not ([MVO]). If $R' \notin < P' >$, then $R \notin < P >$. So we assume that $R' \in < P' >$. Since o(P') = k is prime to 2, we can apply the reducing method ([MVO]) to this case. Namely, we can work in a suitable extension field of K and find an integer x' such that R'=x'P'. Then we get $2^t(R-x'P)=\infty$. If we assume that $R \in <P>$, we get $(R-x'P) \in < P >$. From the group theory, it follows easily that a finite cyclic group $< P >$ has only one subgroup whose order devides m= #< P >. So we get $(R-x'P) \in <kP>$. Now we can change the base P of EDLP into kP, so we have only to find an integer x" such that R−x'P=x"(kP). Since #< kP > is 2^t, we can easily find an integer x" with Pohlig-Hellman's method ([Ko2]). So we can find an integer x by setting x ≡x' + x"k (modulo m) .

The above extended reducing method is summarized like this.

Condition : Find an integer x such that R=xP for given R ∈ $E(K)$. Let m be expressed by $m=2^tk$ (k is an integer prime to 2, t is a positive integer).

Method : (1)Find a non-trivial subgroup $< 2^tP > \subset < P >$ whose order is prime to p=ch(K).
(2)Embed $< 2^tP >$ into the multiplicative group of a suitable extension field of K via an injective homorphism constructed by Weil pairing.
(3)Change EDLP on E to the base P into EDLP on E to the base kP . (Since all of the prime factors of #< kP > are small, we can easily solve.)

The above discussion to add the result of [MVO] completes the proof of the following.

Theorem1 For any elliptic curve E/F_{2^r} and any point $P \in E(F_{2^r})$, we can solve EDLP on E (to the base P) by reducing it to DLP in a suitable extension field of F_{2^r} and (if necessary) changing the base P into kP whose order devides only by 2. (For extension degree, see [MVO], [Be-Sc])

Remark We proved Theorem1 for a field F_{2^r}. In the same way, we can prove the corresponding theorem for a field F_{p^r} if the prime p is so small that we can make p-1 tables of the discrete logarithm.

4-2 Ordinary elliptic curves over F_p

In this subsection, we investigate the case of q=p. Let p be a large prime and m be expressed by $m=p^t k$ (k is an integer prime to p, t is a positive integer). From Hasse's theorem (section 2), there is a bound of $\#E(K)$. So an integer m must satisfy that $(m-p-1)\leqq 2p^{1/2}$.

The next result is easy to prove.

Lemma Let p be a prime more than 7 and E/F_p be an ordinary elliptic curve. We assume there is a point $P\in E(K)$ whose order is divisible by p. Then a point P has exactly order p. Furthermore $E(K)$ is a cyclic group generated by P.

So we try to solve EDLP on the above ordinary elliptic curve, namely an elliptic curve generated by a point of order p. In this case, non-trivial subgroup of $E(K)$ is only itself and p is a large prime. So we cannot apply the extended reducing method in section 4-1 to it.

We assume that $E(K)=<P>$ can be embedding into the multiplicative group of a suitable extension field K^r of K via any way instead of Weil pairing. At this time we can reduce EDLP on E (to the base P) to DLP on K^r. But, for any integer r, there is no any subgroup of K^{r*}, whose order is p. So we cannot embed $<P>$ into the multiplicative group of any extension field of K.

The next result follows the above discussion.

Theorem2 For an elliptic curve E/F_p such that $\#E(F_p)=p$ and any point $P\neq\infty$ of $E(F_p)$, we cannot reduce EDLP on E (to the base P) to DLP in any extension field of F_p by embedding $<P>$ into the multiplicative group of it.

5 Constructing elliptic curves

In this section, we describe the method constructng elliptic curve E/F_p with elements.

In the following, let p be a large prime We get the next result by Hasse's theorem a Deuring's theorem (section2).

Lemma Let k (d) denote t Kronecker class number of d. There exist (1-4p) elliptic curves E/F_p with p element up to isomorphism.

Because of k (1-4p)$\geqq 1$, we get that the exists an elliptic curve E/F_p with p elements So we mention how to construct such an ellipt curve E/F_p. Original work concerning this was done by Deuring ([La2], [At-Mo], [Mo]). In the following, we explain the essence of hi work.

Let d be an integer such that $4p-1=b^2d$ (is an integer). Then there is a polynomial P_d(x called class polynomial. For a definition of th class polynomial, see [La2], [At-Mo].

The class polynomial $P_d(x)$ has th following properties.

(c-1) $P_d(x)$ is a monic polynomial with intege coefficients.

(c-2) The degree of $P_d(x)$ is the class number o an order O_d of an imaginary quadratic field. (For a definition of the order, see [Sil] and for the class number, see [La1].)

(c-3) $P_d(x)=0$ splits completely modulo p.

Let j_0 be a root of $P_d(x)=0$ (modulo p). Then j_0 gives the j-invariant of an elliptic curve E/F_p with p elements. So we make an elliptic curve E/F_p with j-invariant j_0 as we mentioned in section2, and one of twists of E/F_p is an elliptic curve with p elements.

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 $4p-1=b^2d$ (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 $P_d(x)$.

Procedure for constructing an elliptic curve

We can construct an elliptic curve by the following algorithm.

Algorithm

(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 $4p-1=b^2d$ for an integer b.

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

(p-4) Let $j_0 \in F_p$ be one of the roots of $P_d(x)=0$ (modulo 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 $X_t \neq \infty$ of $E_t(F_p)$ and calculate pX_t. If $pX_t = \infty$, then $E_t(F_p)$ has exactly p elements.

Remarks (1) In (p-7), we calculate p-multiple point in order to decide which twist of E/F_p has an order p. This follows the section 4-2.

(2) For a fixed integer d and any integer b, how many primes p satisfy the condition such that $4p-1=b^2d$? This is a problem to be solved.

Example We construct an elliptic curve by the above algorithm.

(p-1) Let d=19 then O_{19} has a class number 1.

(p-2) Let p=23520860746468351934891841623 then $4p-1=19*(1451*48496722383)^2$.

(p-3) Calculate a class polynomial $P_{19}(x)$ then we get $P_{19}(x)=x+884736$.

(p-4) Let $j_0 = -884736$.

(p-5) Let $E : y^2 = x^3 + a*x + b$ with
a=18569100589317119948598822307,
b= 9903520314302463972586038632.

(p-6) Twist of E/F_p is E_1, where E_1 is as following, $E_1 : y^2 = x^3 + a_1 * x + b_1$ with
a_1 = 18569100589317119948598822307
b_1 = 13617340432165887962305802991 .

(p-7) Let $E(F_p) \ni X$ be (1, 12834397719522088187599559212) and $E_1(F_p) \ni X_1$ be (0, 2251799813687456). Calculate pX, pX_1 and we get $pX = \infty$, $pX_1 \neq \infty$. So E/F_p has an order p.

Using the above E/F_p and X, we construct EDLP on E to the base X. Then up to the present, the best algorithms that are known for solving this problem are only the method of Pohlig-Hellman.

We end this section by the next conclusion.

Conclusion With the above algorithm, we can construct EDLP on E/F_p such that we cannot reduce it to DLP in any extension field.

6 Final remarks

For an ordinary elliptic curve E defined over F_p (p is a large prime), we showed in theorem 2 that there exists EDLP on E which cannot be reduced to DLP in any extension field of F_p by any embedding. What is the relation between such EDLP and DLP? It is an open problem to be solved. And which of such elliptic curve cryptosystems is good for the implementation? It is another problem to be considered.

7 Acknowledgements

I wish to thank Makoto Tatebayashi of Matsushita Electric Industrial Corporation for his helpful advice. I would like to thank Yoshihiko Yamamoto of Osaka University for his teaching me about the class polynomial. I am grateful to Francois Morain for sending me his paper [At-Mo]. I am also grateful to Tatsuaki Okamoto for sending me his paper [MVO].

References

[At-Mo] A. O. L. Atkin and F. Morain, "Elliptic curves and primality proving", Research Report 1256, INRIA, Juin 1990. Submitted to Math. Comp.

[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, 417-426.

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

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

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

[Ko2] N. Koblitz, "A course in Numb Theory and Cryptography", GTM11 Springer-Verlag, New York(1987).

[La1] S. Lang, "Algebraic Number Theory GTM110, Springer-Verlag, New York(1986).

[La2] S. Lang, "Elliptic Functions' Addison-Wesley, 1973.

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

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

[Mo] F. Morain, "Building cyclic elliptic curve modulo large primes", Abstracts fo Eurocrypto91 , Brighton, U.K. 160-164.

[MVO] A. Menezes, S. Vanstone and T. Okamoto, "Reducing elliptic curve logarithms to logarithms in a finite field", to appear in Proc. STOC'91.

[Sil] J. H. Silverman, "The Arithmetic of Elliptic Curves", GTM106, Springer-Verlag, New York, 1986

[SIS] H. Shizuya, T. Itoh and K. Sakurai, "On the Complexity of Hyperelliptic Discrete Logarithm Problem", SCIS91.

[Ta] T. Takagi, "Syotou seisuuronn kougi", Kyouritu Syuppan.