Comparing the MOV and FR Reductions in Elliptic Curve Cryptography

Ryuichi Harasawa[1], Junji Shikata[1], Joe Suzuki[1], and Hideki Imai[2]

[1] Department of Mathematics, Graduate School of Science, Osaka University,
1-1 Machikaneyama, Toyonaka, Osaka 560-0043, Japan
{harasawa, shikata, suzuki}@math.sci.osaka-u.ac.jp
[2] Institute of Industrial Science, University of Tokyo, 7-22-1 Roppongi,
Minatoku, Tokyo 106-8558, Japan
imai@iis.u-tokyo.ac.jp

Abstract. This paper addresses the discrete logarithm problem in elliptic curve cryptography. In particular, we generalize the Menezes, Okamoto, and Vanstone (MOV) reduction so that it can be applied to some non-supersingular elliptic curves (ECs); decrypt Frey and Rück (FR)'s idea to describe the detail of the FR reduction and to implement it for actual elliptic curves with finite fields on a practical scale; and based on them compare the (extended) MOV and FR reductions from an algorithmic point of view. (This paper has primarily an expository role.)

1 Introduction

This paper addresses the discrete logarithm problem (DLP) in elliptic curve (EC) cryptography. ECs have been intensively studied in algebraic geometry and number theory. In recent years, they have been used in devising efficient algorithms for factoring integers [11] and primality proving [3], and in the construction of public key cryptosystems [15,9]. In particular, EC cryptography whose security is based on the intractability of the DLP in ECs (ECDLP) has drawn considerable public attention in recent years.

Let E/F_q be an EC given by the Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q, \qquad (1)$$

where $\mathbb{F}_q$ is a finite field with $q = p^m$ elements (p: prime, and $m \geq 1$). The ECDLP in $E/\mathbb{F}_q$ is defined to find $0 \leq l \leq n-1$ such that $R = lP := \underbrace{P + P + \cdots + P}_{l}$ given $P \in E(\mathbb{F}_q)$ and $R \in< P >$, where n is the order of the finite cyclic group $< P >$. Through the paper, we denote for $E(\mathbb{K}) := \{(x, y) \in \mathbb{K} \times \mathbb{K} | (x, y)$ satisfies $Eq.(1)\} \cup \{O\}$, the addition is defined in such a way that $E := E(\bar{\mathbb{K}})$ makes an abelian group, where $\bar{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$, and O is the identity element of the group [22].

The main reason why EC cryptosystems are getting more accepted compared to the conventional schemes is that it is believed that the ECDLP in $E/\mathbb{F}_q$

J. Stern (Ed.): EUROCRYPT'99, LNCS 1592, pp. 190–205, 1999.

generally requires an exponential time in $\log q$ to solve it (V. Miller [15], and J. Silverman and J. Suzuki [23]) while the DLP in $\mathbb{F}_q^*$ can be solved at most within a subexponential time.

In other words, if EC cryptosystems provide equivalent security as the existing schemes, then the key lengths will be shorter. Having short key lengths means smaller bandwidth and memory requirements and can be a crucial factor in some applications, for example the design of smart card systems.

However, it has been reported that for specific cases the ECDLP is no more difficult than the DLP by considering injective homomorphisms that map in a polynomial time from $< P >$ to $\mathbb{F}_q$ or $\mathbb{F}_{q^k}^*$, where $\mathbb{F}_{q^k}^*$ is a suitable extension field of $\mathbb{F}_q$. (For attacks against hyper-EC cryptography, L. Adleman, J. DeMarrais, and M. Huang gave a heuristic argument that under certain assumptions, the DLP in the group of rational points on the Jacobian of a genus g hyper-EC over $\mathbb{F}_p$ is solved in a subexponential time for sufficiently large g and odd p with $\log p \leq (2g+1)^{0.98}$. For the detail, see [1].)

For the reduction to $\mathbb{F}_q$, recently only the case of anomalous ECs, i.e. the case of $q = p$ and $\#E(\mathbb{F}_p) = p$, and its simple generalization have been solved [21,24,18].

On the other hand, for the reduction to $\mathbb{F}_{q^k}^*$, A. Menezes, T. Okamoto, and S. Vanstone [13] proposed the so-called MOV reduction that makes it possible to solve the case of supersingular ECs, i.e. the case of $p|t$ with $t := q+1-\#E(\mathbb{F}_q)$. In other words, for supersingular ECs the ECDLP in $E/\mathbb{F}_q$ is reduced to the DLP in $\mathbb{F}_{q^k}^*$ for some k that is solved in a subexponential time. The DLP obtained in that way is defined in $\mathbb{F}_{q^k}^*$, so that the input size is multiplied by k. In actual, the value of k is the minimum positive integer such that $E[n] \subseteq E(\mathbb{F}_{q^k})$, where $E[n] := \{T \in E | nT = O\}$. Menezes, Okamoto, and Vanstone found in [13] that if $E/\mathbb{F}_q$ is supersingular, such a k is at most six, and constructed a probabilistic polynomial time algorithm to find $Q \in E[n]$ such that the Weil pairing $e_n(P,Q)$ [22] has order n in $\mathbb{F}_{q^k}^*$.

Concerning the reduction to $\mathbb{F}_{q^k}^*$, after the MOV reduction appeared, G. Frey and H. Rück [7] proposed another injective homomorphism based on the Tate pairing (FR reduction). The FR reduction is applied when $n|q-1$. Also, by extending the definition field from $\mathbb{F}_q$ to $\mathbb{F}_{q^k}$, the reduction is possible even for the case of $n|q^k-1$. In this case, k is the minimum positive integer such that $n|q^k-1$. Then, as in the MOV reduction, the input size of the DLP is multiplied by k. But the Ref. [7] dealt with only the conceptual aspect.

At this point, we should be aware that there is a gap between the conditions to which the MOV and FR reductions are applied. In fact, according to R. Schoof [19], if $p \not| n$, $E[n] \subseteq E(\mathbb{F}_{q^k})$ is equivalent to $n|q^k-1$ and other two conditions.

In this paper, we generalize the MOV reduction so that it can be applied to some non-supersingular ECs satisfying $E[n] \subseteq E(\mathbb{F}_{q^k})$ for some k (Section 2). This extension is never straightforward since no algorithm has been proposed to efficiently find for non-supersingular ECs some $Q \in E[n]$ such that $e_n(P,Q)$ is a primitive n^{th} root of unity. We construct a polynomial time algorithm to realize it although those ECs do not cover all the ones satisfying $E[n] \subseteq E(\mathbb{F}_{q^k})$.

Moreover, we prove that it is possible to immediately find such a $Q \in E[n]$ for the MOV reduction unless $c_2 n | c_1$ when we express the group structure as[1]

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}, \quad E[n] \subseteq E(\mathbb{F}_{q^k}), \text{ and } \quad E(\mathbb{F}_{q^k}) \cong \mathbb{Z}_{c_1 n_1} \oplus \mathbb{Z}_{c_2 n_1}$$

with $n_2 | n_1$ and $c_2 | c_1$ (See [13,14]).

On the other hand, quite recently, R. Balasubramanian and N. Koblitz [5] showed that if n is a prime, $n \nmid q$, and $n \nmid q-1$, then $E[n] \subseteq E(\mathbb{F}_{q^k})$ is equivalent to $n | q^k - 1$.

In this sense, if n is a prime, the following are the cases that the (extended) MOV reduction cannot deal with but the FR can:

1. $n | q-1$; and
2. $E[n] \subseteq E(\mathbb{F}_{q^k})$, $c_2 n | c_1$.

Next, we describe the detail algorithm for the FR reduction, and analyze the computational property (in Section 3). We actually implement the FR reduction for many cases. In addition, we compare it with the extended MOV reduction except for those two cases (in Section 4). Consequently, we should suggest that the FR is better than the MOV in any situation.

Through the paper, for brevity, we assume

1. the order n of $< P >$ is a prime.

If the given $n = \prod_i p_i^{e_i}$ is not a prime. the problem is reduced to finding for each i, $l \bmod p_i$ such that $R = lP$. Then, we can obtain the values of $l \bmod p_i^{e_i}$ for all i using the Pohlig-Hellman's algorithm [17] to determine $l \bmod n$ using the Chinese Remainder Theorem. Further, without loss of generality, we can further assume the following two conditions:

2. $p \nmid t$ (non-supersingularity), and
3. $p \nmid n$ (non-anomalousness) i.e. $p \neq n$

because for those cases, the ECDLP has been already solved in subexponential and polynomial times, respectively.

This paper has primarily an expository role.

2 Extending the MOV Reduction

The framework of the MOV reduction can be described as follows ([13], page 71 in [14]). The idea is to extend the definition field from $\mathbb{F}_q$ to $\mathbb{F}_{q^k}$ for some k so that $E[n] \subseteq E(\mathbb{F}_{q^k})$.

Algorithm 1
Input: *an element $P \in E(\mathbb{F}_q)$ of order n, and $R \in < P >$.*
Output: *an integer l such that $R = lP$*

[1] Through the paper, $\mathbb{Z}_n$ denotes $\mathbb{Z}/n\mathbb{Z}$.

Step 1: *determine the smallest integer k such that $E[n] \subseteq E(\mathbb{F}_{q^k})$.*
Step 2: *find $Q \in E[n]$ such that $\alpha = e_n(P,Q)$ has order n.*
Step 3: *compute $\beta = e_n(R,Q)$.*
Step 4: *compute l, the discrete logarithm of β to the base α in $\mathbb{F}^*_{q^k}$.*

Let μ_n be the group of n^{th} roots of unity, e_n: $E[n] \times E[n] \longrightarrow \mu_n$ the Weil pairing [22], and $Q \in E[n]$ such that $e_n(P,Q)$ is a primitive n^{th} root of unity. Then, from the property of the Weil pairing, $\mu_n \subseteq \mathbb{F}^*_{q^k}$ holds. Thus, the group isomorphism $< P > \longrightarrow \mu_n$ defined by $S \mapsto e_n(S,Q)$ gives an injective homomorphism $< P > \longrightarrow \mathbb{F}^*_{q^k}$ [13].

It is known that for any $E/\mathbb{F}_q$ there is a pair (n_1, n_2) such that $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ with $n_2|n_1$ [14]. Ref. [13] proved that if $E/\mathbb{F}_q$ is supersingular,

1. k is at most 6, and
2. if put $E(\mathbb{F}_{q^k}) \cong \mathbb{Z}_{c_1 n_1} \oplus \mathbb{Z}_{c_2 n_1}$ for appropriate c_1 and c_2 with $c_2|c_1$, then $c_1 = c_2$.

In general, the values of c_1 and c_2 can be obtained by the following:

1. Count $\#E(\mathbb{F}_q)$, using Schoof's method [20] or its variant [6,2].
2. For each k,
   (a) compute $\#E(\mathbb{F}_{q^k})$ from $\#E(\mathbb{F}_q)$, using the Weil Theorem [14];
   (b) factor $\#E(\mathbb{F}_{q^k})$; and
   (c) find n'_1 and n'_2 such that $E(\mathbb{F}_{q^k}) \cong \mathbb{Z}_{n'_1} \oplus \mathbb{Z}_{n'_2}$, using Miller's algorithm [16] ($c_1 = n'_1/n_1$ and $c_2 = n'_2/n_1$).

However, it would be time-consuming to follow these steps: the first two steps take polynomial times, the third takes a subexponential time, and the last takes a probabilistic polynomial time, provided k is small enough compared to q. However, in Ref. [13], Algorithm 1', which will be mentioned later, is constructed concretely based on the following facts concerning supersingular ECs:

1. there are six classes of supersingular ECs;
2. the values of k and c $(= c_1 = c_2)$ are uniquely determined by the class; and
3. the class is uniquely determined by the value of $t = q + 1 - \#E(\mathbb{F}_q)$, where t is the trace of q^{th}-power Frobenius endomorphism.

That is, for supersingular ECs, the following algorithm was proposed in [13] [14].
Algorithm $1'$

Input: an element $P \in E(\mathbb{F}_q)$ of order n, and $R \in < P >$.
Output: an integer l such that $R = lP$

Step 1': determine the smallest integer k such that $E[n] \subseteq E(\mathbb{F}_{q^k})$.
Step 2': pick $Q' \in E(\mathbb{F}_{q^k})$ randomly, and compute $Q = [cn_1/n]Q'$.
Step 3': compute $\alpha = e_n(P,Q)$ and $\beta = e_n(R,Q)$.
Step 4': compute l' by solving the discrete logarithm of β to the base α in $\mathbb{F}^*_{q^k}$.
Step 5': check if $l'P = R$ holds. If it does, set $l = l'$. Otherwise, go to Step 2'.

It can be easily seen that Algorithms 1 and $1'$ are essentially the same although they take different step. At this point, we pay attention to how to determine an element $Q \in E[n]$. The correct l is obtained with probability $1 - 1/n$ ($\phi(n)/n$ if n is not a prime) after Steps 1'-5' of Algorithm $1'$.

Since n is large, the expected number of trials is close to one.

Since we consider non-supersingular ECs, we cannot use the above three facts. Let (e, r) be such that $c_1/c_2 = n^e r$ with $e \geq 0$ and $(n, r) = 1$. We propose the details of Step 2 in Algorithm 1 for non-supersingular ECs as follows:

Step 2-1: pick $Q' \in E(\mathbb{F}_{q^k})$ randomly.
Step 2-2: set $Q = [c_1 n_1/n^{e+1}]Q' \in E[n^{e+1}] \cap E(\mathbb{F}_{q^k})$.
Step 2-3: if $Q \notin E[n]$, i.e. if $nQ \neq O$, go to Step 2-1.
Step 2-4: compute $\alpha = e_n(P, Q)$. If $\alpha = 1$, go to Step 2-1.

We should note here that the above modification provides a generalization of the MOV reduction: previously, the MOV can be applied if the EC is supersingular, i.e. $e = 0$ and $r = 1$. If $e = 0$, Step 2-3 can be omitted. The following theorem suggests from a computational point of view that the extension of the MOV reduction in this paper is useful if and only if $e = 0$.

Theorem 1 *The probability that $Q \in E[n^{e+1}] \cap E(\mathbb{F}_{q^k})$ obtained in Step 2-2 satisfies both $Q \in E[n]$ and $e_n(P, Q) \neq 1$ is $\frac{1}{n^e}(1 - \frac{1}{n})$.*

Proof: Consider the map:

$$f : E(\mathbb{F}_{q^k}) \rightarrow E(\mathbb{F}_{q^k}) \ , \quad f(Q) = [c_1 n_1/n^{e+1}]Q \ .$$

Then, since $E(\mathbb{F}_{q^k}) \cong \mathbb{Z}_{c_1 n_1} \oplus \mathbb{Z}_{c_2 n_1}$, the image of f is isomorphic to $\mathbb{Z}_{n^{e+1}} \oplus \mathbb{Z}_n$. Let Ω be the set of Q such that $Q \in E[n]$ and $e_n(P, Q) \neq 1$. From the property of the Weil pairing [22], $e_n(P, Q) = 1$ with $P \neq O$ if and only if $Q \in < P >$. Thus, $\#\Omega = n^2 - n$. If $Q' \in E(\mathbb{F}_{q^k})$ is randomly selected in Step 2-1, the probability of success in Step 2-4 is obtained as:

$$\frac{\#Kerf \times \#\Omega}{\#E(\mathbb{F}_{q^k})} = \frac{\dfrac{c_1 n_1 \times c_2 n_1}{n^{e+1} \times n} \times (n^2 - n)}{c_1 n_1 \times c_2 n_1} = \frac{1}{n^e}(1 - \frac{1}{n})$$

□

Corollary 1 *In Steps 2-1 through 2-4 of Algorithm 1, the expected number of iterations is $n^{e+1}/(n-1) \approx n^e$.*

Proof: From Kac's lemma [8], the expected time is the reciprocal number of the probability $(1 - 1/n)/n^e$ that has been obtained in Theorem 1, i.e.

$$1/[\frac{1}{n^e}(1 - \frac{1}{n})] = \frac{n^{e+1}}{n-1} \ .$$

□

Recall $n = O(q)$, which means Step 2-3 requires an exponential time on average if $e \geq 1$.

If we have $c_2n|c_1$ during the field extension when we apply the MOV reduction, we must give up the reduction process. Such a probability may be small, and we might in the future come up with an alternative method that can deal with even such a case. However, we should keep in mind that there is much additional computation to realize the MOV reduction for nonsupersingular ECs: counting $\#E(\mathbb{F}_q)$, factoring $\#E(\mathbb{F}_{q^k})$, finding the pair (c_1, c_2) for the group structure $E(\mathbb{F}_{q^k})$ (more precisely, the value of c_1n_1/n^{e+1} in Step 2-2), etc., even when $E[n] \subseteq E(\mathbb{F}_{q^k})$ and $c_2n \not| c_1$.

3 Implementing the FR Reduction

In this section, assuming $\mathbb{K} := \mathbb{F}_{q^k}$ for some k. We consider the realization of the FR reduction.

In the original paper by Frey and Rück [7], only the conceptual aspect was stated, and it seems that no realization on the FR reduction has been published because the FR reduction appears to be less familiar to the cryptography community than the MOV reduction. We first describe an algorithm for realizing Frey and Rück's idea, where we assume that k is the minimum integer such that $n|q^k - 1$.

Algorithm 2
Input: *an element $P \in E(\mathbb{F}_q)$ of order n, and $R \in <P>$.*
Output: *an integer l such that $R = lP$.*

```
Step 1: determine the smallest integer $k$ such that $n|q^k - 1$, and set $\mathbb{K} := \mathbb{F}_{q^k}$.
Step 2: pick $S, T \in E(\mathbb{K})$ randomly.
Step 3: compute the element $f \in \mathbb{K}(E)^*$ such that $div(f) = n((P) - (O))$, and
    compute $\alpha = f(S)/f(T)$
Step 4: compute $\gamma = \alpha^{\frac{q^k-1}{n}}$. If $\gamma = 1$, then go to Step 2.
Step 5: compute the element $g \in \mathbb{K}(E)^*$ such that $div(g) = n((R) - (O))$, and
    compute $\beta = g(S)/g(T)$, and $\delta = \beta^{\frac{q^k-1}{n}}$.
Step 6: solve the DLP $\delta = \gamma^l$ in $\mathbb{K}^*$, i.e. the logarithm of $\delta$ to the base $\gamma$ in $\mathbb{K}^*$.
```

3.1 Frey and Rück's Idea

Let $Div(E)$ be the divisor group of E and $supp(D) := \{P \in E(\bar{\mathbb{K}}) : n_P \neq 0\}$ for $D = \sum_{P \in E} n_P(P) \in Div(E)$. Then, since E is defined over $\mathbb{K}$, the Galois group $G_{\bar{\mathbb{K}}/\mathbb{K}}$ acts on $Div(E)$ as $D^\sigma = \sum_{P \in E} n_P(P^\sigma)$ for $D = \sum_{P \in E} n_P(P) \in Div(E)$ and $\sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}$. We say that $D \in Div(E)$ is defined over $\mathbb{K}$ if $D^\sigma = D$ for all $\sigma \in G_{\bar{\mathbb{K}}/\mathbb{K}}$, and denote by $Div_{\mathbb{K}}(E)$ the subset of $Div(E)$ whose elements are defined over $\mathbb{K}$.

For $f \in \bar{\mathbb{K}}(E)^*$, the divisor $div(f)$ is defined by $div(f) := \sum_{P \in E} ord_P(f)(P)$, where $ord_P(f)$ is the multiplicity of zeros (if positive) or poles (if negative) at $P \in E$ with respect to $f \in \bar{\mathbb{K}}(E)^*$, and we refer to such a divisor as the principal divisor.

Let $Div^0(E) := \{D \in Div(E) | deg(D) = 0\}$, where $deg(D) := \sum n_P$, and $Prin(E)$ the subset of $Div^0(E)$ whose elements are principal divisors. Then, we can define the following surjective map:

$$Div^0(E) \to Pic^0(E) := Div^0(E)/Prin(E) \ , \quad D \mapsto \bar{D}$$

and denote $D_1 \sim D_2$ if two divisors D_1 and D_2 have the same image, i.e. $\bar{D_1} = \bar{D_2}$ in $Pic^0(E)$. We further define $Pic^0_{\mathbb{K}}(E)$ to be the set of all divisor classes in $Pic^0(E)$ that have a representative element defined over $\mathbb{K}$, which is a subgroup of $Pic^0(E)$. Moreover, $Pic^0_{\mathbb{K}}(E)_n := \{\bar{D} \in Pic^0_{\mathbb{K}}(E) | n\bar{D} = 0\}$.

It is known that by the isomorphism

$$E(\mathbb{K}) \to Pic^0_{\mathbb{K}}(E) \ , \quad Q \mapsto \overline{(Q) - (O)} \ ,$$

we can identify $E(\mathbb{K})$ with $Pic^0_{\mathbb{K}}(E)$ [22], and denote $\overline{(Q) - (O)}$ by $\bar{Q}$.

Let A be a divisor such that $\bar{A} \in Pic^0_{\mathbb{K}}(E)_n$ and B another divisor $\sum_i a_i(Q_i) \in Div^0_{\mathbb{K}}(E)$ such that $supp(A) \cap supp(B) = \phi$. Since $nA \sim 0$, there exists an element f_A in the function field $\bar{\mathbb{K}}(E)$ such that $div(f_A) = nA$ [22], so that we can put $f_A(B) := \prod_i f_A(Q_i)^{a_i}$.

Then, Frey and Rück [7] proved the following:

Proposition 1 ([7]) *If $n | q-1$, $\{\bar{A}, \bar{B}\}_{0,n} := f_A(B)$ defines a nondegenerate bilinear pairing:*

$$\{,\}_{0,n} : \ E(\mathbb{K})[n] \times E(\mathbb{K})/nE(\mathbb{K}) \to \mathbb{K}^*/(\mathbb{K}^*)^n$$

where $E(\mathbb{K})[n] := E[n] \cap E(\mathbb{K})$.

Then the mapping $\mathbb{K}^* \to \mathbb{K}^*$ defined by $\alpha \mapsto \alpha^{\frac{q^k-1}{n}}$ gives $\mathbb{K}^*/(\mathbb{K}^*)^n \cong \mu_n \subseteq \mathbb{K}^*$, where μ_n is the group of n^{th} roots of unity. From the nondegeneracy of the pairing $\{,\}_{0,n}$, there exists $Q \in E(\mathbb{K})/nE(\mathbb{K})$ such that $\{\bar{P}, \bar{Q}\}_{0,n}^{\frac{q^k-1}{n}}$ is a primitive n^{th} root of unity. Thus, the group isomorphism $< P > \to \mu_n$ defined by $S \mapsto \{\bar{S}, \bar{Q}\}_{0,n}^{\frac{q^k-1}{n}}$ gives an injective homomorphism $< P > \to \mathbb{F}^*_{q^k}$.

The pairing $\{,\}_{0,n}$ can be said to be a variant of the Tate pairing [25].

3.2 Theoretical Analysis

In [7], the computation of Steps 2-5 is supposed to be within a probabilistic polynomial time, now we actually evaluate the computation for each step in Algorithm 2. We assume that the usual multiplication algorithms are used, so that multiplying two elements of length N takes time $O(N^2)$.

For Step 2, we first pick an element $x = a$ in $\mathbb{K}$ to substitute it to Eq. (1). Then, we check if the quadratic equation with respect to y has a solution in $\mathbb{K}$, i.e. if the discriminant is a quadratic residue in $\mathbb{K}$. The probability of the success is approximately a half. If it is successful, it suffices to solve the quadratic equation in a usual manner. The computation to solve the quadratic equation dominants one to compute quadratic roots in $\mathbb{K}$. This takes expected running time $O((\log q^k)^3) = O(k^3(\log q)^3)$ (for the detail, see [4], [10]). We do this process twice to obtain $S, T \in E(\mathbb{K})$.

For Step 3, there is a standard procedure to compute the function $f \in \bar{\mathbb{K}}(E)$ from a principal divisor $div(f) \in Prin(E)$ (see for example pages 63-64 in [14]). Basically, this can be done by the following:

1. Write $div(f) = \sum_i a_i((P_i) - (O))$.
2. For each i, compute $P'_i \in E$ and $f_i \in \bar{\mathbb{K}}(E)$ such that
$$a_i((P_i) - (O)) = (P'_i) - (O) + div(f_i)\ .$$
3. Add the divisors $(P'_i) - (O) + div(f_i)$, for all i.

Then, we can add two divisors as follows: if two divisor D, D' are expressed by

$$D = (P) - (O) + div(f)\ , \qquad D' = (P') - (O) + div(f')$$

with $P, P' \in E$ and $f, f' \in \bar{\mathbb{K}}(E)^*$, then

$$D + D' = (P + P') - (O) + div(ff'g)$$

where $g = l/v$ with l and v are the lines through P and P' and through $P + P'$ and O (in particular, $P' = -P$ implies $v \equiv 1$). We can obtain the value of $\alpha = f(S)/f(T)$ by substituting S, T to the aforementioned f, f', g and multiplying them. Hence, Step 3 takes $O((\log q^k)^2) \times O(\log n) = O(k^2(\log q)^3)$.

For Step 4, the computation of $\gamma = \alpha^{\frac{q^k-1}{n}}$ takes $O(\log(\frac{q^k-1}{n})) \times O((\log q^k)^2) = O(k^3(\log q)^3)$. Moreover, we should evaluate the probability of going back to Step 2 so that we can measure how long it takes to compute the whole steps. The crucial point here is that we should efficiently find $\bar{Q} \in Pic^0_{\mathbb{K}}(E)/nPic^0_{\mathbb{K}}(E)$ such that $\{\bar{P}, \bar{Q}\}_{0,n}$ can be a generator of $\mathbb{K}^*/(\mathbb{K}^*)^n$. We prove the following theorem.

Theorem 2 *Let k be the smallest positive integer such that $n|q^k - 1$ (in this case, $\mathbb{K} = \mathbb{F}_{q^k}$). Then the probability of going back from Step 4 to Step 2 is $1/n$.*

Proof: Note that $E(\mathbb{K}) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, $n_2|n_1$, and $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$. Thus,

$$E(\mathbb{K})[n] \cong \begin{cases} \mathbb{Z}_n & (n \not| n_2) \\ \mathbb{Z}_n \oplus \mathbb{Z}_n & (n|n_2). \end{cases}$$

Also, from the nondegeneracy of the FR reduction,

$$E(\mathbb{K})/nE(\mathbb{K}) \cong \begin{cases} \mathbb{Z}_n & (n \not| n_2) \\ \mathbb{Z}_n \oplus \mathbb{Z}_n & (n|n_2). \end{cases}$$

We consider the two cases separately.

1. $E[n] \not\subseteq E(\mathbb{K})$, i.e. $n \not| n_2$: if we pick $Q \in E(\mathbb{K})$ randomly, the probability of $\{\bar{P}, \bar{Q}\}_{0,n} \notin (\mathbb{K}^*)^n$ is
$$\frac{\#E(\mathbb{K}) - \#nE(\mathbb{K})}{\#E(\mathbb{K})} = \frac{n_1 n_2 - n_1 n_2/n}{n_1 n_2} = 1 - 1/n.$$
2. $E[n] \subseteq E(\mathbb{K})$, i.e. $n|n_2$: let $T := \{Q \in E(\mathbb{K})/nE(\mathbb{K}) \mid \{\bar{P}, \bar{Q}\}_{0,n} \notin (\mathbb{K}^*)^n\}$. Then, $\#T = n^2 - n$. Since the map $\varphi : E(\mathbb{K}) \to E(\mathbb{K})/nE(\mathbb{K})$ is a module homomorphism, the probability of $\{\bar{P}, \bar{Q}\}_{0,n} \notin (\mathbb{K}^*)^n$ is
$$\frac{\#\varphi^{-1}(T)}{\#E(\mathbb{K})} = \frac{\#\mathrm{Ker}(\varphi) \times \#T}{\#E(\mathbb{K})} = \frac{(n_1 n_2/n^2)(n^2 - n)}{n_1 n_2} = 1 - 1/n.$$

□

The probability of going back from Step 4 to Step 2 is almost close to zero since we assume that n is considerably large.

For Step 5, we can estimate the computation as $O(k^3(\log q)^3)$.

From the above insight, if k can be assumed to be small enough compared to q, the expected running time of the FR reduction (from Step 2 to Step 5 in Algorithm 2) is $O((\log q)^3)$.

3.3 Implementation

We made several experiments including the following four cases. The CPU is Pentium 75MHz (SONY Quarter L, QL-50NX, the second cache capacity: 256kB)

In Examples 1 and 2, the FR reduction was applied to ECs with trace 2.

Example 1 (EC with trace 2, i.e. $\#E(\mathbb{F}_p) = p - 1$) *Suppose that the curve $E/\mathbb{F}_p$: $y^2 = x^3 + ax + b$, the base point $P = (x_0, y_0) \in E(\mathbb{F}_p)$, the order n of P, and a point $R = [l]P = (x_1, y_1)$ are given as follows:*
$p = 23305425500899$ *(binary 45-bits, $p - 1 = 2 \times 3^2 \times 1137869^2$),*
$a = 13079575536215$, $b = 951241857177$,
$n = 1137869$,
$x_0 = 17662927853004$, $y_0 = 1766549410280$,
$x_1 = 2072411881257$, $y_1 = 5560421985272$.
Then, we find that $l = 709658$.

Example 2 (EC with trace 2, i.e. $\#E(\mathbb{F}_p) = p - 1$) *Suppose that the curve $E/\mathbb{F}_p$: $y^2 = x^3 + ax + b$, the base point $P = (x_0, y_0) \in E(\mathbb{F}_p)$, the order n of P, and a point $R = [l]P = (x_1, y_1)$ are given as follows:*
$p = 93340306032025588917032364977153$
(binary 107-bits, $p - 1 = 2^{10} \times 7^2 \times 163 \times 847321^2 \times 3986987^2$),
$a = 71235469403697021051902688366816$, $b = 47490312935798014034601792244544$,
$n = 3986987$,
$x_0 = 10362409929965041614317835692463$, $y_0 = 79529049191468905652172306035573$,
$x_1 = 15411349585423321468944221089888$, $y_1 = 94160529078832780887823358300 33$.

For Example 2, the reduction process was implemented as follows:

1) Choose random points $S, T \in E(\mathbb{F}_p)$:
   $R = (x_2, y_2)$,
   $x_2 = 781831266536229655644442556815 46$, $y_2 = 785889451358545608004936721812 65$,
   $S = (x_3, y_3)$,
   $x_3 = 587146588843218597063396580123 14$, $y_3 = 293523592943075483044814000791 14$.
   The time of computation : 177 sec.
2) Compute the FR pairing:
   Set $div(f) := n((P) - (O))$, $div(g) := n((R) - (O))$ and $D := (S) - (T)$, then
   $\{\bar{P}, \bar{D}\}_{0,n} = \frac{f(S)}{f(T)} = 280896737020849225791892103620 50$,
   $(\frac{f(S)}{f(T)})^{\frac{p-1}{n}} = 860485481197365375119399092795 95$,
   $\{\bar{Q}, \bar{D}\}_{0,n} = \frac{g(S)}{g(T)} = 545381056152818070323809147441 28$,
   $(\frac{g(S)}{g(T)})^{\frac{p-1}{n}} = 441794237239751734273448931821 75$.
   The time of computation:

   computation of $f(S)$: 982 sec, computation of $f(T)$: 996 sec,
   computation of $g(S)$: 971 sec, computation of $g(T)$: 968 sec,
   computation of $(\frac{f(S)}{f(T)})^{\frac{p-1}{n}}$: 5 sec, computation of $(\frac{g(S)}{g(T)})^{\frac{p-1}{n}}$: 6 sec.
3) Solve the DLP: $(860485481197365375119399092795 95)^l$
   $= 441794237239751734273448931821 75 \bmod p$,
   find that $l = 764009$.

Next, in Examples 3 and 4, the FR and MOV reductions were applied to supersingular-ECs, and experimental data in the both reductions were analyzed and compared.

Example 3 (Supersingular-EC) *Suppose that the curve $E/\mathbb{F}_p$: $y^2 = x^3 + ax + b$, the base point $P = (x_0, y_0) \in E(\mathbb{F}_p)$, the order n of P, and a point $R = [l]P = (x_1, y_1)$ are given as follows:*
$p = 23305425500899$ *(binary* 45*-bits,* $p + 1 = 2^2 \times 5^2 \times 29 \times 1217 \times 6603413$*),*
$a = 1$, $b = 0$,
$n = 6603413$,
$x_0 = 18414716422748$, $y_0 = 9607997424906$,
$x_1 = 22829488331658$, $y_1 = 15463570264423$.

Since $E(\mathbb{F}_p) \cong \mathbb{Z}_{p+1}$, $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \oplus \mathbb{Z}_{p+1}$ [13], the definition field $\mathbb{F}_p$ is extended to $\mathbb{F}_{p^2}$ to apply the FR and MOV reductions. Then, we find that $l = 4500974$.

Example 4 (Supersingular-EC) *Suppose that the curve $E/\mathbb{F}_p$: $y^2 = x^3 + ax + b$, the base point $P = (x_0, y_0) \in E(\mathbb{F}_p)$, the order n of P, and a point $R = [l]P = (x_1, y_1)$ are given as follows:*
$p = 1020213065766829380286510327794694206093068319698 3$

(binary 163-bits, $p+1 = 2^3 \times 3^3 \times 59 \times 113$
$\times 70844587337774040484538990258451952825488847$*),*
$a = 1$*,* $b = 0$*,*
$n = 7084458733777404048453899025845195282548847$*,*
$x_0 = 6361408431660145018472734964469918949727993631117$*,*
$y_0 = 2224285726125163515264642109319596318772261 49291$*,*
$x_1 = 1791400202383882094094972648523798358242766050148$*,*
$y_1 = 6662282879825452479945554028296857282243572635001$*.*

Since $E(\mathbb{F}_p) \cong \mathbb{Z}_{\frac{p+1}{2}} \oplus \mathbb{Z}_2$*,* $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \oplus \mathbb{Z}_{p+1}$ *[13], the definition field* $\mathbb{F}_p$ *is extended to* $\mathbb{F}_{p^2}$ *to apply the FR and MOV reductions. Set* $g(\alpha) := \alpha^2 + 1$*. Then* $\mathbb{F}_{p^2} \cong \mathbb{F}_p[\alpha]/g(\alpha)$*.*

For Example 4, the FR and MOV reductions process were implemented as follows:

(FR reduction):

1) Choose random points $S, T \in E(\mathbb{F}_p)$:
   $S = (x_2, y_2)$,
   $x_2 = 5$,
   $y_2 = 2785279641020018517947594885587158401374598752249\alpha$
   $T = (x_3, y_3)$,
   $x_3 = 3385306113851451711868938545058221186172597937436$,
   $y_3 = 4986770654406953531745186184758026961048619598992$.
   The time of computation : 2245 sec;

2) Compute the FR pairing:
   Set $div(f) := n((P) - (O))$, $div(g) := n((R) - (O))$ and $D := (S) - (T)$, then
   $\{\bar{P}, \bar{D}\}_{0,n} = \frac{f(S)}{f(T)}$
   $= 3533166625479465632799073949081211397797456268974\alpha$
   $+4001496656282493042880656119736166996221452751615$,
   $(\frac{f(S)}{f(T)})^{\frac{p^2-1}{n}} = 5010350267319872795048848896836646242920060597592\alpha$
   $+6845979045282387430745118341017487648956259367889$,
   $\{\bar{R}, \bar{D}\}_{0,n} = \frac{g(S)}{g(T)}$
   $= 7618053821224285687383466174720252396501663499416\alpha$
   $+5910267516953452268669659762088222325143176074230$,
   $(\frac{g(S)}{g(T)})^{\frac{p^2-1}{n}} = 1354335315181821211682485365859218098755278877378\alpha$
   $+8654410318384179317451981196322210287393432354847$.
   The time of computation :

   computation of $f(S)$: 39667 sec, computation of $f(T)$: 40023 sec,
   computation of $g(S)$: 39634 sec, computation of $g(T)$: 39646 sec,
   computation of $(\frac{f(S)}{f(T)})^{\frac{p^2-1}{n}}$: 116 sec, computation of $(\frac{g(S)}{g(T)})^{\frac{p^2-1}{n}}$: 136 sec.

3) Solve the DLP
   $(5010350267319872795048848896836646242920060597592\alpha$

$+684597904528238743074511834101748764895625936788 9)^l$
$= 1354335315181821211682485365859218098755278877378\alpha$
$+8654410318384179317451981196322210287393432354847$ in $\mathbb{F}^*_{p^2}$,
find $l = 388267735689900037826187381399337 8$.

(MOV reduction): Let R, S be as in FR reduction.

1) Compute $Q = (x_4, y_4) = [\frac{p+1}{n}]S$ with order n.
$x_4 = 268607399899856195293423320463290449641853638513 8$,
$y_4 = 769368303013534155401573490515765808450022343909 5\alpha$.
The time of computation Q : 1203 sec.

2) Compute the Weil pairing:
Set $div(f) = n((P + S) - (S))$, $div(g) = n((R + S) - (S))$ and
$div(h) = (Q + T) - (T)$,
then
$e_n(P, Q) = \frac{f(Q+T)}{f(T)} \times \frac{h(S)}{h(P+S)}$
$= 5191780390348421007816254381110295818010622599391\alpha$
$+6845979045282387430745118341017487648956259367889$,
$e_n(R, Q) = \frac{g(Q+T)}{g(T)} \times \frac{h(S)}{h(R+S)}$
$= 8847795342486472591182617912087723962175404319605\alpha$
$+8654410318384179317451981196322210287393432354847$.
The time of computation:

computation of $f(Q + T)$: 39972 sec, computation of $f(T)$: 39720 sec,
computation of $h(S)$: 39626 sec, computation of $h(P + S)$: 39850 sec,
computation of $g(Q + T)$: 39992 sec, computation of $g(T)$: 39956 sec,
computation of $h(R + S)$: 39862 sec.

3) Solve the DLP:
$(5191780390348421007816254381110295818010622599391\alpha$
$+6845979045282387430745118341017487648956259367889)^l$
$= 8847795342486472591182617912087723962175404319605\alpha$
$+8654410318384179317451981196322210287393432354847$ in $\mathbb{F}^*_{p^2}$,
find $l = 3882677356899000378261873813993378$.

When we implement the FR and MOV reductions, two random points are needed. The numbers of function values needed to compute the pairings for the FR and MOV reductions are four and seven, respectively. In the both reductions, the computation of function values dominates the whole computation time (Table 1).

From the implementation data and the above consideration, the computation of function values needed to implement the FR and MOV reductions may be a heavy load. For each reduction, the computation of pairings actually dominates the whole computation time while other steps theoretically take $O((\log q)^3)$ as well. We find that the running time of the FR reduction is almost 4/7 times as much as that of the MOV reduction.

Table 1. The time of computation in Examples 1-4

Type	$\log q$	k	Running time(sec)	
Example 1	46	1	FR reduction	419
Example 2	108	1	FR reduction	4105
Example 3	46	2	FR reduction	999
			MOV reduction	1872
Example 4	164	2	FR reduction	161467
			MOV reduction	282426

$\log q$ and k are the binary size of the definition field and the necessary minimum extension degree, respectively.

4 Comparing the (Extended) MOV and FR Reductions

We extended the MOV reduction so that it can be applied to some non-supersingular ECs, and implemented the FR reduction to understand the whole process. Now time to compare the two reductions.

4.1 On the Extension Degrees

Bad news for the MOV reduction is the following fact on group structures, which is due to R. Schoof [19]

Proposition 2 ([20]) *The following two conditions are equivalent:*

1. $E[n] \subseteq E(\mathbb{F}_{q^k})$;
2. $n | q^k - 1$, $n^2 | \# E(\mathbb{F}_{q^k})$, *and either* $\phi \in Z$ *or* $\mathcal{O}(\frac{t_k^2 - 4q^k}{n^2}) \subseteq \mathrm{End}_{\mathbb{F}_{q^k}}(E)$,

where ϕ *and* t_k *denote the* q^k*-Frobenius endomorphism of* $E/\mathbb{F}_{q^k}$ *and its trace, respectively, and* $\mathcal{O}(\frac{t_k^2-4q^k}{n^2})$ *and* $End_{\mathbb{F}_{q^k}}(E)$ *are the order of discriminant* $\frac{t_k^2-4q^k}{n^2}$ *and the endomorphism ring of* $E/\mathbb{F}_{q^k}$ *in which the isogenies are defined over* $\mathbb{F}_{q^k}$, *respectively.*

In this sense, the condition under which the FR can be applied generally includes the one under which the MOV can be applied.

On the contrary, here's good news for the MOV reduction: the difference is not so large between the two conditions for extension degree k under which the MOV and FR reductions can be applied. In fact, R. Balasubramanian and N. Koblitz [5] proved the following:

Proposition 3 ([5]) *Suppose* $n | \# E(\mathbb{F}_q)$, *and that* n *is a prime with* $p \neq n$, $n \not| q - 1$. *Then,*

$$E[n] \subseteq E(\mathbb{F}_{q^k}) \Longleftrightarrow n | q^k - 1$$

Based on the proof of Proposition 3 [5], we show the following result that provides us with important information for comparing the extension degrees for the MOV and FR reductions although it may be clear from Ref. [5].

Remark 1 *Suppose $E[n] \not\subseteq E(\mathbb{F}_q)$, and that n is a prime. If $n | q-1$*

$$E[n] \subseteq E(\mathbb{F}_{q^k}) \Longleftrightarrow k = nj \text{ with } j \geq 1$$

Proof: We pick the basis $\{P, T\}$ of $E[n]$ so that the matrix expression on $E[n]$ of the q-Frobenius endomorphism ϕ is given by

$$M_\phi = \begin{pmatrix} 1 & a \\ 0 & q \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}_n) \ .$$

(Recall $q \equiv 1 \bmod n$.) Then, the matrix that ϕ^k expresses is $M_{\phi^k} = \begin{pmatrix} 1 & ka \\ 0 & 1 \end{pmatrix}$. Thus,

$$\phi^k(T) = T \Leftrightarrow ka \equiv 0 \bmod n \Leftrightarrow k \equiv 0 \bmod n \ ,$$

where we have used $a \not\equiv 0 \bmod n$ since $E[n] \not\subseteq E(\mathbb{F}_{q^k})$. Thus, $k = nj$ with $j \geq 1$.

□

If $E[n] \not\subseteq E(\mathbb{F}_q)$ and $n | q-1$, Remark 2 implies that the extension degree k is no less than n, which further means that an exponential number of extensions are needed in the MOV reduction. Hence, then, we will have to give up applying the MOV reduction.

4.2 On the Efficiency of the Reductions

In the following, assuming $n \not| q-1$, we compare the efficiency of the MOV and FR reductions.

We exclude the following computation in the pre-processing:

1. counting $\#E(\mathbb{F}_q)$, say by Schoof's algorithm [20,6,2], and
2. factoring $\#E(\mathbb{F}_q)$.

Moreover, suppose that the DLP that is obtained by the both reductions from the ECDLP essentially has the same difficulty. Then, all we should compare is the main part of the reductions, i.e. Steps 2-3 in Algorithms 1 and Step 2-5 in Algorithm 2.

However, as considered in Section 2, compared to the FR reduction, additional computation is needed to find the group structure for $E(\mathbb{F}_{q^k})$ for the proposed MOV reduction, although it is computed in a subexponential time.

Moreover, as for application of the MOV reduction, we must give up the application if $e \geq 1$ in Theorem 1. Besides, we should notice that computing the Weil pairing requires almost twice time that the pairing in the FR reduction takes.

4.3 The Actual Difference of the Conditions Between the Two Reductions

At present, we find that there are still two conditions under which the FR can be applied but the MOV cannot:

1. $n|q-1$; and
2. $E[n] \subseteq E(\mathbb{F}_{q^k})$, $c_2 n | c_1$.

Besides, the factorization of $\#E(\mathbb{F}_{q^k})$ is needed to apply Miller's algorithm. (This might be solved immediately because Miller's algorithm sometimes does not require complete factorization.)

Even if the second condition is cleared in the future, the FR reduction is superior to the MOV reduction for the computation of the main part, i.e. for computing the pairings, the MOV requires almost twice time that the FR takes.

In this regard, we must conclude that practically, in any situation the FR reduction is better than the MOV reduction from an algorithmic point of view.

Acknowledgement

Authors would like to thank the program commitee for their comments.

References

1. L. Adleman, J. DeMarrais, and M. Huang, *A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields*, Algorithmic Number Theory, Lecture Notes in Computer Science, volume 877, Springer-Verlag, 1994, pp. 28-40.
2. A. O. Atkin, *The number of points on an elliptic curve modulo a prime*, preprint, 1988.
3. A. Atkin and F. Morain, *Elliptic curves and primality proving*, Mathematics of Computation **61** (1993), 29-68.
4. E.Bach,*Algorithmic Number Theory, Volume I; Efficient Algorithms*, MIT Press, Cambridge, Massachusetts, 1996.
5. R. Balasubramanian and N. Koblitz, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, Journal of Cryptography **11** (1998), 141-145.
6. N. Elkies, *Explicit isogenies*, preprint, 1991.
7. G. Frey and H. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation **62** (1994), 865-874.
8. M. Kac, *On the notion of recurrence in discrete stochastic processes*, Ann. of Math. Statist., **53** (1947), 1002-1010.
9. N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation **48** (1987), 203-209.
10. N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, New York, 2nd edition, 1996.

11. H. W. Lenstra, *Factoring integers with elliptic curves.* Annals of Mathematics, 126 (1987), 649-673.
12. R. Lercier and F. Morain, *Counting the number of points on elliptic curves over finite fields: strategy and performance*, Advances in Cryptology, EUROCRYPT'95, Lecture Notes in Computer Science 921 (1995), 79-94.
13. A. Menezes, T. Okamoto, and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **39** (1993), 1639-1646.
14. A. Menezes, *Elliptic curve public key cryptosystems*, Kluwer Academic Publishes (1994).
15. V. S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptography CRYPTO '85 (Lecture Notes in Computer Science, vol 218), Springer-Verlag, 1986, pp. 417-426.
16. V. Miller, *Short program for functions on curves*, unpublished manuscript, 1986.
17. S.C.Pohlig and M.E.Hellman, *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Transactions on Information Theory, **24** (1978),pp 106-110.
18. T. Satoh and K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, Commentarii Math,Univ,Saniti Pauli, **47** ,1,pp 88 - 92 (1998).
19. R. Schoof, *Nonsingular plane cubic curves over finite fields*, Journal of Combination Theory, Vol. A. 46 (1987), 183-211.
20. R. Schoof, Elliptic curves over finite fields and the computation of square roots modulo p Math. Comp. **44** (1985), 483-494.
21. I. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Mathematics of Computation **67** (1998), 353-356.
22. J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1994.
23. J. H. Silverman, J. Suzuki, *Elliptic curve discrete logarithms and index calculus*, ASIACRYPT'98 (Lecture Notes in Computer Science), to appear.
24. N. Smart, *The discrete logarithm problem on elliptic curves of trace one*, preprint, 1997.
25. J. Tate, *WC-groups over p-adic fields*, ann Sci. Ecole, Norm. Sup. **2** (1969), 521-560