PAPER

Realizing the Menezes-Okamoto-Vanstone (MOV) Reduction Efficiently for Ordinary Elliptic Curves

Junji SHIKATA[†], **Yuliang ZHENG**[††], ***Nonmembers***, **Joe SUZUKI**[†], ***and*** **Hideki IMAI**[†††], ***Members***

SUMMARY The problem we consider in this paper is whether the Menezes-Okamoto-Vanstone (MOV) reduction for attacking elliptic curve cryptosystems can be realized for genera elliptic curves. In realizing the MOV reduction, the base field $\boldsymbol{F}_q$ is extended so that the reduction to the discrete logarithm problem in a finite field is possible. Recent results by Balasubramanian and Koblitz suggest that, if $l \not| q-1$, such a minimum extension degree is the minimum k such that $l|q^k-1$, which is equivalent to the condition under which the Frey-Rück (FR) reduction can be applied, where l is the order of the group in the elliptic curve discrete logarithm problem. Our point is that the problem of finding an l-torsion point required in evaluating the Weil pairing should be considered as well from an algorithmic point of view. In this paper, we actually propose a method which leads to a solution of the problem. In addition, our contribution allows us to draw the conclusion that the MOV reduction is indeed as powerful as the FR reduction under $l \not| q-1$ not only from the viewpoint of the minimum extension degrees but also from that of the effectiveness of algorithms.

key words: *elliptic curve cryptography, elliptic curve discrete logarithm problem, Menezes-Okamoto-Vanstone (MOV) algorithm, supersingular elliptic curves, ordinary elliptic curves*

1. Introduction

Let E be an elliptic curve defined by

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (a_1, a_2, a_3, a_4, a_6 \in \boldsymbol{F}_q),$$

where $\boldsymbol{F}_q$ is a finite field with $q = p^m$ (p : a prime number) elements. The Elliptic Curve Discrete Logarithm Problem (ECDLP) asks: given a base point $P \in E(\boldsymbol{F}_q)$ and $R \in \langle P \rangle$, find an integer n such that $R = [n]P$, where $E(\boldsymbol{F}_q)$ is the set of its $\boldsymbol{F}_q$-rational points.

In 1985, N. Koblitz [12] and V. Miller [18] independently proposed the use of elliptic curves over finite fields for public-key cryptography, based on the presumed intractability of the ECDLP. Since that time, elliptic curve cryptosystems have gained a tremendous amount of attention. The main reason is that they have two potential advantages over the conventional systems: the great diversity of elliptic curves available to provide the groups; and the absence of subexponential time algorithms such as index calculus type that can find discrete logarithms in these groups. (For example, see [29].)

Of the developments in elliptic curve cryptography, the most dramatic was the demonstration by A. Menezes, T. Okamoto and S. Vanstone [17] in 1991 that the ECDLP on a so-called supersingular elliptic curve can be reduced to the Discrete Logarithm Problem (DLP) in the multiplicative subgroup of a finite field (MOV reduction). This result means that one should avoid the set of supersingular curves if one wants to have a secure cryptosystem. (After the MOV reduction appeared, several attacks against the ECDLP have been proposed thus far: G. Frey and H.G. Rück [8] devised a reduction of the ECDLP to the DLP in the multiplicative subgroup of a finite field that can be applied under a certain condition (FR reduction); and I. Semaev [26], N. Smart [30], T. Satoh and K. Araki [22] independently announced reductions of the ECDLP to the DLP of the additive group structure of the base field for so-called anomalous curves.)

In this paper, we raise a natural and important question: can the MOV reduction be realized for general elliptic curves ? We solve this problem in the affirmative from an algorithmic point of view.

In the following discussion, we assume that $l = \#\langle P \rangle$ is a prime number, which is not restrictive since we can reduce the composite case to the prime one by applying the Chinese Remainder Theorem and the Pohlig-Hellman algorithm. Moreover, we assume that $l \not| q$ since the l-part DLP is solved by the obvious extension of [22], [26], [30] in polynomial time when $l|q$.

Before we see how hard the problem is, let us briefly review how the MOV reduction works [16], [17]. The idea is to find the minimum extension degree k such that $E[l] \subset E(\boldsymbol{F}_{q^k})$, where $E[l]$ is the set of l-torsion points, i.e. $\{T \in E | [l]T = O\}$. Then, the group isomorphism $\langle P \rangle \to \mu_l \subset \boldsymbol{F}_{q^k}$ defined by $S \mapsto e_l(S, Q)$ is available if we can find a point $Q \in E[l]$ such that $e_l(P, Q)$ is a generator of μ_l, where $e_l : E[l] \times E[l] \to \mu_l$ is the Weil pairing [28], and μ_l is the multiplicative group of l-th roots of unity. Thus, we can successfully reduce the ECDLP to the DLP in a finite field.

In particular, for supersingular elliptic curves,

Manuscript received May 25, 1999.
Manuscript revised September 1, 1999.

[†]The authors are with the Graduate School of Science, Osaka University, Toyonaka-shi, 560-0043 Japan.
[††]The author is with the Faculty of Information Technology, Monash University, Melbourne, Victoria 3199, Australia.
[†††]The author is with the Institute of Industrial Science, the University of Tokyo, Tokyo, 106-8558 Japan.

Menezes, Okamoto, and Vanstone

1. showed that such a k is at most six; and
2. constructed a method to find such a Q in probabilistic polynomial time in $k \log q$ ($k \leq 6$).

Therefore, those facts lead to the realization of the reduction that works in probabilistic polynomial time in $k \log q$ ($k \leq 6$) for supersingular elliptic curves, and consequently the MOV algorithm is completed in probabilistic subexponential time in $\log q$ for supersingular elliptic curves.

However, there exist two major problems to be clear, from an algorithmic point of view, in applying the MOV reduction to general elliptic curves (assuming that $l = \#\langle P \rangle$ is a prime number and $l \not| q$):

1. the problem of explicitly determining the minimum positive integer k such that $E[l] \subset E(\boldsymbol{F}_{q^k})$.
2. the problem of efficiently finding an l-torsion point Q such that $e_l(P, Q)$ has order l. (i.e. $e_l(P, Q) \neq 1$ because of the assumption that l is a prime number. In the sequel, we refer to such an l-torsion point Q as a "good" l-torsion point.)

For the first problem, we can find an answer to it in a recent paper by Balasubramanian and Koblitz [3]. They proved that if $l \not| q-1$, k is the minimum positive integer such that $q^k \equiv 1 \bmod l$. (It is interesting to note that this condition is identical to the one under which the FR reduction is applied.) In the same paper, they also suggest that we need $k = l$ if $l | q - 1$ and $E[l] \not\subset E(\boldsymbol{F}_q)$. Thus, when l is much larger than $\log q$, we may give up applying the MOV reduction since the extension degree in this case is too large in order for the reduced DLP in $\boldsymbol{F}^*_{q^k}$ to be solved in subexponential time in $\log q$.

For the second problem, we cannot find any answer which covers all the case in open literatures: we need some assumptions in order for currently known methods [10], [17] to work efficiently even if k is small. Thus, an efficient method which solve the second problem for the general case will be desired from mathematical and algorithmic points of view.

The major contribution of this paper is to solve the second problem described above by actually proposing a method that efficiently finds a "good" l-torsion point for ordinary (non-supersingular) elliptic curves (see [17] for supersingular elliptic curves). The proposed method is completed in probabilistic polynomial time in $k \log q$, more precisely $O(k^3 \log^3 q)$ if $\#E(\boldsymbol{F}_q)$ is given beforehand and otherwise $O(k^3 \log^3 q + \log^6 q)$, where k is the minimum positive integer with $q^k \equiv 1 \bmod l$. The running time seems to be asymptotically optimal, since it is equal to that of randomly picking a point in $E(\boldsymbol{F}_{q^k})$, which seems to be needed in any situation, except for computing $\#E(\boldsymbol{F}_q)$. Also, our method is completed in probabilistic polynomial time in $\log q$ whenever k is small enough to solve the DLP in $\boldsymbol{F}^*_{q^k}$ in subexponential time in $\log q$. As a result, we can successfully realize the MOV reduction for the general case, in a true sense.

Now, we turn our attention to comparing the MOV and FR reductions. It may have been believed by some cryptographers that assuming $l \not| q - 1$, the MOV reduction is as powerful as the FR reduction in the sense that their minimum extension degrees k coincide when the base field $\boldsymbol{F}_q$ is extended to $\boldsymbol{F}_{q^k}$ in order to apply those reductions. However, so far there has been a lack of a formal proof that supports the belief. As pointed out in [10], the problem of efficiently finding an l-torsion point required in evaluating the Weil pairing should be solved as well for the general case. Thus, our contribution allows us to finally draw the conclusion that the MOV reduction is indeed as powerful as the FR reduction under $l \not| q - 1$, in a true sense: not only from the viewpoint of the minimum extension degrees of the base field but also from that of the effectiveness of algorithms.

The rest of this paper is organized as follows: In Sect. 2, we briefly review some basic facts on elliptic curves over finite fields, the MOV algorithm and the answer to the first problem obtained by Balasubramanian and Koblitz. In Sect. 3, we actually propose a method for finding a "good" l-torsion point, which leads to the solution of the second problem. It turns out that the proposed method is completed in probabilistic polynomial time in $k \log q$ under $l \not| q - 1$.

2. Preliminaries

In this section, we briefly review some materials on elliptic curves over finite fields. (See [28] for more details.)

Let $\boldsymbol{F}_q$ be a finite field with q elements and of characteristic p, and $\bar{\boldsymbol{F}}_q$ its algebraic closure. Let E be an elliptic curve over $\boldsymbol{F}_q$ given by the Weierstrass equation

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

whose coefficients lie in $\boldsymbol{F}_q$. For each extension field K of $\boldsymbol{F}_q$, $E(K)$ is given by

$$E(K) = \{(x, y) \in K \times K | (x, y) \text{ satisfies } (1)\} \cup \{O\}$$

where O is a special point called the point at infinity. There is an abelian group structure on the points of $E(K)$, in which O serves as its identity element, given by the so-called *tangent-and-chord* method. We express its abelian group structure additively.

Let l be a positive integer relatively prime to p, the characteristic of $\boldsymbol{F}_q$. The *Weil pairing* is the map

$$e_l: \ E[l] \times E[l] \longrightarrow \mu_l \subset \bar{\boldsymbol{F}}_q$$

where $E[l] = \{T \in E(\bar{\boldsymbol{F}}_q) | [l]T = O\}$ is the group of l-torsion points and μ_l is the subgroup of l-th roots of

unity in $\bar{\boldsymbol{F}}_q$. For properties of the Weil pairing, see [16], [28].

Let $P \in E[l]$ be a point of order l. Then, we have the following:

Proposition 1[17], [28]**:** There exists $Q \in E[l]$ such that $e_l(P,Q)$ is a primitive l-th root of unity. Therefore,

$$f_Q : \langle P \rangle \longrightarrow \mu_l, \quad f_Q(S) = e_l(S,Q)$$

is a group isomorphism.

Based on this fact, the framework of the MOV algorithm can be described as follows:

Algorithm 1 (The MOV Algorithm [16], [17])**:**

Input: An element $P \in E(\boldsymbol{F}_q)$ of order l, and $R \in \langle P \rangle$.
Output: An integer n such that $R = [n]P$.
Step 1: Determine the minimum positive integer k such that $E[l] \subset E(\boldsymbol{F}_{q^k})$.
Step 2: Find $Q \in E[l]$ such that $\alpha = e_l(P,Q)$ has order l.
Step 3: Compute $\beta = e_l(R,Q)$.
Step 4: Compute n, the discrete logarithm of β to the base α in $\boldsymbol{F}^*_{q^k}$.

This algorithm is somewhat incomplete in that the method for determining k and that for finding a point Q are not explicitly given. For supersingular elliptic curves, the methods which settle those problems are given in [17]; the resulting minimum k are $k = 1, 2, 3, 4$, or 6, and for each corresponding k, Q is efficiently obtained by using the group structure of $E(\boldsymbol{F}_{q^k})$. Therefore, for supersingular elliptic curves, the reduction procedure (i.e. Step 2 and 3) is completed in probabilistic polynomial time in $\log q$ and the algorithm mentioned above takes probabilistic subexponential time in $\log q$.

In the following, we consider the two problems described in Sect. 1 esspecially for ordinary (non-supersingular) elliptic curves.

For the problem of determining the minimum positive integer k such that $E[l] \subset E(\boldsymbol{F}_{q^k})$, recently, Balasubramanian and Koblitz [3] have obtained the following result:

Proposition 2[3]**:** Let E be an elliptic curve defined over $\boldsymbol{F}_q$, and suppose that l is a prime number such that $l | \#E(\boldsymbol{F}_q)$, $l \not| q-1$. Then, $E[l] \subset E(\boldsymbol{F}_{q^k})$ if and only if $l | q^k - 1$.

Remark 1: It is important to note that Balasubramanian and Koblitz's results also suggest that we need $k = l$ if $l | q-1$ and $E[l] \not\subset E(\boldsymbol{F}_q)$. Thus, when l is much larger than $\log q$, we may give up applying the MOV reduction since the extension degree in this case is too large in order for the reduced DLP in $\boldsymbol{F}^*_{q^k}$ to be solved in subexponential time in $\log q$.

3. An Efficient Method for Finding l-Torsion Points

In this section, we consider the problem of finding an l-torsion point $Q \in E[l]$ such that $\alpha = e_l(P,Q)$ has order l. (See Algorithm 1 in Sect. 2.) We refer to such an l-torsion point Q as a "good" l-torsion point. In this section, we actually propose a method which finds a "good" l-torsion point, and estimate the running time.

As before, we assume the following:

Assumption 1: (1) l is an odd prime number; (2) $l \not| q$; (3) $l \not| q-1$.

The first condition is not restrictive since we can reduce the composite case to the prime one by applying the Chinese Remainder Theorem and the Pohlig-Hellman algorithm; the second one is necessary, since the Weil pairing is not defined otherwise, and more importantly when $l | q$, the l-part DLP is solved by the obvious extension of [22], [26], [30] in polynomial time; the third one is reasonable from the result by Balasubramanian and Koblitz (See Remark 1 in Sect. 2).

Also, as before, we use the following notation: P is a base point with order l (Thus, $E(\boldsymbol{F}_q)[l] = \langle P \rangle \cong \boldsymbol{Z}/l$.); k is a positive integer such that $E[l] \subset E(\boldsymbol{F}_{q^k})$. If we are interested in the minimum k such that $E[l] \subset E(\boldsymbol{F}_{q^k})$, see Proposition 2 in Sect. 2.

Let N_k be the number of $\boldsymbol{F}_{q^k}$-rational points on E, and $E(\boldsymbol{F}_{q^k})_l$ the l-part of $E(\boldsymbol{F}_{q^k})$, i.e.

$$N_k = \#E(\boldsymbol{F}_{q^k}), \qquad E(\boldsymbol{F}_{q^k})_l = \bigcup_{i \geq 1} E(\boldsymbol{F}_{q^k})[l^i],$$

and let $d = v_l(N_k)$ denote the largest integer such that $l^d | N_k$.

For supersingular elliptic curves, the method for finding a "good" l-torsion point is considered based on the fact that $E(\boldsymbol{F}_{q^k}) \cong \boldsymbol{Z}/cl \times \boldsymbol{Z}/cl$, where c is some constant and determined based on the class of supersingular elliptic curves. For ordinary (non-supersingular) elliptic curves, the similar method is presented in [10] assuming some condition on the group structure of $E(\boldsymbol{F}_{q^k})$ in order to work efficiently.

On the other hand, one might easily come up with the following method: pick a point $V \in E(\boldsymbol{F}_{q^k})_l$ randomly using the map $[N_k/l^d]$, and compute its order, say l^t. Then we have $Q = [l^{t-1}]V \in E[l]$. However, if we consider the case that $E(\boldsymbol{F}_q)_l \cong \boldsymbol{Z}/l^r$ $(r \geq 2)$ and $E(\boldsymbol{F}_{q^k})_l \cong \boldsymbol{Z}/l^r \times \boldsymbol{Z}/l^s$ with some $s < r$, where l is exponential in $\log q$, this method takes exponential time in $\log q$ even for small k. We briefly explain the reason. The probability that the order of V is l^r is $\varphi(l^r)l^s/l^{r+s} = l^{r-1+s}(l-1)/l^{r+s} = 1 - 1/l$, where φ is the Euler function. If V has order l^r, then, $Q = [l^{r-1}]V$ is in $\langle P \rangle$, so that $e_l(P,Q) = 1$. Thus, the probability of obtaining a "good" l-torsion point is less than $1/l$. Therefore, this means that the expected number of iterations is at least l. Since l is exponential in $\log q$, it is exponentially large.

The key idea commonly seen in these methods is to use constant maps $\boldsymbol{Z} \subset \mathrm{End}_{F_{q^k}}(E)$ in a suitable way,

where $\mathrm{End}_{F_{q^k}}(E)$ is the ring of endomorphisms of E defined over $\boldsymbol{F}_{q^k}$. In addition to this idea, by using the q-th power Frobenius map, we propose a method which finds a "good" l-torsion point. It will turn out that our method works efficiently without assuming any condition on the group structure of $E(\boldsymbol{F}_{q^k})$, i.e. for the general case.

Before giving a method of finding a "good" l-torsion point, we analyze the group structure $E(\boldsymbol{F}_{q^k})$. If an elliptic curve E is supersingular, it is explicitly given in [24]. Thus, what remains to be investigated is the ordinary (non-supersingular) case.

Theorem 1[†]**:** Let E be an ordinary elliptic curve over $\boldsymbol{F}_q$ and l an odd prime number. Suppose that $v_l(\#E(\boldsymbol{F}_q)) = r \geq 1$ and that $l \not| q-1$, $l \not| q$. For a given positive integer k, we set $\eta := v_l(k)$ and $\omega := v_l(q^k-1)$. Then, we have

$$E(\boldsymbol{F}_{q^k})_l \simeq \boldsymbol{Z}/l^{r+\eta} \times \boldsymbol{Z}/l^{\delta},$$

where δ is given as follows: if $\omega < \eta + r$, then $\delta = \omega$; if $\omega > \eta + r$, then $\delta = \eta + r$; and if $\omega = \eta + r$, then δ is some positive integer with $\delta \geq \omega (= \eta + r)$.

Proof of Theorem 1. The case of $k = 1$ is trivial. We assume $k \geq 2$ in the sequel.

Let ϕ be the q-th power Frobenius map and $D_{\boldsymbol{Z}[\phi]}$ denote the discriminant of the ring $\boldsymbol{Z}[\phi]$. Since $l|\#E(\boldsymbol{F}_q) = q + 1 - t$ and $l \not| q - 1$, we have $D_{\boldsymbol{Z}[\phi]} = t^2 - 4q \equiv (q+1)^2 - 4q \equiv (q-1)^2 \not\equiv 0 \bmod l$. Thus, l does not divide the conductor of $\mathcal{O}$ in $\mathcal{O}_K$, where $\mathcal{O} = \mathrm{End}_{F_q}(E) = \mathrm{End}_{\bar{F}_q}(E)$ (note that the last equality follows since E is ordinary), and $\mathcal{O}_K$ is the maximal order of $K = \boldsymbol{Q} \otimes \boldsymbol{Z}[\phi]$.

Now, we consider the ideal decomposition of $l\mathcal{O}_K$ in $\mathcal{O}_K$. The minimal polynomial of ϕ is $X^2 - tX + q \in \boldsymbol{Z}[X]$ and it decomposes as

$$X^2 - tX + q \equiv (X-1)(X-q) \bmod l. \tag{2}$$

Since $q \not\equiv 1 \bmod l$, Eq. (2) has two distinct roots. Therefore, we see that l splits completely in $\mathcal{O}_K$ and that the prime ideal decomposition of $l\mathcal{O}_K$ in $\mathcal{O}_K$ is $l\mathcal{O}_K = \mathcal{L}\bar{\mathcal{L}}$, where $\mathcal{L} = l\mathcal{O}_K + (\phi - 1)\mathcal{O}_K$.

Let $(\mathcal{O}_K)_{\mathcal{L}}$ and $(\mathcal{O}_K)_{\bar{\mathcal{L}}}$ be the localizations of the ring $\mathcal{O}_K$ at primes $\mathcal{L}$ and $\bar{\mathcal{L}}$, respectively. Also, let $v_{\mathcal{L}}$ and $v_{\bar{\mathcal{L}}}$ be the normalized discrete valuations with respect to $\mathcal{L}$ and $\bar{\mathcal{L}}$, respectively.

We claim that if $v_{\mathcal{L}}((\phi^k - 1)\mathcal{O}_K) = a$ and $v_{\bar{\mathcal{L}}}((\phi^k - 1)\mathcal{O}_K) = b$, then $E(\boldsymbol{F}_{q^k})_l \simeq \boldsymbol{Z}/l^a \times \boldsymbol{Z}/l^b$. In fact, let N be the norm, then $N(\phi^k - 1) = \#E(\boldsymbol{F}_{q^k})$. Thus, $v_l(\#E(\boldsymbol{F}_{q^k})) = a + b$ is obtained. On the other hand, $E[l^c] \subset E(\boldsymbol{F}_{q^k})$ if and only if $\phi^k - 1$ is divisible by l^c in $\mathcal{O}$ (see [20, Lemma 1]). Putting $c := \min(a, b)$, we have $E[l^c] \subset E(\boldsymbol{F}_{q^k})$ and $E[l^{c+1}] \not\subset E(\boldsymbol{F}_{q^k})$ since l does not divide the conductor of $\mathcal{O}$. Thus, we have $E(\boldsymbol{F}_{q^k})_l \simeq \boldsymbol{Z}/l^a \times \boldsymbol{Z}/l^b$.

From the assumption that $v_l(\#E(\boldsymbol{F}_q)) = r$ and $l \not| q - 1$ (this implies $E[l] \not\subset E(\boldsymbol{F}_q)$), it follows that

$$v_{\mathcal{L}}(\phi - 1) = r \qquad \text{and} \tag{3}$$
$$v_{\bar{\mathcal{L}}}(\phi - 1) = 0. \tag{4}$$

If we set

$$\eta := v_{\mathcal{L}}(\phi^k - 1) - r \qquad \text{and}$$
$$\delta := v_{\bar{\mathcal{L}}}(\phi^k - 1),$$

we can write

$$E(\boldsymbol{F}_{q^k})_l \simeq \boldsymbol{Z}/l^{r+\eta} \times \boldsymbol{Z}/l^{\delta}.$$

In the sequel, we evaluate η and δ in the discrete valuation rings $(\mathcal{O}_K)_{\mathcal{L}}$ and $(\mathcal{O}_K)_{\bar{\mathcal{L}}}$, respectively.

First, we evaluate η. Let π be some prime element with $v_{\mathcal{L}}(\pi) = 1$. Then, we can write ϕ in the form

$$\phi = 1 + u\pi^r,$$

(See (3)), where u is some unit in $(\mathcal{O}_K)_{\mathcal{L}}$. Thus, we have

$$\phi^k = (1 + u\pi^r)^k = 1 + k\pi^r u + \sum_{i=2}^{k} \binom{k}{i} \pi^{ri} u^i. \tag{5}$$

Here, we apply the following lemma.

Lemma 1: Let k be an integer no less than two and l an odd prime number. Then, for any positive integer w such that $2 \leq w \leq k$,

$$v_l(\binom{k}{w}) - v_l(k) + (w-1) > 0.$$

Proof. Considering the l-adic expansion of w, we can write w uniquely in the form $w = \sum_{i=0}^{m} w_i l^i$ with $0 \leq w_i < l$ and $w_m \neq 0$. Since $v_l(w!) = \sum_{i \geq 1} \lfloor w/l^i \rfloor$, we have $v_l(w!) = \sum_{i=1}^{m} (\sum_{j=0}^{i-1} l^j) w_i$. Thus,

$$\begin{aligned} v_l(\binom{k}{w}) &- v_l(k) + w - 1 \\ &= v_l((k-1)(k-2)\cdots(k-w+1)) \\ &\quad - v_l(w!) + w - 1 \\ &= v_l((k-1)(k-2)\cdots(k-w+1)) \\ &\quad + \sum_{i=1}^{m} (l^i - \sum_{j=0}^{i-1} l^j) w_i + (w_0 - 1). \end{aligned}$$

Clearly, $l^i - \sum_{j=0}^{i-1} l^j > 0$ for any $i \geq 1$. From the assumption that l is an odd prime and $w \geq 2$, it follows that

$$\sum_{i=1}^{m} (l^i - \sum_{j=0}^{i-1} l^j) w_i + (w_0 - 1) > 0.$$

Therefore, the proof is completed. □

Now, we are back to the proof of Theorem 1. From

[†]Recently, Saito and Uchiyama [21] reported a relevant result to Theorem 1.

Lemma 1, it follows that

$$\begin{aligned} v_{\mathcal{L}}(k\pi^r u) &= v_l(k) + r \\ &< v_l(\binom{k}{i}) + ri \qquad (\text{ by Lemma 1}) \\ &= v_{\mathcal{L}}(\binom{k}{i}\pi^{ri}u^i) \end{aligned}$$

for any $i \geq 2$. Therefore, we have

$$v_{\mathcal{L}}(\phi^k - 1) = v_{\mathcal{L}}(k\pi^r u) = v_l(k) + r,$$

from which we obtain $\eta = v_l(k)$.

Next, we evaluate δ. We discuss it in the ring $(\mathcal{O}_K)_{\bar{\mathcal{L}}}$. Since $\phi\bar{\phi} = q$ and $\bar{\phi}$ is a unit (note that $l \not| q$), we have

$$\phi^k - 1 = \frac{q^k}{\bar{\phi}^k} - 1 = \frac{q^k - \bar{\phi}^k}{\bar{\phi}^k}.$$

Therefore, $v_{\bar{\mathcal{L}}}(\phi^k - 1) = v_{\bar{\mathcal{L}}}(q^k - \bar{\phi}^k)$.

Let π' be some prime element with $v_{\bar{\mathcal{L}}}(\pi') = 1$. From (3), we can write $\bar{\phi}$ in the form

$$\bar{\phi} = 1 + u'(\pi')^r$$

for some unit $u' \in (\mathcal{O}_K)_{\bar{\mathcal{L}}}$. Therefore, we obtain

$$\begin{aligned} q^k - \bar{\phi}^k &= (q^k - 1) - ku'(\pi')^r \\ &\quad - \sum_{i=2}^{k} \binom{k}{i}(u')^i(\pi')^{ri}, \end{aligned} \tag{6}$$

and for any i with $2 \leq i \leq k$,

$$\begin{aligned} & v_{\bar{\mathcal{L}}}(\binom{k}{i}(u')^i(\pi')^{ri}) - v_{\bar{\mathcal{L}}}(ku'(\pi')^r) \\ &= (v_l(\binom{k}{i}) + ir) - (v_l(k) + r) \\ &= v_l(\binom{k}{i}) - v_l(k) + (i-1)r \\ &\geq v_l(\binom{k}{i}) - v_l(k) + (i-1) \\ &> 0 \qquad\qquad (\text{by Lemma 1}). \end{aligned}$$

Thus,

$$v_{\bar{\mathcal{L}}}(ku'(\pi')^r) = v_l(k) + r < v_{\bar{\mathcal{L}}}(\binom{k}{i}(u')^i(\pi')^{ri})$$

for any i with $2 \leq i \leq k$. Set $\omega := v_l(q^k - 1)$. Then from the formula (6), if $\omega < \eta + r$ (note that $\eta = v_l(k)$), then $\delta = v_{\bar{\mathcal{L}}}(\phi^k - 1) = \omega$; if $\omega > \eta + r$, then $\delta = v_{\bar{\mathcal{L}}}(\phi^k - 1) = \eta + r$; if $\omega = \eta + r$, then $\delta = v_{\bar{\mathcal{L}}}(\phi^k - 1) \geq \omega = \eta + r$. Thus, the proof is completed. □

3.1 Proposed Method

In this subsection, we actually propose a method which efficiently finds a "good" l-torsion point. Since the method for the supersingular case is already given in [17], we forcus on the ordinary case. The following is our proposed method for ordinary elliptic curves.

Let k be the minimum positive integer such that $E[l] \subset E(\boldsymbol{F}_{q^k})$, or equivalently the minimum k such that $l | q^k - 1$. (See Proposition 2 in Sect. 2.)

Procedure:

Step 1: Compute $N_1 = \#E(\boldsymbol{F}_q)$ and $r = v_l(N_1)$.
Step 2: Compute $N_k = \#E(\boldsymbol{F}_{q^k})$ from N_1, using the Weil conjecture.
Step 3: Compute $d = v_l(N_k)$ and $s := d - r$. If $r > s$, go to Step 5.
Step 4: (the case of $r \leq s$)
  (4-1): Pick $Q \in E(\boldsymbol{F}_{q^k})$ randomly.
  (4-2): Compute $Q' := [N_k/l^{r+1}]Q \in E[l]$.
  (4-3): Compute $\alpha := e_l(P, Q')$. If $\alpha = 1$, go to Step (4-1). Otherwise, go to Step 6.
Step 5: (the case of $r > s$)
  (5-1): Pick $Q \in E(\boldsymbol{F}_{q^k})$ randomly.
  (5-2): Compute $Q' := (\phi - 1) \circ [N_k/l^{r+1}]Q \in E[l]$. If $Q' = O$, then go to Step (5-1).
  (5-3): Compute $\alpha := e_l(P, Q')$.
Step 6: Store Q' and α.

3.2 Validity of the Proposed Method

In this subsection, we give explanation of each step in the proposed method.

In Step 1, we compute N_1 in polynomial time in $\log q$ using the Schoof-Elkies-Atkin algorithm and its variants [1], [2], [4]–[7], [11], [14], [15], [19], [25].

In Step 2, we can compute N_k as follows: compute t_i $(1 \leq i \leq k)$ recursively by $t_i = t_1 t_{i-1} - q t_{i-2}$, $t_0 = 2$, $t_1 = q + 1 - N_1$ (note that t_1, the trace of the q-th power Frobenius map, is already computed in the course of computing N_1), then we obtain $N_k = q^k + 1 - t_k$.

In Step 3, in order to compute d and s, we set $c_i := c_{i-1}/l$, $c_0 := N_k/l^{r+1}$. If c_m is the first number that is not an integer, $d = m + r$ and $s = m$ are obtained. In this step, we can know the group structure $E(\boldsymbol{F}_{q^k})_l$: since $v_l(k) = 0$, by Theorem 1 we have

$$\begin{aligned} E(\boldsymbol{F}_{q^k})_l &= \langle S \rangle \times \langle T \rangle \\ &\simeq \boldsymbol{Z}/l^r \times \boldsymbol{Z}/l^s \quad (1 \leq r,\ 1 \leq s) \\ &\quad \text{with} \quad \langle P \rangle \subset \langle S \rangle, \end{aligned}$$

where S and T are generators of orders l^r and l^s, respectively.

In Step 4, we assume that $r \leq s$. If $r = s$, then $E(\boldsymbol{F}_{q^k})_l \cong \boldsymbol{Z}/l^s \times \boldsymbol{Z}/l^s$. The image of the multiplication by N_k/l^{r+1} map $[N_k/l^{r+1}] = [l^{s-1}] \circ [N_k/l^d] : E(\boldsymbol{F}_{q^k}) \to E(\boldsymbol{F}_{q^k})$ is $E[l]$. Since the map $[N_k/l^{r+1}]$ is an abelian group homomorphism, the uniform distribution on $E(\boldsymbol{F}_{q^k})$ induces the uniform distribution on $E[l]$. Thus, if we pick $Q \in E(\boldsymbol{F}_{q^k})$ randomly, we can get $Q' = [N_k/l^{r+1}]Q \in E[l]$ randomly. Then the success probability in Step (4-3) (i.e. the probability of

not going back to Step (4-1)) is

$$\frac{\#E[l]-\#\langle P\rangle}{\#E[l]}=\frac{l^2-l}{l^2}=1-\frac{1}{l}=1-o(1),$$

where $o(1)\to 0$ as $l\to\infty$. Thus, the expected number of iterations is $1+o(1)$.

If $r<s$, the image of the multiplication by $[N_k/l^{r+1}]$ map $[N_k/l^{r+1}]$: $E(\boldsymbol{F}_{q^k})\to E(\boldsymbol{F}_{q^k})$ is isomorphic to $\boldsymbol{Z}/l$ and $\mathrm{Im}[N_k/l^{r+1}]\neq\langle P\rangle$. Thus, the success probability in Step (4-3) is

$$\frac{\#(\boldsymbol{Z}/l)^\times}{\#(\boldsymbol{Z}/l)}=\frac{l-l}{l}=1-\frac{1}{l}=1-o(1).$$

Thus, the expected number of iterations is $1+o(1)$.

In Step 5, we assume that

$$\begin{aligned}E(\boldsymbol{F}_{q^k})_l &= \langle S\rangle\times\langle T\rangle\\ &\simeq \boldsymbol{Z}/l^r\times\boldsymbol{Z}/l^s\quad(1\le s<r)\\ &\text{with}\quad\langle P\rangle\subset\langle S\rangle,\end{aligned}$$

where S and T are generators of orders l^r and l^s, respectively. In order to explain the validity of this step, we apply the following theorem:

Theorem 2: We assume that

$$E(\boldsymbol{F}_q)_l=\langle S\rangle\cong\boldsymbol{Z}/l^r\ (\text{thus},\langle P\rangle=\langle l^{r-1}S\rangle)$$

$$E(\boldsymbol{F}_{q^k})_l=\langle S\rangle\times\langle T\rangle\cong\boldsymbol{Z}/l^r\times\boldsymbol{Z}/l^s\quad(1\le s\le r),$$

where S and T are generators of orders l^r and l^s, respectively. Consider the map:

$$f=(\phi-1)\circ[l^{s-1}]:\ E(\boldsymbol{F}_{q^k})\longrightarrow E(\boldsymbol{F}_{q^k}).$$

Then, we have $\mathrm{Im}(f|_{E(F_{q^k})_l})\cong\boldsymbol{Z}/l$ and $\mathrm{Im}(f|_{E(F_{q^k})_l})\neq\langle P\rangle$.

Proof. Let $T_l(E)$ be the l-adic Tate module of E and $\pi_r:T_l(E)\to E[l^r]$ the canonical projection. Let $\{\hat{S},\hat{U}\}$ be a basis of $T_l(E)$ over $\boldsymbol{Z}_l$ such that $S=\pi_r(\hat{S})$, $U=\pi_r(\hat{U})$ and $T=l^{r-s}U$. Let $M_\phi=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ be the representation matrix of ϕ with respect to the basis $\{\hat{S},\hat{U}\}$ of $T_l(E)$. Since $\phi(S)=S$, we have $a\equiv 1 \bmod l^r$ and $c\equiv 0 \bmod l^r$. Also, $\det M_\phi=q$ gives $d\equiv q \bmod l^r$.

Clearly, $(\phi-1)(l^{s-1}S)=O$. And $(\phi-1)(U)=(b \bmod l^r)S+(q-1 \bmod l^r)U$, from which we have

$$\begin{aligned}&(\phi-1)(l^{s-1}T)\\ &\quad=(b \bmod l)l^{r-1}S+(q-1 \bmod l)l^{s-1}T.\end{aligned}$$

Since $l\not| q-1$, it follows that $(q-1 \bmod l)l^{s-1}T\neq O$. Therefore, the proof is completed. □

Since $(\phi-1)\circ[N_k/l^{r+1}]=(\phi-1)\circ[l^{s-1}]\circ[N_k/l^d]$, the image of the map $(\phi-1)\circ[N_k/l^{r+1}]:E(\boldsymbol{F}_{q^k})\to E(\boldsymbol{F}_{q^k})$ is isomorphic to $\boldsymbol{Z}/l$ and it is different from $\langle P\rangle$ by Theorem 2. Thus, the success probability in Step (5-2) (i.e. the probability of not going back to Step (5-1)) is

$$\frac{\#(\boldsymbol{Z}/l)^\times}{\#(\boldsymbol{Z}/l)}=\frac{l-1}{l}=1-\frac{1}{l}=1-o(1).$$

Thus, the expected number of iterations is $1+o(1)$.

3.3 Theoretical Analysis of the Proposed Method

In this subsection, we estimate the success probability and running time of the proposed method.

The success probability in each step can be estimated as follows:

1. the success probability in Step 4 is $1-1/l$. (See Sect. 3.2.)
2. the success probability in Step 5 is $1-1/l$. (See Sect. 3.2.)

For the running time, we assume that the usual multiplication method is used, so that multiplying two elements of length N takes $O(N^2)$ bit operations. The running time of the following major computation can be estimated as follows:

1. Computation of $\#E(\boldsymbol{F}_q)$ using the Schoof-Elkies-Atkin algorithm and its variants (in Step 1): this procedure requires $O(\log^6 q)$.
2. Picking a random point on $E(\boldsymbol{F}_{q^k})$: this procedure requires $O(k^3\log^3 q)$.
3. Computation of Q': computation of Q' in Step (4-2) requires $O((\log N_k)(k\log q)^2)=O((k\log q)(k\log q)^2)=O(k^3\log^3 q)$. Computation of Q' in Step (5-2) requires $O((\log N_k)(k\log q)^2+(\log q)(k\log q)^2)=O(k^3\log^3 q+k^2\log^3 q)=O(k^3\log^3 q)$.
4. Computation of the Weil pairing $e_l(P,Q')$: this procedure requires $O(k^3\log^3 q+(\log l)(k\log q)^2)=O(k^3\log^3 q+k^2\log^3 q)=O(k^3\log^3 q)$.

Also, each procedure except the above requires at most $O(k^3\log^3 q)$. Therefore, our method is completed in probabilistic polynomial time in $k\log q$, more precisely, $O(k^3\log^3 q+\log^6 q)$.

4. Concluding Remarks

In this paper, we have proposed a method which efficiently finds an l-torsion point needed to evaluate the Weil pairing in the MOV reduction for ordinary elliptic curves under $l\not| q-1$. Our method is completed in probabilistic polynomial time in $k\log q$, more precisely $O(k^3\log^3 q)$ if $\#E(\boldsymbol{F}_q)$ is given beforehand and otherwise $O(k^3\log^3 q+\log^6 q)$, where k is the minimum positive integer with $q^k\equiv 1 \bmod l$. This seems to be asymptotically optimal, since it is equal to that of randomly picking a point in $E(\boldsymbol{F}_{q^k})$, which seems to be

needed in any situation, except for computing $\#E(\boldsymbol{F}_q)$.

Also, our method is completed in probabilistic polynomial time in $\log q$ whenever k is small enough to solve the DLP in $\boldsymbol{F}_{q^k}^*$ in subexponential time in $\log q$. As a result, we can obtain the MOV algorithm which works under $l \not| q-1$ for ordinary elliptic curves in subexponential time in $\log q$ if the DLP in $\boldsymbol{F}_{q^k}^*$ is solved in subexponential time in $\log q$. Concerning the condition on k under which the DLP in $\boldsymbol{F}_{q^k}^*$ is solved in subexponential time in $\log q$, in [3], [13] it was pointed out that one needs $k = O((\log q)^{2-\epsilon})$, where ϵ is any positive constant, under the currently optimistic assumption that the DLP in $\boldsymbol{F}_{q^k}^*$ can be solved in time $L_{q^k}[1/3, -] = \exp(O((\log q^k)^{1/3}(\log\log q^k)^{2/3}))$ (See [23]).

In addition, our contribution allows us to finally draw the conclusion that the MOV reduction is as powerful as the FR reduction under $l \not| q-1$ not only from the viewpoint of the minimum extension degrees of the base field but also from that of the effectiveness of algorithms.

Acknowledgements

The authors would like to thank Prof. Yoshihiko Yamamoto, Dr. Nigel Smart, Dr. Shigenori Uchiyama, and Mr. Taiichi Saito for fruitful discussion and useful comments. Also, the authors would like to thank an anonymous reviewer for pointing out an error in the proof of the main result on the previous version.

References

[1] A.O.L. Atkin, The number of points on an elliptic curve modulo a prime, Draft, 1988.
[2] A.O.L. Atkin, The number of points on an elliptic curve modulo a prime (ii), Draft, 1992.
[3] R. Balasubramanian and N. Koblitz, "The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm," J. Cryptology, vol.11, pp.141–145, 1998.
[4] J.M. Couveignes and F. Morain, "Schoof's algorithm and isogeny cycles," Proc. ANTS-I, Lecture Notes in Computer Science, vol.877, pp.43–58, 1994.
[5] J.M. Couveignes, L. Dewaghe, and F. Morain, "Isogeny cycles and the Schoof-Elkies-Atkin algorithm," LIX/RR/96/03, 1996.
[6] J.M. Couveignes, "Computing l-isogenies using the p-torsion," Proc. ANTS-II, Lecture Notes in Computer Science, vol.1122, pp.59–65, Springer, 1996.
[7] N.D. Elkies, Explicit isogenies, Draft, 1991.
[8] 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.
[9] G. Frey, M. Müller, and H.G. Rück, "The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems," preprint, 1998.
[10] R. Harasawa, J. Shikata, J. Suzuki, and H. Imai, "Comparing the MOV and FR reductions in elliptic curve cryptography," Advances in Cryptology—EUROCRYPT'99, Lecture Notes in Computer Science, vol.1592, pp.190–205, 1999.
[11] T. Izu, J. Kogure, M. Noro, and K. Yokoyama, "Efficient implementation of Schoof's algorithm," Advances in Cryptology—ASIACRYPT'98, Lecture Notes in Computer Science, vol.1514, pp.66–79, Springer, 1998.
[12] N. Koblitz, "Elliptic curve cryptosystems," Math. Comp., vol.48, pp.203–209, 1987.
[13] N. Koblitz, "Elliptic curve implementation of zero-knowledge blobs," J. Cryptology, vol.4, no.3, pp.207–213, 1991.
[14] R. Lercier and F. Morain, "Counting the number of points on elliptic curves over finite fields: Strategy and performances," Advances in Cryptology—EUROCRYPT'95, Lecture Notes in Computer Science, vol.921, pp.79–94, 1995.
[15] R. Lercier, "Computing isogenies in F_{2^n}," Proc. ANTS-II, Lecture Notes in Computer Science, vol.1122, pp.197–212, Springer, 1996.
[16] A. Menezes, Elliptic Curve Public Key Cryptosystem, Kluwer Acad. Publ., Boston, 1993.
[17] A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms in a finite field," IEEE Trans. Inf. Theory, vol.IT-39, no.5, pp.1639–1646, 1993.
[18] V. Miller, "Use of elliptic curves in cryptography," Advances in Cryptology—CRYPTO'85, Lecture Notes in Computer Science, vol.218, pp.417–426, Springer, 1986.
[19] F. Morain, "Calcul du nombre de points sur une courbe elliptique dans un corps fini: Aspects algorithmiques," J. Théor. Nombres Bordeaux, vol.7, pp.255–282, 1995.
[20] H.G. Rück, "A note on elliptic curves over finite fields," Math. of Comp., vol.49, no.179, pp.301–304, 1987.
[21] T. Saito and S. Uchiyama, "A remark on the MOV algorithm," IEICE Technical Report, ISEC99-27, July 1999.
[22] T. Satoh and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves," Commentarii Math. Univ. St. Pauli, vol.47, no.1, pp.81–92, 1998.
[23] O. Schirokauer, D. Weber, and T. Denny, "Discrete logarithms: The effectiveness of the index calculus method," Proc. ANTS-II, Lecture Notes in Computer Science, vol.1122, pp.337–362, Springer-Verlag, 1996.
[24] R. Schoof, "Nonsingular plane cubic curves over finite fields," J. Combinatorial Theory, Series A, vol.46, pp.183–211, 1987.
[25] R. Schoof, "Counting points on elliptic curves over finite fields," J. Théor. Nombres Bordeaux, vol.7, pp.219–254, 1995.
[26] I. Semaev, "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p," Math. of Computation, vol.67, pp.353–356, 1998.
[27] J. Shikata, Y. Zheng, J. Suzuki, and H. Imai, "Generalizing the Menezes-Okamoto-Vanstone (MOV) algorithm to non-supersingular elliptic curves," Proc. 1999 Symposium on Cryptography and Information Security (SCIS'99), Kobe, Japan, Jan. 26–29, 1999.
[28] J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.
[29] J. Silverman and J. Suzuki, "Elliptic curve discrete logarithms and index calculus," Advances in Cryptology—ASIACRYPT'98, Lecture Notes in Computer Science, vol.1514, pp.110–125, Springer, 1998.
[30] N. Smart, "The discrete logarithm problem on elliptic curves of trace one," J. Cryptology, vol.12, no.3, pp.193–196, 1999.

Junji Shikata received the B.S. and M.S. degrees from Kyoto University, Kyoto, Japan, in 1994, 1997, respectively. Currently, he is a Ph.D. student of Osaka University.

Yuliang Zheng received his B.Sc. degree in computer science from Nanjing Institute of Technology, China, in 1982, and the M.E. and Ph.D. degrees, both in electrical and computer engineering, from Yokohama National University, Japan, in 1988 and 1991 respectively. From 1982 to 1984 he was with the Guangzhou Research Institute for Communications, Guangzhou (Canton), China, and from February 1991 to January 1992 he was a Post-Doctoral Fellow at the Computer Science Department, University College, University of New South Wales, in Canberra, Australia. From February 1992 to January 1995 he was with the Computer Science Department, University of Wollongong. Since February 1995 he has been with the Faculty of Information Technology, Monash University, in Melbourne. Currently he is Reader of the Faculty, and heads Monash's Laboratory for Information and Network Security (LINKS). His research interests include cryptography and its applications secure electronic commerce. Dr. Zheng is a member of IACR, ACM and IEEE.

Joe Suzuki was born in Tokyo, Japan, 1960. He received the B.E., M.E., and Dr. of Engineering degrees from Waseda University, Tokyo, Japan, in 1984, 1986, 1993, respectively. In 1994, he joined a faculty member of the Department of Mathematics, Osaka University, Osaka, Japan. He was Visiting Assistant Professor of Stanford University (1995–1997) and Visiting Scientist of Brown University (1998). Currently, he is Associate Professor of Osaka University. His research interests are mainly on mathematical analyses of computer science such as universal data compression, Kolmogorov complexity, statistical model selection, Bayesian belief networks, genetic algorithms, elliptic curve cryptosystems, algebraic geometry codes.

Hideki Imai was born in Shimane, Japan on May 31, 1943. He received the B.E., M.E., and Ph.D. degrees in electrical engineering from the University of Tokyo in 1966, 1968, 1971, respectively. From 1971 to 1992 he was on the faculty of Yokohama National University. In 1992 he joined the faculty of the University of Tokyo, where he is currently a Full Professor in the Institute of Industrial Science. His current research interests include information theory, coding theory, cryptography, spread spectrum systems and their applications. He received Excellent Book Awards from IEICE in 1976 and 1991. He also received the Best Paper Award (Yonezawa Memorial Award) from IEICE in 1992, the Distinguished Services Award form the Association for Telecommunication Promotion Month in 1994, the Telecom System Technology Prize from the Telecommunication Advancement Foundation and Achievement Award from IEICE in 1995. In 1998 he was awarded Golden Jubilee Paper Award by the IEEE Information Theory Society. In 1999 he was awarded Honor Doctor Degree from Soonchunhyang University, Korea. He was elected an IEEE Fellow for his contributions to the theory of coded modulation and two-dimensional codes in 1992. He chaired several committees of scientific societies and chaired many international conferences. He served as the leader of research projects supported by JSPS etc. and as the editor for scientific journals of IEICE, IEEE etc. Dr. Imai has been on the board of IEICE, the IEEE Information Theory Society, Japan Society of Security Management (JSSM) and the Society of Information Theory and Its Applications (SITA). He served as President of the IEICE Engineering Sciences Society and SITA.