IEICE TRANS. FUNDAMENTALS, VOL. E76-A, NO. 1 JANUARY 1993

PAPER Special Section on Cryptography and Information Security

Elliptic Curve Cryptosystems Immune to Any Reduction into the Discrete Logarithm Problem

Atsuko MIYAJI†, *Member*

SUMMARY In 1990, Menezes, Okamoto and Vanstone proposed a method that reduces EDLP to DLP, which gave an impact on the security of cryptosystems based on EDLP. 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 to which we cannot apply the reducing. In this paper, we investigate the condition for which this reducing is invalid.

key words: *public-key, discrete logarithms, elliptic curves*

1. Introduction

Koblitz[7] and Miller[12] described how the group of points on an elliptic curve over a finite field can be used to construct public key cryptosystems. 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 square root attacks[15],[16]. Recently Menezes, Okamoto and Vanstone[13] proposed a noble method (the MOV reduction) 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. If EDLP on E/F_q is reduced to DLP in a small extension field of F_q, we must construct E over an enough large field to realize a secure cryptosystem. It is no good for the fast implementation. To achieve a secure and fast cryptosystem, Beth and Schaefer,[2] and Koblitz[9] discussed the case where the extension degree of a finite field, in which EDLP is reduced to DLP, is large enough.

The MOV reduction is constructed by a pairing, called the Weil pairing, defined over an m-torsion subgroup of an elliptic curve. If an elliptic curve is supersingular, the Weil pairing is defined over any m-torsion subgroup of it and we can apply the MOV reduction. On the other hand, if an elliptic curve is ordinary (non-supersingular), there exists an m-torsion subgroup on which the Weil pairing can't be defined. Our main motivation for this work is to study EDLP on such an m-torsion group of an ordinary elliptic curve.

Our result of this paper is the following.

- For any elliptic curve E defined over F_{2^r}, we can reduce EDLP on E to EDLP, to which the MOV reduction is applicable in an expected polynomial time (Theorem 3).
- For a certain ordinary elliptic curve E defined over F_p, there exists EDLP on E which makes any embedding to DLP in any extension field of F_p inapplicable (Theorem 4). Then such EDLP on E/F_p (p is a large prime) is secure enough for all known attacks.
- We give a procedure that enables us to construct such an elliptic curve in a practical time on a 32 bits personal computer.

After briefly reviewing some facts of the elliptic curves (Sect.2), we outline the MOV reduction (Sect.3). Section 4 studies the case where we cannot apply the MOV reduction and shows Theorem 3 and Theorem 4. Section 5 constructs ordinary elliptic curves E defined over any finite field F_p that makes reducing EDLP on E to DLP by embedding impossible.

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
$\bar{K}$: 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

2. Background on Elliptic Curves

We briefly describe some properties of elliptic curves[17] that we will use later. In the following, we denote a finite field F_q by K.

• The j-invariant

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

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

Manuscript received May 1, 1992.
Manuscript revised August 10, 1992.

† The author is with Matsushita Electric Industrial Co., Ltd., Kadoma-shi, 571 Japan.

The j-invariant of E, denoted $j(E)$, 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 $\bar{K}$) 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 and $ch(K) \geqq 5$, $j(E)$ equals j_0, where

$$E: y^2 = x^3 + \frac{3j_0}{1728 - j_0} x + \frac{2j_0}{1728 - j_0}. \qquad (1)$$

• The Group Law

A group law is defined over the set of points of an elliptic curve, and the set of points of an elliptic curve forms an abelian group. We denote the identity element $\mathcal{O}$. The set of K-rational points on the elliptic curve E, denoted $E(K)$, is the set

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

$E(K)$ is a subgroup of E and a finite abelian group. So we can define the discrete logarithm problem over it (Definition 1).

• Twist of E/K

A twist of E/K is an elliptic curve that is isomorphic to E over $\bar{K}$. We idntify two twists if they are isomorphic over K. The set of twists of E/K, modulo K-isomorphism, is denoted $Twist(E/K)$. If $ch(K) > 3$ and $j(E) \neq 0$, 1728, $Twist(E/K)$ is canonically isomorphic to K^*/K^{*2}.

Remark 1: Let $ch(K) > 3$ and $j(E) \neq 0$, 1728. Then two elliptic curves E/K and E_1/K given below are the representative elements of $Twist(E/K)$,

$$E: y^2 = x^3 + a_4x + a_6,$$
$$E_1: y^2 = x^3 + a_4c^2x + a_6c^3, \qquad (2)$$

where $c \in K^* \backslash K^{*2}$.

• 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,

$$E[m] = \{P \in E | mP = \mathcal{O}\}.$$

We fix an integer $m \geqq 2$, which is prime to $p = ch(K)$. Let μ_m be the subgroup of the m-th roots of unity in $\bar{K}$. The Weil e_m-Pairing is a pairing defined over $E[m] \times E[m]$

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

• Number of Rational Points

As for $\# E(K)$, the following Hasse's theorem gives a bound of the number of rational points on an elliptic curve.

Theorem 1: (Hasse) Let E/K be an elliptic curve. Then

$$|\# E(K) - q - 1| \leqq 2\sqrt{q}.$$

Let $\# E(K) = q + 1 - a_q$. If $K = F_p$, we further have the next theorem by Deuring.[5]

Theorem 2: (Deuring) Let a_p be any integer such that $|a_p| \leqq 2\sqrt{p}$. Letting $k(d)$ denote the Kronecker class number of d, there exist $k(a_p^2 - 4p)$ 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

We briefly describe the MOV reduction of EDLP via Weil pairing.[13] First we give the definition of EDLP.

Definition 1[8]: 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 such that $xP = R$ if such an integer x exists.

In the following, we denote a finite field F_q by K and fix an elliptic curve E/K and a point $P \in E(K)$. We further assume that $o(P) = m$ is prime to $p = ch(K)$.

The subgroup $\langle P \rangle \subset E(K)$ generated by a point P can be embedded into the multiplicative group of a finite extension field of K. This embedding is constructed via Weil pairing. It is the essence of the MOV reduction. We will mention about the embedding briefly.

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

$$f: \langle P \rangle \to K^{r*}$$

by setting

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

From the definition of Weil pairing, it follows easily that f is an injective homomorphism from $\langle P \rangle$ into K^{r*}. So the subgroup $\langle P \rangle$ of E is a group isomorphism to the subgroup μ_m of K^{r*}.

With the above homomorphism f, the MOV reduction reduces EDLP to DLP as follows. We can check whether $R \in \langle P \rangle$ or not in a probabilistic polynomial time. So we assume that $R \in \langle P \rangle$. Then the above injective homomorphism f from $\langle P \rangle$ into K^{r*} can change the problem, EDLP on E, to finding an integer x such that $f(R) = f(P)^x$ for a given $f(R)$, $f(P) \in K^r$, namely DLP on 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 2: Let E/F_q be an elliptic curve. If E has the properties $E[p^t]=\mathcal{O}$ for all integer $t\geqq 1$, then we say that E is supersingular. Otherwise we say that E is ordinary.

Remark 2: 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, where q is set large enough to be secure against the square root attacks, and fix an elliptic curve E/K and 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}

Let us see the case of $q=2^r$. Let m be expressed by $m=2^t k$ (k is an integer prime to 2, t is a positive integer). Then EDLP on E to the base P is finding an integer x such that $R=xP$ for given $R\in E(K)$ (Sect. 2). As we assume that g.c.d$(m, 2)+1$, we can't apply the MOV reduction directly to this case. So we extend the MOV reduction as follows.

Theorem 3: (The extended reducing method) For any elliptic curve E/F_{2^r} and any point $P\in E(F_{2^r})$, we can reduce EDLP on E (to the base P), in an expected polynomial time, to EDLP that we can apply the MOV reduction to and whose size is same as or less than the original EDLP.

Proof: We prove only the case whehe k has a large prime factor. Let $P'=2^tP$, $R'=2^tR$. Then in a probabilistic polynomial time, we can check whether $R'\in\langle P'\rangle$ or not Ref.(13). If $R'\notin\langle P'\rangle$, then $R\notin\langle P\rangle$. So we assume that $R'\in\langle P'\rangle$. Since $o(P')=k$ is prime to 2, we can apply the MOV reduction 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 $2^t(R-x'P)=\mathcal{O}$. If we assume that $R\in\langle P\rangle$, we get $(R-x'P)\in\langle P\rangle$. From the group theory, it follows easily that a finite cyclic group $\langle P\rangle$ has only one subgroup whose order divides $m=\#\langle P\rangle$. So we get $(R-x'P)\in\langle kP\rangle$. Now we change the base P of EDLP into kP, then we have only to find an integer x'' such that $R-x'P=x''(kP)$. Since $\#\langle kP\rangle$ is 2^t, we can easily find an integer x'' with Pohlig-Hellman's method.[8] So we can find an integer x by setting $x\equiv x'+x''k \pmod m$. □

We summarize the extended reducing method as follows.

step 1: Find a non-trivial subgroup $\langle 2^tP\rangle\subset\langle P\rangle$ whose order is prime to $2=ch(K)$.

step 2: Embed $\langle 2^tP\rangle$ into the multiplicative group of a suitable extension field of K via an injective homomorphism constructed by Weil pairing.

step 3: Change EDLP on E to the base P into EDLP on E to the base kP. (Since all of the prime factors of $\#\langle kP\rangle$ are small, we can easily solve such EDLP.)

Remark 3: We proved Theorem 3 for a field F_{2^r}. We can extend the theorem to a field F_{p^r} if we can generate tables of the discrete logarithm in a polynomial time in the element size.

4. 2 Ordinary Elliptic Curves Over F_p

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

The next lemma is easy to prove.

Lemma 1: Let p be a prime more than 7 and E/F_p be an ordinary elliptic curve. We assume that there is a point $P\in E(K)$ whose order is divisible by p. Then the point P has exactly order p. Furthermore $E(K)$ is a cyclic group generated by P.

Lemma 1 says that non-trivial subgroup of $E(K)$ is only itself. So we cannot apply the extended reducing method in Sect.4.1 to EDLP on E. We assume that $E(K)=\langle P\rangle$ can be embedded 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 case P) to DLP on K^r. But, for any integer r, there isn't any subgroup of K^{r*}, whose order is p. So we cannot embed $\langle P\rangle$ into the multiplicative group of any extension field of K.

The next theorem follows the above discussion.

Theorem 4: For an elliptic curve E/F_p such that $\#E(F_p)=p$ and any point $P\neq\mathcal{O}$ of $E(F_p)$, we cannot reduce EDLP on E (to the base P) to DLP in any extension field F_{p^r} of F_p by any embedding $\langle P\rangle$ into the multiplicative group of F_{p^r}. □

5. Constructing Elliptic Curves

In this section, we describe the method of constructing elliptic curve E/F_p with p elements of Theorem 4. In the following, let p be a large prime. We get the next result by Hasse's theorem and Deuring's theorem (Sect.2).

Lemma 2: Let $k(d)$ denote the Kronecker class number of d. There exist $k(1-4p)$ elliptic curves E/F_p with p elements, up to isomorphism. □

Because of $k(1-4p)\geqq 1$, we get that there exists at least one elliptic curve E/F_p with p elements for any given prime p. Now we mention how to construct such an elliptic curve E/F_p generally. Original work concerning this was done by Deuring.[11],[1]

Let d be an integer such that $4p-1=b^2d$ (b is an

integer). Then there is a polynomial $P_d(x)$ called class polynomial.[11] The class polynomial $P_d(x)$ has the following properties.

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

(c-2) The degree of $P_d(x)$ equals the class number of an order O_d of an imaginary quadratic field. (For a definition of the order, see Ref.(17) and for the class number, see Ref.(10).)

(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. For any elliptic curve, there are at most six twists modulo F_p-isomorphism and one of them is just an elliptic curve with p elements. Next we discuss how to find such a curve among all twists in a practical way.

For each twist E_t of E/F_p with j-invariant j_0, fix arbitrary 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. This follows Sect. 4.2. So we can decide which of the at most 6 twists of E/F_p has an order p in a polynomial time of the element size.

Now we get the following procedure to construct such an elliptic curve.

Procedure

(p-1) Choose an integer d.

(p-2) Search 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) Find a root $j_0 \in F_p$ of $P_d(x) \equiv 0 \pmod p$.

(p-5) Construct an elliptic curve E/F_p with j-invariant j_0 by (1).

(p-6) Construct all twists of E/F_p by (2).

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

In step (p-1), we can choose an integer d such that O_d has a small class number from a list.[18] This is because the degree of $P_d(x)$ becomes small and we can construct $P_d(x)$ easily. Table 1 lists some examples of d and a root of $P_d(x)$ whose degree equals 1. If we use d in Table 1 for the step (p-1), there are only two twists in the step (p-6). So in the step (p-7) we have only to calculate pX_t for one twist E_t. If $pX_t=\mathcal{O}$, then $E_t(F_p)$ has exactly p elements. If not, then the other has exactly p elements.

In step (p-3), we need a prime $p=(b^2d+1)/4$. There is a conjecture that there are infinitely many primes $p=(b^2d+1)/4$.[6]

Table 1 Integers d and the root j of $P_d(x)=0 \pmod p$.

d	j
11	$(-2^5)^3$
19	$(-2^5*3)^3$
43	$(-2^6*3*5)^3$
67	$(-2^5*3*5*11)^3$
163	$(-2^6*3*5*23*29)^3$

In order to make EDLP on E/F_p insolvable by the square root attacks, the prime p must be more than 30 digits. For this range of p, the procedure enables us to construct such an elliptic curve in a practical time on a 32 bit personal computer. We show an example for the case $d=163$.

Example ($d=163$)

(p-2) With a deterministic primality test,[3],[4] we search a prime represented by

$$4p-1=163 * b^2$$

for an integer b. As a result, we get

$$p=1000000000000888501978955285 71,$$

$$4p-1=163 * 49537740461829^2.$$

(p-5) Using Eq.(1), we get

$$E: y^2=x^3+a * x+b$$

with

$$a=695398375530858856440294407 81,$$

$$b=218021029362593423479110852 54.$$

(p-6) Using Eq.(2), we get the twist E_1 of E/F_p,

$$E_1: y^2=x^3+a_1 * x+b_1$$

with

$$a_1=435316280575131977978239227 59,$$

$$b_1=635877365577786970313712523 31.$$

(p-7) Let $E(F_p) \ni X=(x_0, y_0)$ and

$E_1(F_p) \ni X_1=(x_1, y_1)$ where

$$x_0=0,$$

$$y_0=129719387051917083519003545 86,$$

$$x_1=272295868705069338357958923 72,$$

$$y_1=770215841726736966061910910 4.$$

Calculate pX, pX_1 and we get

$$pX_1=\mathcal{O}, pX \neq \mathcal{O}.$$

So E_1/F_p, generated by X_1, has an order p.

Using the above E_1/F_p and X_1, we construct EDLP on E_1 to the base X_1. Then up to the present, it is secure for all considerable attacks. We implemented the procedure to construct such elliptic curves E_1/F_p on a 32 bit personal computer (20 MHz). It took the average 59.9 seconds to construct such E_1/F_p in the range of $p \in [10^{29}, 4 * 10^{29}]$. We found the running time of the procedure is dominated by the step (p-2). If we use a probabilistic primality test[14] in the step (p-2), the running time would be faster.

For other cases of d, we could construct such elliptic curves in 65.2~83.2 seconds. The difference in

the running time for the different integer d should be further investigated.

6. Conclusion

We have clarified the condition for which the MOV reduction is invalid. For a small prime p, we have proved that we can reduce EDLP on E/F_{p^r}, in an expected polynomial time, to EDLP that we can apply the MOV reduction to and whose size is same as or less than the original EDLP (theorem 3). For a large p, we have proved that EDLP on E/F_p cannot be reduced to DLP in any extension field of F_p by any embedding (theorem 4). We have also given a procedure to construct an elliptic curve in the sense of theorem 4. With the procedure we have shown we can construct an elliptic curve E/F_p that can be used for secure cryptosystems in a practical time on a 32 bits computer.

Acknowledgements

The author would like to thank Makoto Tatebayashi for his helpful advice. The author expresses my gratitude to Yoshihiko Yamamoto for his teaching me about the class polynomial. The author also wishes to thank the anonymous refrees for their valuable comments.

References

(1) Atkin, A. O. L. and Morain, F., "Elliptic curves and primality proving," *Research Report 1256, INRIA,* Juin 1990. Submitted to Math. Comp., 1990.
(2) Beth, T. and Schaefer, F., "Non supersingular elliptic curves for public key cryptosystems," *Advances in Cryptology-Proc. of EUROCRYT '91* Lecture Notes in Computer Science, 547, Springer-Verlag, pp. 316-327, 1991.
(3) Cohen, H. and Lenstra, Jr., H. W., "Primality testing and jacobi sums," *Mathematics of computation*, vol. 42, pp. 297-330, 1984.
(4) Cohen, H. and Lenstra, Jr., H. W., "Implementation of a new primality test," *Mathematics of computation*, vol. 48, pp. 103-121, 1987.
(5) Deuring, M., "Die Typen der Multiplikatorenringe elliptischer Funktionenkorper," *Abh. Math. Sem. Hamburg*, vol. 14, pp. 197-272, 1941.
(6) Hardy G. and Wright, E., *An Introduction to the Theory of Numbers,* Oxford Univ. Press, 1960.
(7) Koblitz, N., "Elliptic curve cryptosystems," *Math. Comp.,* vol. 48, pp. 203-209, 1987.
(8) Koblitz, N., *A course in Number Theory and Cryptography*, GTM114, Springer-Verlag, New York, 1987.
(9) Koblitz, N., "Cm-curves with good cryptographic properties," *Advances in Cryptology-Proc. of CRYPTO '91,* Lecture Notes in Computer Science, 576, Springer-Verlag, pp. 279-287, 1992.
(10) Lang, S., *Algebraic Number Theory*, GTM110, Springer-Verlag, New York (1986).
(11) Lang, S., *Elliptic Functions,* GTM112, Springer-Verlag, New York, 1987.
(12) Miller, V. S., "Use of elliptic curves in cryptography," *Advances in Cryptology-Proceedings of Crypto '85*, Lecture Notes in Computer Science, 218, Springer-Verlag, pp. 417-426, 1986.
(13) Menezes, A., Okamoto, T. and Vanstone, S., "Reducing elliptic curve logarithms to logarithms in a finite field," *Proc. of the 22nd Annual ACM Symposium on The Theory of Computing*, pp. 80-89, 1991.
(14) Rabin, M. O., "Probabilistic algorithms," in *Algorithms and complexity-new directions and recent results,* ed. J. F. Traub, Academic Press, 1976.
(15) Pohlig, S. and Hellman, M., "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance," *IEEE Trans. Inf. Theory,* vol. 24, pp. 106-110, 1978.
(16) Pollard, J., "Monte Carlo methods for index computation (mod p)," *Mathematics of Computation,* vol. 32, pp. 918-924, 1978.
(17) Silverman, J. H., *The Arithmetic of Elliptic Curves*, GTM106, Springer-Verlag, New York, 1986.
(18) Takagi, T., *Syotou seisuuronn kougi*, Kyouritu Syuppan, 1971.

Atsuko Miyaji was born in Osaka, Japan, in 1965. She received the B.Sc. and the M.Sc. degrees in mathematics from Osaka University, Osaka, Japan in 1988 and 1990, respectively. Since 1990, she has been with Communication Systems Research Laboratory in Matsushita Electric Industrial Co., Ltd. and engaged in research for secure communication. Her research interest includes the application of projective varieties theory into cryptosystems.