LETTER *Special Section on Discrete Mathematics and Its Applications*

A Remark on the MOV Algorithm for Non-supersingular Elliptic Curves

Taiichi SAITO[†a)] ***and*** **Shigenori UCHIYAMA**[††], ***Regular Members***

SUMMARY In recent years, the study of the security of Elliptic Curve Cryptosystems (ECCs) have been received much attention. The MOV algorithm, which reduces the elliptic curve discrete log problem (ECDLP) to the discrete log problem in finite fields with the Weil pairing, is a representative attack on ECCs. Recently Kanayama et al. observed a realization of the MOV algorithm for non-supersingular elliptic curves under the weakest condition. Shikata et al. independently considered a realization of the MOV algorithm for non-supersingular elliptic curves and proposed a generalization of the MOV algorithm. This short note explicitly shows that, under a usual cryptographical condition, we can apply the MOV algorithm to non-supersingular elliptic curves by using the multiplication by constant maps as in the case of supersingular. Namely, it is explicitly showed that we don't need such a generalization in order to realize the MOV algorithm for non-supersingular elliptic curves under a usual cryptographical condition.

key words: *elliptic curve discrete logarithm problem, MOV algorithm*

1. Introduction

In recent years, the study of the security of Elliptic Curve Cryptosystems (ECCs) have been received much attention. In [4], Menezes, Okamoto and Vanstone proposed an algorithm (MOV algorithm) for reducing the elliptic curve discrete log problem (ECDLP) to the discrete log problem in a finite field with the Weil pairing, and explicitly showed that the algorithm is effective for supersingular elliptic curves. Namely, it is a subexponential time algorithm for supersingular elliptic curves. Furthermore, Frey and Ručk [1] generalized this for any algebraic curve by using the Tate pairing.

Recently Kanayama et al. [2] observed a realization of the MOV algorithm for non-supersingular elliptic curves under the weakest condition. Shikata et al. [7] independently studied a realization of the MOV algorithm for non-supersingular elliptic curves and proposed a generalization of the MOV algorithm. But they did not consider the application of the MOV algorithm to all non-supersingular elliptic curves in [7]. Actually, Lemma 1 in [7] does not hold in general. Very recently, [8] studied the group structures of the points on non-supersingular elliptic curves and presented a different algorithm in order to correct the result in [7]. Although, it must be very important result from a computational view point, it is obvious that in order to realize the MOV algorithm for non-supersingular elliptic curves, one does not need such a consideration of the group structures of the points on non-supersingular elliptic curves from the result in [2].

This short note explicitly shows that, under a usual cryptographical condition, we can apply the MOV algorithm to non-supersingular elliptic curves by using the multiplication by constant maps as in the case of supersingular. Namely, it is showed that one does not need a generalization in order to realize the MOV algorithm for non-supersingular elliptic curves under a usual cryptographical condition. Note that this result has been already briefly mentioned in [2], and presented in [5], although, since our below discussion is slightly different and simpler than that in [5], this short note would explicitly introduce it*.

First we define the elliptic curve discrete log problem over E.

Definition 1.1: Let E be an elliptic curve over a finite field $\mathbf{F}_q$, $P \in E(\mathbf{F}_q)$ a point of order l, and $Q \in E(\mathbf{F}_q)$. Given E, P and Q, the elliptic curve discrete logarithm problem over E is to find the unique integer m $(0 \leq m < l)$ such that $Q = [m]P$, if such an integer exists.

From now on, we assume that l is an odd prime number such that $\#E(\mathbf{F}_q) = lv$, where $l \sim \#E(\mathbf{F}_q)$, $\gcd(l, v) = 1$ and $Q \in \langle P \rangle$ from the cryptographical standpoint. In the case that $l \mid q$, we can employ the SSSA algorithm to compute the discrete logarithm. Thus, we also assume that $l \nmid q$.

2. The MOV Algorithm

In [4], Menezes, Okamoto and Vanstone proposed the following algorithm for reducing the ECDLP to the discrete log problem in a finite field with the Weil pairing e_l.

Algorithm 1 ([4])

[Input] An element $P \in E(\mathbf{F}_q)$ of order l, and $Q \in \langle P \rangle$.

Manuscript received August 31, 2000.

[†]The author is with Telecommunications Advancement Organization of Japan, Yokohama-shi, 221-0031 Japan.

[††]The author is with NTT Laboratories, Yokosuka-shi, 239-0847 Japan.

a) E-mail: taiichi@sucada.isl.ntt.co.jp

*The discussion described in this paper is essentially the same as that in [6]. Because the proceedings of [6] may not be widely distributed, we would like to describe it again.

[**Output**] An integer m $(0 \leq m < l)$ such that $[m]P = Q$.

[**Step 1**] Determine the smallest integer k such that $E[l] \subset E(\mathbf{F}_{q^k})$.
[**Step 2**] Find $S \in E[l]$ such that $\alpha = e_l(P, S)$ has order l.
[**Step 3**] Compute $\beta = e_l(Q, S)$.
[**Step 4**] Compute m, the discrete logarithm of β to the base α in $\mathbf{F}_{q^k}$.

In [4], for supersingular elliptic curves, they determined the extension degree k such that $E[l] \subset E(\mathbf{F}_{q^k})$ (**Step 1**) and the group structure of $E(\mathbf{F}_{q^k})$, and explicitly proposed the method for finding the point S in **Step 2**.

Namely, we have to consider **Step 1** and **2** in order to realize **Algorithm 1** for non-supersingular elliptic curves.

For the determining extension degree k such that $E[l] \subset E(\mathbf{F}_{q^k})$ for any elliptic curve, we can easily determine it by using **Theorem 2.3** in [10]. Here we note that the extension degree k is exponential in $\log q$ in the case of $l|(q-1)$.

So, the next section studies the action of the Frobenius on the Tate module and discusses a method for finding the point S in **Step 2** in the case of $l \not|(q-1)$.

3. The Action of the Frobenius on the Tate Module

This section studies the action of the Frobenius on the Tate module and proposes a method for finding a point S in $E[l]$ where $e_l(P, S)$ has order l, in the case of $l \not|(q-1)$.

This section's theoretical background can be found in [9].

Since $l^2 \not| \#E(\mathbf{F}_q)$ and $l \not|(q-1)$, an l-adic representation of the q^{th}-Frobenius endomorphism ϕ on-the Tate module $T_l(E)$ has two distinct eigenvalues λ_1, λ_2 in the l-adic integers such that $\lambda_1 \equiv 1$, $\lambda_2 \equiv q \pmod{l}$.

Thus, the Tate module $T_l(E)$ has a decomposition

$$T_l(E) = T_{\lambda_1} \oplus T_{\lambda_2},$$

where T_{λ_1}, T_{λ_2} correspond to eigenvalues λ_1, λ_2, respectively.

This implies that the i-th component of Tate module, $E[l^i]$, can be decomposed as

$$E[l^i] = (T_{\lambda_1})_i \oplus (T_{\lambda_2})_i,$$

where $(T_{\lambda_1})_i$, $(T_{\lambda_2})_i$ denote the i-th components of T_{λ_1}, T_{λ_2}, respectively. We note that $(T_{\lambda_1})_i$ and $(T_{\lambda_2})_i$ are cyclic groups with l^i elements.

Here, we consider the action of ϕ on $(T_{\lambda_1})_2$. It is easy to see that this action can be identified as the multiplication by λ_1 mod l^2. Also we can set $\lambda_1 \equiv 1 + al \pmod{l^2}$, where a is an integer with $l \not| a$. So we have $\lambda_1^l \equiv (1+al)^l \equiv 1 \pmod{l^2}$. Namely, the points in $(T_{\lambda_1})_2$ are $\mathbf{F}_{q^l}$-rational.

Thus we can couclude that when we determine the minimum extension degree k satisfying that $q^k \equiv 1 \pmod{l}$ by **Theorem 2.3** in [10], we have

$$E(\mathbf{F}_{q^k}) \cap (T_{\lambda_1})_i = \langle P \rangle \text{ for any } i$$

since $k|(l-1)$.

[3] considered the case that, in the l-part of $E(\mathbf{F}_{q^k})$, there exits a cyclic group which contains $\langle P \rangle$, and the cardinality of the cyclic group is divisible by l^2. It also pointed out the difficulty of finding the suitable point for computing non-degenerate pairing in the case above. Although, based on the above consideration, we can conclude that such a case never occurs under the usual cryptographical condition $l^2 \not| \#E(\mathbf{F}_q)$.

Now we describe the method for finding the point S in $E[l]$ where $e_l(P, S)$ has order l, in the case of $l \not|(q-1)$.

Let k be the minimum integer such that $l|(q^k-1)$. Note that $E[l] \subset E(\mathbf{F}_{q^k})$ by **Theorem 2.3**.

Let n be the cardinality of $E(\mathbf{F}_{q^k})$ and e the maximum integer such that l^e divides n.

Algorithm 2

[**Input**] E, P, l as in **Algorithm 1**. The minimum integer k such that $l|(q^k-1)$ and the cardinality n of $E(\mathbf{F}_{q^k})$ and the maximum integer e such that l^e divides n.
[**Output**] A point S such that $\alpha = e_l(P, S)$ has order l.

[**Step 1**] Choose any point $Q \in E(\mathbf{F}_{q^k})$, and compute $Q' = [n/l^e]Q$. If $Q' \in \langle P \rangle$ goto **Step 1**.
[**Step 2**] Find the minimum integer j such that $[l^j]Q' = \mathcal{O}$, and output $S = [l^{j-1}]Q'$.

We examine the correctness and complexity of **Algorithm 2**.

In **Step 1**, we can pick points Q uniformly and randomly on $E(\mathbf{F}_{q^k})$ in probabilistic polynomial time of $\log q^k$ (see [4]), so the points $Q' = [n/l^e]Q$ are uniformly distributed about the l-partof $E(\mathbf{F}_{q^k})$.

By properties of the Weil pairing, it is easy to see that if $Q' \notin \langle P \rangle$ then $e_l(P, S)$ has order l. Because the l-part of $E(\mathbf{F}_{q^k})$ is decomposed as

$$\langle P \rangle \oplus (T_{\lambda_2})_i$$

with some i, the probability that $Q' \in \langle P \rangle$ is

$$\frac{\#\langle P \rangle}{\#\langle P \rangle \times \#(T_{\lambda_2})_i},$$

which is less than $1/l$. Then we can find Q' such that $Q' \notin \langle P \rangle$ with the probability more than $1 - 1/l$.

Thus, if k has a boundness of polynomial of $\log q$, we can find the point S in $E[l]$ such that $e_l(P, S)$ has order l in probabilistic polynomial time of $\log q$.

Here we note that **Algorithm 2** is essentially the same as the proposed algorithm for supersingular elliptic curves in [4]. So, we can conclude that, when the extension degree k is sufficiently small, the original MOV algorithm can be effectively applied to non-supersingular elliptic curves under the usual cryptographical conditon $l^2 \not| \# E(\mathbf{F}_q)$.

4. Conclusion

This short note explicitly showed that, under a usual cryptographical condition, we can apply the MOV algorithm to non-supersingular elliptic curves by using the multiplication by constant maps as in the case of supersingular. Namely, it has been showed that one does not need a generalization in order to realize the MOV algorithm for non-supersingular elliptic curves under a usual cryptographical condition. Note that this result has been already briefly mentioned in [2] and presented in [5], although, since our discussion presented in this paper was slightly different and simpler than that in [5], this short note would explicitly introduced it.

References

[1] G. Frey and H.G. Rück, “A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves,” Math. Comp., vol.62, no.206, pp.865–874, 1994.

[2] N. Kanayama, T. Kobayashi, T. Saito, and S. Uchiyama, “Remarks on elliptic curve discrete logarithm problems,” IEICE Trans. Fundamentals, vol.E83-A, no.1, pp.17–23, Jan. 2000.

[3] R. Harasawa, J. Shikata, J. Suzuki, and H. Imai, “Comparing the MOV and FR reductions in elliptic curve cryptography,” Proc. Eurocrypt’99, LNCS 1592, pp.190–205, Springer-Verlag, 1999.

[4] A. Menezes, T. Okamoto, and S. Vanstone, “Reducing elliptic curve logarithms to logarithms in a finite field,” IEEE Trans. Inf. Theory, vol.39, no.5, pp.1639–1646, 1993.

[5] T. Saito and S. Uchiyama, “A remark on the MOV algorithm,” IEICE Technical Report, ISEC99-27, 1999.

[6] T. Saito and S. Uchiyama, “A remark on the MOV algorithm,” IEICE Society-Taikai, 1999.

[7] J. Shikata, Y. Zheng, J. Suzuki, and H. Imai, “Optimizing the Menezes-Okamoto-Vanstone (MOV) algorithm for non-supersingular elliptic curves,” Proc. Asiacrypto’99, LNCS 1716, pp.86–102, Springer-Verlag, 1999.

[8] J. Shikata, Y. Zheng, J. Suzuki, and H. Imai, “Realizing the MOV algorithm for non-supersingular elliptic curves (2),” IEICE Technical Report, ISEC99-58, 1999.

[9] J.H. Silverman, The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, 1986.

[10] S. Uchiyama and T. Saitoh, “A note on the discrete logarithm problem on elliptic curves of trace two,” IEICE Technical Report, ISEC98-27, 1998.