PAPER

New explicit conditions of elliptic curve traces for FR-reduction

Atsuko MIYAJI[†], *Member*, **Masaki NAKABAYASHI**[†], *and* **Shunzou TAKANO**[††], *Nonmembers*

SUMMARY Elliptic curve cryptosystems([19],[25]) are based on the elliptic curve discrete logarithm problem(ECDLP). If elliptic curve cryptosystems avoid FR-reduction([11],[17]) and anomalous elliptic curve over $\mathbb{F}_q$ ([3],[33],[35]), then with current knowledge we can construct elliptic curve cryptosystems over a smaller definition field. ECDLP has an interesting property that the security deeply depends on elliptic curve traces rather than definition fields, which does not occur in the case of the discrete logarithm problem(DLP). Therefore it is important to characterize elliptic curve traces explicitly from the security point of view. As for FR-reduction, supersingular elliptic curves or elliptic curve $E/\mathbb{F}_q$ with trace 2 have been reported to be vulnerable. However unfortunately these have been only results that characterize elliptic curve traces explicitly for FR- and MOV-reductions. More importantly, the secure trace against FR-reduction has not been reported at all. Elliptic curves with the secure trace means that the reduced extension degree is always higher than a certain level.

In this paper, we aim at characterizing elliptic curve traces by FR-reduction and investigate explicit conditions of traces vulnerable or secure against FR-reduction. We show new explicit conditions of elliptic curve traces for FR-reduction. We also present algorithms to construct such elliptic curves, which have relation to famous number theory problems.

key words: *elliptic curve cryptosystems, trace, FR-reduction*

1. Introduction

Koblitz and Miller proposed independently a public key cryptosystem based on an elliptic curve E defined over a finite field $\mathbb{F}_q$ $(q = p^r)$([19],[25]). If elliptic curve cryptosystems satisfy so called FR-conditions ([11],[17],[24]) and avoid anomalous elliptic curve over $\mathbb{F}_q$ ([3],[33],[35]), then the only known attacks are the Pollard ρ-method ([27]) and the Pohlig-Hellman method ([26]). Hence with current knowledge, we can construct elliptic curve cryptosystems over a smaller definition field than the discrete logarithm problem (DLP)-based cryptosystems like the ElGamal cryptosystems ([13]) or the DSA ([12]) and RSA cryptosystems ([28]). Elliptic curve cryptosystems with a 160-bit key are thus believed to have the same security as both the ElGamal cryptosystems and RSA cryptosystems with a 1,024-bit key.

Recently some researches on comparing MOV and FR-reductions have been reported in [15], [18]. These attacks imbed a subgroup $< G > \subset E(\mathbb{F}_q)$ to $\mathbb{F}^*_{q^k}$ for an extension field $\mathbb{F}_{q^k}$ and reduce ECDLP based on $< G > \subset E(\mathbb{F}_q)$ to DLP based on a subgroup of $\mathbb{F}^*_{q^k}$, where $G \in E(\mathbb{F}_q)$ is called a basepoint for ECDLP. MOV-reduction reduces ECDLP to DLP by using the Weil pairing ([34]). Supersingular elliptic curves ([34]) have been reported to be vulnerable against MOV-reduction, which can be easily recognized by the trace t of the q^{th}-power Frobenius endomorphism, $t = q + 1 - \#E(\mathbb{F}_q)$: an elliptic curve is supersingular if and only if $t \equiv 0 \pmod{p}$. On the other hand, FR-reduction reduces ECDLP to DLP by using the Tate pairing. FR-reduction can attack elliptic curves with trace 2 in addition to supersingular elliptic curves. In fact, these have been only results that characterize elliptic curve traces explicitly from a point of view of FR- and MOV-reductions. It is interesting that in the case of $E/\mathbb{F}_p$ over a prime field, dangerous elliptic curve traces happen to be equal to 0 (supersingular), 1 (anomalous) and 2, which can be easily recognized from other elliptic curves. Thus ECDLP has an interesting property that the security deeply depends on elliptic curve traces rather than definition fields, which does not occur in the case of DLP. Therefore it is important to characterize elliptic curve trace from the security point of view.

Balasubramanian and Koblitz investigate that extension degrees required to apply both reductions for ECDLP on $G \in E(\mathbb{F}_q)$ with order n are the same if $n \not| q - 1$([4]). Therefore without loss of generality we deal with only FR-reduction. By FR-reduction, ECDLP on $G \in E(\mathbb{F}_q)$ with order n is reduced to DLP on $\mathbb{F}^*_{q^k}$ if and only if $n|q^k - 1$. The probability that elliptic curves are vulnerable against FR-reduction, i.e. the extension degree k is small, is shown to be highly unlikely ([4]): FR-reduction is considered not to be threat in a realistic sense. Nevertheless all but supersingular and trace 2 elliptic curves have not been proved to be secure in a sense that they are strong against FR-reduction. There might

Manuscript received August 31, 2000.
Manuscript revised August 31, 2000.

[†]The author is with Japan Advanced Institute of Science and Technology, Ishikawa-ken, 923-1292 Japan.

[††]The author is with Matsushita Communication Industrial Co., Ltd., Kanagawa-ken, 223-8639 Japan. This work was conducted when he was with JAIST.

exist another trace of elliptic curves which is reduced to at most 6, seriously low, degree extension field, whose trace might not be simple like 0 or 2. In fact, supersingular elliptic curves have rather special properties compared with ordinary elliptic curves([34]), which is thought to cause such a weak factor. However also in the case of ordinary elliptic curves, non-special elliptic curves, there might exist elliptic curve traces with a weak factor.

More importantly, the secure trace against FR-reduction has not been reported yet. Elliptic curves with the secure trace means that the reduced extension degree is always higher than a certain level. This means that the security of ECDLP over $E/\mathbb{F}_q$ is guaranteed by the security of widely known DLP on $\mathbb{F}^*_{q^k}$ with higher k than a certain level since FR-reduction gives an isomorphism between ECDLP over $E/\mathbb{F}_q$ and DLP based on a subgroup of $\mathbb{F}^*_{q^k}$([20]). In another light, the secure trace against FR-reduction is useful for construction of elliptic curve cryptosystems. Let's consider the following requirements: it is desirable that a domain parameter such as an elliptic curve or a basepoint should be chosen independently by each entity or by each application in order to keep security high([1]), and that such an initialization could be done more easily over lower CPU power or smaller memory like a smart card. In such requirements, it would be certainly desirable that an elliptic curve is constructable at least as easy as generating a prime number, which is a dominant step of RSA-key generation([28]). This is why explicit conditions of secure elliptic-curve traces is useful since we can construct easily an elliptic curve with a given specific trace. Apparently SEA algorithm([7],[10], [30], [32]) is not suitable since it requires rather large memory.

In this paper, we aim at characterizing elliptic curve traces by FR-reduction and investigate explicit conditions of traces vulnerable or secure against FR-reduction. Here we summarize our results on new explicit conditions of elliptic curve traces against FR-reduction.

• Let $E/\mathbb{F}_q$ be an elliptic curve with prime order and the trace t.

∘ **Theorem 2**: ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^3}$ by FR-reduction

$\Leftrightarrow$ (i) (q,t) can be represented by $q = 12l^2 - 1$ and $t = -1 \pm 6l$ $(l \in \mathbb{Z})$,or

(ii) (q,t) can be represented by $q = p^r$ (r is even) and $t = \pm\sqrt{q}$ (i.e. supersingular elliptic curves).

∘ **Theorem 3**: ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^4}$ by FR-reduction

$\Leftrightarrow$ (i) (q,t) can be represented by $q = l^2 + l + 1$ and $t = -l, l+1$ $(l \in \mathbb{Z})$, or

(ii) (q,t) can be represented by $q = 2^r$ (r is odd) and $t = \pm\sqrt{2q}$ (i.e. supersingular elliptic curves).

∘ **Theorem 4**: ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^6}$ by FR-reduction

$\Leftrightarrow$ (i) (q,t) can be represented by $q = 4l^2 + 1$ and $t = 1 \pm 2l$ $(l \in \mathbb{Z})$, or

(ii) (q,t) can be represented by $q = 3^r$ and $t = \pm\sqrt{3q}$ (r is odd) (i.e. supersingular elliptic curve).

Up to the present, it has not been reported whether there exist another elliptic curve trace, except supersingular and trace 2, reduced to at most 6-degree extension field or not. However, our explicit conditions mean that prime-order elliptic curves are reduced to at most 6-degree extension field if and only if they satisfy at least one of conditions of Theorems 2, 3 and 4.

• Let ECDLP on $E(\mathbb{F}_q)$ with the trace t be reduced to DLP on $\mathbb{F}^*_{q^k}$.

∘ **Theorem 5**: If $t \geq 3$, then the extension degree k satisfies

$$k \geq \frac{\log q}{\log(t-1)} - \varepsilon,$$

where ε is a real number such that $\frac{1}{10} > \varepsilon > 0$.

∘ **Corollary 4**: Let $t = 3$. Then the extension degree k satisfies

$$k > \log q - \varepsilon.$$

Theses are the first explicit elliptic-curve-trace conditions on which reduced extension degrees are always higher than a certain level. In the case of $E/\mathbb{F}_p$, dangerous elliptic curve traces happen to be equal to 0, 1 and 2. To the contrary, our result shows that $E/\mathbb{F}_p$ with trace 3 is secure against FR-reduction.

Furthermore, we present an algorithm to construct elliptic curves with the above conditions and present some examples.

This paper is organized as follows. Section 2 summarizes MOV- and FR-reductions. Section 3 investigates new explicit conditions vulnerable or secure against FR-reduction by showing Theorem 2, 3, 4, and 5. Section 4 shows algorithms to construct elliptic curves with new explicit conditions. Section 5 presents some examples.

2. MOV-reduction and FR-reduction

In this section, we summarize MOV- and FR-reductions against ECDLP on $G \in E(\mathbb{F}_q)$ with order n. Here the n-torsion subgroup is denoted by $E[n] = \{P \in E \mid nP = \mathcal{O}\}$.

We compare MOV-reduction with FR-reduction. In MOV-reduction, ECDLP on G is reduced to DLP for the smallest integer k such

that $E[n] \subset E(\mathbb{F}_{q^k})$. Thus supersingular elliptic curves can be efficiently reduced to $\mathbb{F}^*_{q^k}$ for $k \leq 6$. On the other hand, in FR-reduction ECDLP on G is reduced to DLP for the smallest integer k such that $n|q^k - 1$. If $E[n] \subset E(\mathbb{F}_{q^k})$, then $n|q^k - 1$ ([31]). Therefore such an elliptic curve vulnerable against MOV-reduction is also vulnerable against FR-reduction. In fact FR-reduction works also for elliptic curves with trace 2 efficiently in addition to supersingular elliptic curves.

Table 1 Known explicit conditions for FR-reduction

$\mathbb{F}_q(q = p^r)$	trace(E)	extension degree
$p \not\equiv 1 \pmod 4$ if r is even	0	2
$p \not\equiv 1 \pmod 3$ if r is even	$\pm\sqrt{q}$	3
$p = 2$ and r is odd	$\pm\sqrt{2q}$	4
$p = 3$ and r is odd	$\pm\sqrt{3q}$	6
r is even	$\pm 2\sqrt{q}$	1
$\forall q$	2	1

Balasubramanian and Koblitz ([4]) show that if n is a prime and $n \not| q - 1$, then

$$E[n] \subset E(\mathbb{F}_{q^k}) \Leftrightarrow n \mid q^k - 1.$$

As a result there is no difference between MOV-reduction and FR-reduction except elliptic curves with trace 2. Without loss of generality, we deal with the only FR-reduction in this paper.

Table 1 summarizes known explicit conditions of elliptic curve traces for FR-reduction, where the extension degree k means that ECDLP on $E(\mathbb{F}_q)$ is reduced to DLP on a subgroup of $\mathbb{F}^*_{p^k}$.

As for the probability such that ECDLP is reduced to the lower degree extension field by FR-reduction, Balasubramanian and Koblitz show the next theorem.

Theorem 1 ([4]): Let (p, E) be a randomly chosen pair of a prime p in the interval $M/2 \leq p \leq M$ and an elliptic curve $E/\mathbb{F}_p$ with prime order n. The probability Pr of $n|p^k - 1$ for some $k \leq (\log p)^2$ satisfies

$$Pr < C\frac{(\log M)^9(\log\log M)^2}{M}$$

for $C > 0$. ∎

Theorem 1 says that FR-reduction is highly unlikely to be efficient attack against ECDLP. However we note that Theorem 1 does not describe whether there might exist another explicit criterion of an elliptic curve trace vulnerable or secure against FR-reduction or not. From Table 1, we see that such an explicit condition that gives the extension degree higher than a certain level has not been reported.

3. New explicit conditions for elliptic curve traces

In this section, we investigate new explicit conditions of elliptic curve traces for FR-reduction. Table 2 shows our results, which will be discussed in the following sections.

Table 2 New explicit conditions for FR-reduction

$\mathbb{F}_q(q = p^r)$	t = trace(E)	extension degree k
$12l^2 - 1$	$-1 \pm 6l$	3
$l^2 + l + 1$	$-l, l + 1$	4
$4l^2 + 1$	$1 \pm 2l$	6
$\forall q$	$t \geq 3$	$k \geq \frac{\log q}{\log(t-1)} - \varepsilon$

3.1 New explicit conditions vulnerable against FR-reduction

In this section, we investigate new conditions of which ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on seriously low extension field like $\mathbb{F}_{q^3}$, $\mathbb{F}_{q^4}$, and $\mathbb{F}_{q^6}$, which just occurs in the case of supersingular elliptic curves. Supersingular elliptic curves have rather special properties compared with ordinary elliptic curves([34]), which would no doubt cause such vulnerable factor. Here we show that there exist also vulnerable conditions of traces in the case of ordinary elliptic curves.

Let $E/\mathbb{F}_q$ be an elliptic curve with order $n = \#E(\mathbb{F}_q) = q + 1 - t$, where t is the trace of E. Then we show the conditions of which ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^3}$ by FR-reduction.

Theorem 2: Let $E/\mathbb{F}_q$ be an elliptic curve with prime order n ($q > 64$). ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^3}$ by FR-reduction if and only if one of the following conditions holds,

(i) (q, t) can be represented by $q = 12l^2 - 1$ and $t = -1 \pm 6l$ $(l \in \mathbb{Z})$.

(ii) (q, t) can be represented by $q = p^r$ (r is even) and $t = \pm\sqrt{q}$ (i.e. supersingular elliptic curves).

proof: We assume that ECDLP on $E/\mathbb{F}_q$ with prime order n is reduced to DLP on $\mathbb{F}^*_{q^3}$ by FR-reduction. From the condition of FR-reduction, n satisfies that $n|q^3 - 1$ and $n \not| q - 1$ since n is a prime. Therefore there is an integer λ such that $q^2 + q + 1 = \lambda n$. By setting $n = q + 1 - t$ and $q^2 + q + 1 = (q + 1)^2 - t^2 + t^2 - q$, we get the following equation,

$$(q + 1 - t)(q + 1 + t - \lambda) = q - t^2. \quad (1)$$

By Hasse's Theorem, the trace t satisfies $|t| \leq 2\sqrt{q}$. Hence, (1) satisfies

$$-3 \leq (1 + \frac{1}{q} - \frac{t}{q})(q + 1 + t - \lambda) \leq 1. \quad (2)$$

For the assumption of $q, t \in \mathbb{Z}$ and $q > 64$, we conclude that (q, t) satisfies one of the following equations,

$$q + 1 + t - \lambda = -3, -2, -1, 0, 1 \tag{3}$$

By substituting (3) to (1), we get that (q, t) satisfies the following equations,

$$t^2 + 3t - 4q - 3 = 0, \tag{4}$$
$$t^2 + 2t - 3q - 2 = 0, \tag{5}$$
$$t^2 + t - 2q - 1 = 0, \tag{6}$$
$$t^2 - q = 0, \tag{7}$$
$$t^2 - t + 1 = 0. \tag{8}$$

By simple discussion on the existence of integer solutions for congruence equations, we get that $(t, q) \in \mathbb{Z} \times \mathbb{Z}$ exists if and only if (t, q) satisfies (5) or (7).

In the case of (5), (t, q) is expressed by $t = -1 \pm 6l$ and $q = 12l^2 - 1$ for $l \in \mathbb{Z}$ since $q = p^r$ for a prime p, and $t \in \mathbb{Z}$ satisfies

$$t = -1 \pm \sqrt{3(q+1)}.$$

In the case of (7), (t, q) is expressed by $t = \pm\sqrt{q} = \pm\sqrt{p^r}$ for even integers r. This is just a supersingular elliptic curve.

Conversely, if a prime-order elliptic curve $E/\mathbb{F}_q$ satisfies (i) or (ii) in Theorem 2, then $\#E(\mathbb{F}_q) = n$ satisfies $n|q^3 - 1$. Therefore ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^3}$. ∎

Note that possible order of elliptic curves is given by Deuring([9]) and Waterhouse([17]). In the case of $E/\mathbb{F}_p$, there exactly exists an elliptic curve of type (i) in Theorem 2. In the case of $\mathbb{F}_{2^r}$, there does not exist any elliptic curve of type (i) in Theorem 2, but in the case of $\mathbb{F}_{p^r} (p \geq 3)$ there exists.

We get the next corollary easily from Theorem 2.

Corollary 1: Let $E/\mathbb{F}_q$ be an elliptic curve with trace t. If (q, t) can be represented by $q = 12l^2 - 1$ and $t = -1 \pm 6l (l \in \mathbb{Z})$, then ECDLP on $E(\mathbb{F}_q)$ is reduced to DLP on $\mathbb{F}^*_{q^3}$ by FR-reduction.

proof: Here we set $\#E(\mathbb{F}_q) = n$ and let order of $G \in \boldsymbol{E}(\mathbb{F}_q)$ be m. Then m divides n. From the assumption, $n = 12l^2 \pm 6l + 1$. This yields $12l^2 \equiv \pm 6l - 1 \pmod{n}$. Then by using the relation of both $12l^2 \equiv \pm 6l - 1 \pmod{n}$ and $q = 12l^2 - 1$, we get

$$\begin{aligned} q^3 - 1 &= (12l^2 - 2)((12l^2 - 1)^2 + 12l^2) \\ &\equiv (12l^2 - 2)((\pm 6l - 2)^2 + (\pm 6l - 1)) \pmod{n} \\ &\equiv (12l^2 - 2)(36l^2 \mp 18l + 3) \pmod{n} \\ &\equiv 0 \pmod{n} \\ &\equiv 0 \pmod{m}. \end{aligned}$$

Therefore ECDLP on $\forall < G > \subset E(\mathbb{F}_q)$ is reduced to DLP on $\mathbb{F}^*_{q^3}$ by FR-reduction. ∎

Next we show the conditions of which ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^4}$ by FR-reduction.

Theorem 3: Let $E/\mathbb{F}_q$ be an elliptic curve with prime order n $(q > 36)$. ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^4}$ by FR-reduction if and only if one of the following conditions holds,

(i) (q, t) can be represented by $q = l^2 + l + 1$ and $t = -l,\ l + 1$ for $l \in \mathbb{Z}$.
(ii) (q, t) can be represented by $q = 2^r$ (r is odd) and $t = \pm\sqrt{2q}$ (i.e. supersingular elliptic curves).

proof: We assume that ECDLP on $E/\mathbb{F}_q$ with prime order n is reduced to DLP on $\mathbb{F}^*_{q^4}$ by FR-reduction. From the condition of FR-reduction, n satisfies that $n|q^4 - 1$ and $n \not| q^2 - 1$ since n is a prime. Therefore there is an integer λ such that $q^2 + 1 = \lambda n$. In the same way as Theorem 2, we get the following equation,

$$(q + 1 - t)(q + 1 + t - \lambda) = 2q - t^2. \tag{9}$$

From Hasse's Theorem, (9) satisfies that

$$-2 \leq (1 + \frac{1}{q} - \frac{t}{q})(q + 1 + t - \lambda) \leq 2. \tag{10}$$

In the same discussion as Theorem 2, we get that $(t, q) \in \mathbb{Z} \times \mathbb{Z}$ exists if and only if (t, q) satisfies

$$t^2 - 2q = 0, \tag{11}$$
$$t^2 - t - q + 1 = 0. \tag{12}$$

In the case of (11), t satisfies $t = \pm\sqrt{2q} = \pm\sqrt{2p^r}$ for $p = 2$ and an odd positive integer r. This is just a supersingular elliptic curve. In the case of (12), (t, q) is expressed by $t = -l, l + 1$ and $q = l^2 + l + 1$ for $l \in \mathbb{Z}$ since $t \in \mathbb{Z}$ satisfies

$$t = \frac{1 \pm \sqrt{4q - 3}}{2}.$$

Apparently if a prime-order elliptic curve $E/\mathbb{F}_q$ satisfies (i) or (ii) in Theorem 3, then ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^4}$. ∎

The next corollary follows from Theorem 3.

Corollary 2: Let $E/\mathbb{F}_q$ be an elliptic curve with trace t. If (q, t) can be represented by $q = l^2 + l + 1$ and $t = -l,\ l + 1$ for $l \in \mathbb{Z}$, then ECDLP on $E(\mathbb{F}_q)$ is reduced to DLP on $\mathbb{F}^*_{q^4}$ by FR-reduction.

In the same way as Theorems 2 and 3, the explicit conditions of which ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^6}$ by FR-reduction are shown as follows.

Theorem 4: Let $E/\mathbb{F}_q$ be an elliptic curve with prime order n. ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^6}$ by FR-reduction if and only if one of

the following conditions holds,
(i) (q,t) can be represented by $q = 4l^2 + 1$ and $t = 1 \pm 2l$ for $l \in \mathbb{Z}$.
(ii) (q,t) can be represented by $q = 3^r$ and $t = \pm\sqrt{3q}$ for an odd integer r (i.e. supersingular elliptic curve).

Corollary 3: Let $E/\mathbb{F}_q$ be an elliptic curve with trace t. If (q,t) can be represented by $q = 4l^2 + 1$ and $t = 1 \pm 2l$ for $l \in \mathbb{Z}$, then ECDLP on $E/\mathbb{F}_q$ is reduced to DLP on $\mathbb{F}^*_{q^6}$ by FR-reduction.

Remark 1: Theorems 2, 3, and 4 use the fact that the k-th cyclotomic polynomial is decomposed into at most 2-degree irreducible polynomials over $\mathbb{Z}$ in the case of $k = 3$, 4, and 6, respectively. For other cases of k, the same discussion might be used if the k-th cyclotomic polynomial is decomposed into irreducible polynomials with rather small degrees over $\mathbb{Z}$.

3.2 New explicit conditions secure against FR-reduction

In this section, from a secure point of view we investigate a new explicit condition of elliptic curve traces on which the reduced extension degree is always higher than a certain level. As for the known results on $E/\mathbb{F}_p$, dangerous elliptic curves happen to be small traces like 0, 1 and 2. However, on the contrary, our results of Theorems 2, 3 and 4 suggest that the elliptic curve trace whose order is near upper bound in Hasse's Theorem([34]) should be vulnerable. As a result, we show that the extension degree is higher than a certain level when the positive trace except for $t = 0, 1$ and 2 is small enough.

Theorem 5: Let $E/\mathbb{F}_q$ be an elliptic curve with prime order n ($q > 861$), ECDLP on $E(\mathbb{F}_q)$ be reduced to DLP on $\mathbb{F}^*_{q^k}$, and t be the elliptic curve trace. If $t \geq 3$, then the extension degree k satisfies

$$k \geq \frac{\log q}{\log(t-1)} - \varepsilon,$$

where ε is a real number such that $\frac{1}{10} > \varepsilon > 0$.

proof: ECDLP on $E(\mathbb{F}_q)$ is reduced to DLP on $\mathbb{F}_{q^k}$ if and only if

$$q^k \equiv 1 \pmod{n}. \tag{13}$$

By substituting $n = q + 1 - t$ to (13), we get that k is the smallest integer satisfying

$$(t-1)^k \equiv 1 \pmod{n}. \tag{14}$$

From the assumption and Hasse's theorem, t satisfies $3 \leq t \leq 2\sqrt{q} \ll q \approx n$. Therefore

$$1 < (t-1)^k < n < n+1$$

if $1 \leq k < \frac{\log n}{\log(t-1)}$. Then it follows that the smallest integer k such that $(t-1)^k \equiv 1 \pmod{n}$ is greater than or equal to $\frac{\log n}{\log(t-1)}$. Furthermore by substituting $n = q + 1 - t$, we get that

$$k \geq \frac{\log q}{\log(t-1)} - \varepsilon,$$

where $\varepsilon = -\log_{t-1}(1 - \frac{t-1}{q})$. By using the relation of $3 \leq t \leq 2\sqrt{q}$, we get easily that

$$0 < \varepsilon < -\log_{t-1}(1 - \frac{2}{\sqrt{q}} + \frac{1}{q}) < \frac{1}{10},$$

if $q > 861$. Apparently the larger q is, the smaller ε is. Thus the lower bound of extension degree is given by

$$k \geq \frac{\log q}{\log(t-1)} - \varepsilon.$$

∎

The above theorem gives a lower bound of extension degree k in the case of small $t \geq 3$, which ensures the security of ECDLP over $E/\mathbb{F}_q$ by that of widely known DLP on $\mathbb{F}^*_{q^k}$.

The next corollary easily follows from Theorem 5.

Corollary 4: Let $E/\mathbb{F}_q$ be an prime order elliptic curve with $t = 3$ ($q > 861$) and ECDLP on $E(\mathbb{F}_q)$ be reduced to DLP on $\mathbb{F}^*_{q^k}$. Then the extension degree k satisfies

$$k > \log q - \varepsilon,$$

where ε is a real number such that $\frac{1}{10} > \varepsilon > 0$.

Remark 2: The extension degree $k < \log q$ means that FR-reduction gives a subexponential attack against ECDLP under the index calculus method([8]), which runs over any field $\mathbb{F}_q$ in time $L_q[1/2, c] = \exp((c+O(1))(\log q)^{1/2}(\log\log q)^{1/2})$. On the other hand, the extension degree $k < (\log q)^2$ means that FR-reduction gives a subexponential attack against ECDLP under the number field sieve([14]) which runs over some fields $\mathbb{F}_q$ in time $L_q[1/3, c] = \exp((c + O(1))(\log q)^{1/3}(\log\log q)^{2/3})$. Therefore in order to construct enough secure elliptic curve cryptosystems it would be desirable that $k \geq (\log q)^2$. However the condition of $k \geq \log q$ in Corollary 4 is not highly optimistic if we estimate under a rather realistic assumption of the discrete logarithm algorithm for definition fields of elliptic curves([8], [29]).

In the case of prime-order elliptic curves $E/\mathbb{F}_p$ with $t = 3$, we will easily see that the following strict condition also holds: the extension degree is just exponential.

Corollary 5: Let $E/\mathbb{F}_p$ be a prime-order elliptic curve with $t = 3$ (i.e. $\#E(\mathbb{F}_p) = p - 2$ is prime). If 2 is a primitive root in $\mathbb{F}_{p-2}$, then the extension degree k such that ECDLP on $E(\mathbb{F}_p)$ is reduced to DLP on $\mathbb{F}^*_{p^k}$ satisfies $k = p - 3$.

4. Algorithm

In this section, we describe algorithms to construct elliptic curves vulnerable or secure against FR-reduction in Section 3 and confirm that such elliptic curves exist in a realistic sense (i.e. constructable). From the point of view of theoretical interest, each construction is deeply related to each famous number theory problem: the former is a problem of finding integer solutions of Pell's equation([16]), and the latter is a problem of finding twin prime numbers.

4.1 Construction of elliptic curves reducible to lower extension degree

Here we present an algorithm to construct elliptic curves over $\mathbb{F}_p$ in Corollary 1 since Theorem 2 is a special case of Corollary 1. By using the CM-method([2])†, the dominant step of construction of elliptic curves with both $p = 12l^2-1$ and $t = -1\pm 6l (l \in \mathbb{Z})$ is finding integer solutions (l, y) of $12l^2 \pm 12l - 5 = dy^2$ for a given positive integer $d \equiv 3 \pmod 4$, which is easily transformed into finding integer solutions of an indeterminate equation

$$x^2 - 3dy^2 = 24. \tag{15}$$

From the elementary number theory([36]), all integer solutions (x, y) of (15) is given by

$$x + y\sqrt{3d} = (x_1 + y_1\sqrt{3d})(t_0 + u_0\sqrt{3d})^n,$$

where (t_0, u_0) is the *minimum positive integer solution* on $\epsilon = t_0 + u_0\sqrt{3d} > 0$ of Pell's equation,

$$T^2 - 3dU^2 = 1, \tag{16}$$

and (x_1, y_1) is an integer solution of (15) in the following domain Dom,

$$Dom = \{(x, y) | \sqrt{24} \le x < t_0\sqrt{24},\ 0 \le x < u_0\sqrt{24}\}.$$

Here we call two integer solutions (x, y) and (x', y') of (15) are associated if

$$x + y\sqrt{3d} = \pm(x' + y'\sqrt{3d})(t_0 + u_0\sqrt{3d})^n$$

for $\exists n \in \{0, \pm1, \pm2, \cdots\}$.

After finding an integer solution (x, y) of (15) in the above procedure, the construction of elliptic curves $E/\mathbb{F}_p$ with the trace t easily follows the CM-method. In order to find integer solutions efficiently, we need some techniques specific to (15). Here we show only specific techniques, all of which are proved by simple discussion on the existence of integer solutions for congruence equations.

Lemma 1: If there exists an integer solution (l, y) of $12l^2 \pm 12l - 5 = dy^2$, then $d \equiv 19 \pmod{24}$.

proof: From $dy^2 = 12l^2 \pm 12l - 5 = 12l(l \pm 1) - 5 \equiv 19 \pmod{24}$, we get $dy^2 \equiv 19 \pmod{24}$. By using the fact of $y^2 \equiv 0, 1, 4, 9, 12, 16 \pmod{24}$, we get that $d \equiv 19 \pmod{24}$ if there exists an integer solution of $dy^2 \equiv 19 \pmod{24}$. ∎

Lemma 2: Let $d \in \mathbb{Z}$ be $d \equiv 19 \pmod{24}$. If there exists an integer solution (x_0, y_0) of (15), then $\gcd(x_0, y_0) = 1$.

proof: Let (x, y) be an integer solution of (15) and $\gcd(x, y) = g > 1$. Then $g = 2$ since $g^2|24$. So we can set $x = 2x'$ and $y = 2y'$ $(x', y' \in \mathbb{Z})$ with $\gcd(x', y') = 1$. From the assumption of $d \equiv 19 \pmod{24}$, (x', y') satisfies $x'^2 + 3y'^2 \equiv 6 \pmod{12}$. This is contradictory because there does not exist any integer solution (x, y) of $x^2 + 3y^2 \equiv 6 \pmod{12}$. ∎

Corollary 6: Let $d \in \mathbb{Z}$ be $d \equiv 19 \pmod{24}$. If there exists an integer solution (x_0, y_0) of (15), then both x_0 and y_0 are odd.

proof: This follows from Lemma 2. ∎

Lemma 3: Let $d \in \mathbb{Z}$ be $d \equiv 19 \pmod{24}$ and (x_0, y_0) be a set of integer solutions of (15). Then both (x_0, y_0) and $(x_0, -y_0)$ are not associated.

proof: Two solutions (x, y) and (x', y') of (15) are associated if and only if $xy' - x'y \equiv 0 \pmod{24}$ (see Section 34 in [36]). Therefore if both (x_0, y_0) and $(x_0, -y_0)$ are associated, then $2x_0y_0 \equiv 0 \pmod{24}$. This is contradictory to Corollary 6. ∎

Lemma 4: Let $d \in \mathbb{Z}$ be $d \equiv 19 \pmod{24}$. Then there are at most two integer solutions in Dom for (15).

proof: From Lemma 2, there exist an integer solution s satisfying the following conditions:

$12d = s^2 - 96m$, $\gcd(24, s, m) = 1$,

†The procedure of the CM-method includes a step of computing the Hilbert class polynomials([23]), $P_d(x)$. The computation of the Hilbert class polynomials are not so easy if the degree of the Hilbert class polynomial, $\deg(P_d(x))$, namely the class number is large. Therefore we usually fix d and so $P_d(x)$ beforehand in order to avoid the computation of $P_d(x)$ as we will see in Algorithm 2. In another way, we may make use of the recent researches([5], [6]) on the construction of the CM elliptic curves by both the CM tests and liftings instead of the CM-method.

$s^2 \equiv 12d \pmod{96}$, and $-24 \leq s < 24$,
if there exist an integer solution (x, y) in Dom for (15)(see Section 35 in [36]). From the simple discussion on the existence of integer solutions for congruence equations, there are at most two integer solutions s satisfying the above conditions. Therefore there are at most two integer solutions in Dom for (15). ∎
The next proposition follows from Lemmas 3 and 4.

Proposition 1: Let $d \in \mathbb{Z}$ be $d \equiv 19 \pmod{24}$. Then there exist just two sets of integer solutions in Dom for (15) if there exist.

Here we give the algorithm as follows:

Algorithm 1: Given the upper bound $UP > 0$ on a prime p, this algorithm outputs (p, d, l), or *fail* if such a (p, d, l) does not exist.

1. Choose a positive integer d such that $d \equiv 19 \pmod{24}$.
2. Find the minimum positive integer solution (t_0, u_0) of (16).
3. Find an integer solution $(x, y) \in Dom$ of (15), if exists.
   Otherwise, output *fail* and terminate the algorithm.
4. For $n \geq 1$, set x_n, y_n in such a way that
   $x_n + y_n\sqrt{3d} := (x + y\sqrt{3d})(t_0 + u_0\sqrt{3d})^n$.
5. Set $l_{1,n} := (x_n - 3)/6$, $l_{2,n} := (x_n + 3)/6$, $p_{1,n} := 12l_{1,n}^2 - 1$, and $p_{2,n} = 12l_{2,n}^2 - 1$.
6. If $p_{1,n} > UP$ and $p_{2,n} > UP$, then output *fail* and terminate the algorithm.
7. If $p_{1,n}$ or $p_{2,n}$ is prime, then output $(p_{1,n}, d, l_{1,n})$ or $(p_{1,n}, d, l_{2,n})$ respectively, and terminate the algorithm.
   Otherwise goto 4.

4.2 Construction of elliptic curves reducible to higher extension degree

Here we present an algorithm to construct elliptic curves $E/\mathbb{F}_p$ with $t = 3$ in Corollary 4, in which the CM-method is also used in the same way as Section 4.1. By using the CM-method, the dominant steps of construction of prime-order elliptic curves $E/\mathbb{F}_p$ with $t = 3$, namely $\#E(\mathbb{F}_p) = p - 2$, are finding a prime number $p = dl^2 + dl + \frac{d+9}{4}$ with $l \in \mathbb{Z}$ for an given positive integer $d \equiv 3 \pmod 4$, and checking $p - 2$ is also prime.

In this case we can easily show the following condition of d.

Lemma 5: Let $p \in \mathbb{Z}$ be $p = dl^2 + dl + \frac{d+9}{4}$ with a positive integer $d \equiv 3 \pmod 4$. If both p and $p - 2$ are prime, then $d \equiv 19 \pmod{24}$.

proof: For the assumption of $d \equiv 3 \pmod 4$, we set $d = 3 + 4m$ ($m \in \mathbb{Z}$). Then

$$\begin{aligned} p &= dl^2 + dl + \frac{d+9}{4} \\ &= dl(l+1) + (m+3) \qquad (17) \\ &\equiv m + 1 \pmod 2. \qquad (18) \end{aligned}$$

Since p is prime, $m \equiv 0 \pmod 2$ from (18). So we can set $d = 3 + 8m'$ ($\exists m' \in \mathbb{Z}$). On the other hand, we get $p \equiv 1 \pmod 6$ since both p and $p - 2$ are prime and also get easily $l(l+1) \equiv 0, 2 \pmod 6$ for $\forall l \in \mathbb{Z}$. If $l(l+1) \equiv 0 \pmod 6$, then $m' \equiv 2 \pmod 3$ from (17). This yields $d \equiv 19 \pmod{24}$. If $l(l+1) \equiv 2 \pmod 6$, then this yields contradictory. In this way we get $d \equiv 19 \pmod{24}$. ∎
Here we give the algorithm as follows:

Algorithm 2: Given the upper bound $UP > 0$ on a prime p, this algorithm outputs a prime-order elliptic curve $E/\mathbb{F}_p$ with $t = 3$, or *fail* if such an $E/\mathbb{F}_p$ does not exist.

1. Choose a positive integer d such that $d \equiv 19 \pmod{24}$.
2. Set $p = dl^2 + dl + \frac{d+9}{4}$, $\mathbb{Z} \ni l > 0$.
3. If $p > UP$, then output *fail* and terminate the algorithm.
   Otherwise goto step 4.
4. If both p and $p-2$ are prime, then goto step 5. Otherwise goto step 2 and try the next l.
5. Compute the Hilbert class polynomial $P_d(x)$.
6. Solve a root j_0 of $P_d(x) \equiv 0 \pmod p$.
7. Construct two elliptic curves E_{j_0} and E'_{j_0},
   $E_{j_0} : y^2 = x^3 + a_{j_0}x + b_{j_0}$,
   $E'_{j_0} : y^2 = x^3 + a_{j_0}c^2x + b_{j_0}c^3$,
   where $a_{j_0} = \frac{3j_0}{1728 - j_0} \pmod p$,
   $b_{j_0} = \frac{2j_0}{1728 - j_0} \pmod p$, and
   c is any quadratic non-residue in $\mathbb{F}_p$.
8. Output $E \in \{E_{j_0}, E'_{j_0}\}$ with $\#E(\mathbb{F}_p) = p - 2$ and terminate the algorithm.

Note that the step 8 can be performed easily: output E such that $(p-2)G = \mathcal{O}$ for $\boldsymbol{E}(\mathbb{F}_p) \ni \exists G \neq \mathcal{O}$.

5. Experimental results

In this section, we present some examples in both vulnerable and secure cases.

5.1 Elliptic curves reducible to lower extension degree

We present one example which satisfies the condition of Corollary 1. We searched elliptic curves $E/\mathbb{F}_p$ in the range of $0 < p < 2^{1000}$ by using Algorithm 1. Our modulo arithmetic uses the GNU MP Library GMP([37]). The platform is an Alpha

21264(500 MHz/C Compiler for Digital UNIX). It took on the average 0.101 sec to find an elliptic curve $E/\mathbb{F}_p$ in the case of $d = 19$. We have also confirmed experimentally that vulnerable elliptic curves with new explicit conditions are constructable systematically in the same way as supersingular or trace 2 elliptic curves. This means that even in the case of ordinary elliptic curves, we must check FR-conditions.

Recently some researches([21], [22]) on a protocol using an elliptic curve $E/\mathbb{F}_p$ with the *computable* FR-reduction have been proposed, in which an elliptic curve $E/\mathbb{F}_p$ reduced to $\mathbb{F}_{p^k}$ with the computable lower extension degree is desired. Our approach is also deeply related to their researches.

Example 1:
$E/\mathbb{F}_p : x^3 + ax + b$
p = 9 08761 00379 04279 08077 54895 57583 80356 67582 90265 31247 (170-bit),
a = 8 18416 34259 48882 91485 04408 88116 40789 05308 57899 75506,
b = 6 66070 44332 39783 49780 03588 18034 13282 86571 48420 57992,
$t = -5$ 22138 20118 54029 93899 01413,
$\#E(\mathbb{F}_p) = 7^2 * 313 * n$,
n = 59 25285 28258 73893 72612 30363 15589 78126 20544 05453 (156-bit).

5.2 Elliptic curves reducible to higher extension degree

We present experimental results and some examples of elliptic curves in Corollaries 4 and 5. We have confirmed that secure elliptic curves with new explicit conditions are constructible systematically. Table 3 shows numerical results of twin primes $(p, p-2)$ with $p = dl^2+dl+\frac{d+9}{4}$, which was searched in the range of $2^{76} - 2^{20} \le l \le 2^{76} + 2^{20}$. Our modulo arithmetic uses the GNU MP Library GMP([37]). The platform is an Alpha 21264(500 MHz/C Compiler for Digital UNIX). It took on the average 0.053 sec to find a pair of $(p, p-2)$ in the case of $d = 163$. For other cases of d, we could found such a pair of primes on the average 0.064 $\sim$ 1.402 sec.

Fig.1 shows the plot of Table 3 from the point of view of $\deg(P_d(x))$ and the size of d on $P_d(x)$. From our experimental result, we have found a heuristic property that the number of twin primes are closely related to two factors, $\deg(P_d(x))$ and the size of d on $P_d(x)$. If we fix the size of d, then the larger $\deg(P_d(x))$ is, the less twin primes are found. If we fix $\deg(P_d(x))$, then the larger the size of d is, the more twin primes are found.

We present $E/\mathbb{F}_p : y^2 = x^3 + ax + b$ with $t = 3$ in the following. In Examples 2 $\sim$ 4, 2 is a primitive root in $\mathbb{F}_{p-2}$.

Table 3 The number of twin primes $(p, p-2)$

d	$\deg(P_d(x))$	# twin primes	times (sec)
19	1	190	0.55097
43	1	1,157	0.094596
67	1	1,902	0.064297
91	2	450	0.365852
115	2	1,036	0.209392
139	3	139	0.323987
163	1	5,158	0.053331
187	2	1,402	0.107929
211	3	292	1.401844
235	2	2,523	0.089963
259	4	247	0.348319
283	3	645	0.234224
307	3	696	0.134928
331	3	1,458	0.103192
355	4	635	0.261890
379	3	1,583	0.074222
403	2	3,392	0.069164

$p = dl^2 + dl + \frac{d+9}{4}$, $(2^{76} - 2^{20} \le l \le 2^{76} + 220)$

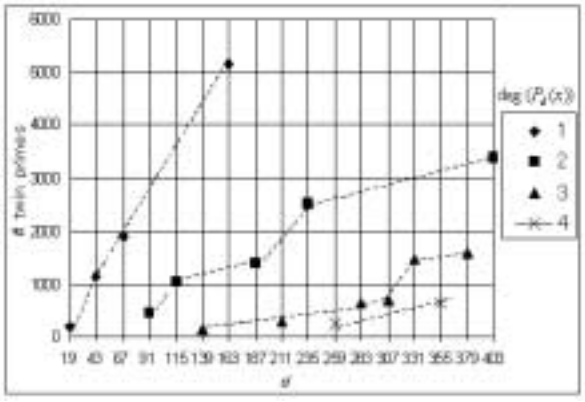


Fig. 1 Relations between # twin primes and $P_d(x)$

Example 2:
$E_1/\mathbb{F}_p : y^2 = x^3 + a_1x + b_1$, $E_2/\mathbb{F}_p : y^2 = x^3 + a_2x + b_2$, $(|p| = 159 - bit)$
p = 519 51816 01449 69382 38659 23754 49686 02163 04833 66071,
n = 519 51816 01449 69382 38659 23754 49686 02163 04833 66069,
a_1 = 35 29380 82819 03345 16798 59515 21747 57876 817006 32697,
b_1 = 408 46477 52610 12095 24877 04686 28212 53233 12948 77155,
a_2 = 43 94541 02577 39111 90178 78324 59422 25137 69507 32067,
b_2 = 375 64238 02684 72329 52558 68052 72738 84867 16227 32092.

Example 3:
$E_1/\mathbb{F}_p : y^2 = x^3 + a_1x + b_1$, $E_2/\mathbb{F}_p : y^2 = x^3 + a_2x + b_2$, $E_3/\mathbb{F}_p : y^2 = x^3 + a_3x + b_3$, $(|p| = 159 - bit)$
p = 793 54971 71445 13671 92705 06772 26939 83458 80422 30471,
n = 793 54971 71445 13671 92705 06772 26939 83458 80422 30469,
a_1 = 622 32433 75781 36504 38145 80347 56708 57012 73203 93428,
b_1 = 679 39946 41002 62226 89665 55822 46785 65828 08943 39109,

a_2 = 546 59131 03249 88457 46494 19390 10636 40227 07442 50852,

b_2 = 364 39420 68833 25638 30996 12926 73757 60151 38295 00568,

a_3 = 261 88075 85593 34219 51163 09691 46231 55329 60288 84192,

b_3 = 179 85880 00172 30155 26919 24926 22984 48533 06563 08058.

Example 4:
$E/\mathbb{F}_p : y^2 = x^3 + ax + b$, ($|p| = 240 - bit$)

p = 112 49846 54526 86189 73518 65205 55113 42541 99281 27068 83806 23265 87119 55023 07023,

n = 112 49846 54526 86189 73518 65205 55113 42541 99281 27068 83806 23265 87119 55023 07021,

a = 52 37381 80880 77183 56601 62811 25609 08710 91667 71974 15904 90057 09224 69377 60775,

b = 34 91587 87253 84789 04401 08540 83739 39140 61111 81316 10603 26704 72816 46251 73850.

Example 5:
$E_1/\mathbb{F}_p : y^2 = x^3 + a_1x + b_1$, $E_2/\mathbb{F}_p : y^2 = x^3 + a_2x + b_2$, $E_3/\mathbb{F}_p : y^2 = x^3 + a_3x + b_3$, ($|p| = 240 - bit$)

p = 145 62684 79172 80895 91487 33486 94032 72646 08218 46342 12380 03553 12226 43548 52871,

n = 145 62684 79172 80895 91487 33486 94032 72646 08218 46342 12380 03553 12226 43548 52869,

a_1 = 144 44371 02824 33267 37769 11780 11326 91187 09134 83450 79361 18648 91066 43377 85210,

b_1 = 50 11979 94855 57136 68786 73438 08285 32827 34850 99302 48151 81056 65622 14743 74505,

a_2 = 26 77304 81723 26198 90654 78404 65044 67257 17139 39775 54321 43896 98924 70624 48137,

b_2 = 66 39098 14206 44431 24265 63432 08040 69053 47499 08631 07007 63782 36691 94932 49715,

a_3 = 47 49197 80769 28734 86477 41659 37707 95433 64827 81423 90680 35668 50843 51479 03933,

b_3 = 31 66131 87179 52489 90984 94439 58471 96955 76551 87615 93786 90445 67229 00986 02622.

6. Conclusion

In this paper, we have shown some new explicit conditions of elliptic curve traces vulnerable or secure against FR-reduction. We have also presented algorithms to construct elliptic curves with our new explicit conditions. Especially our new secure elliptic curve realizes rather light initialization, which sets up a pair of elliptic curve and basepoint.

Acknowledgments

The authors are grateful to anonymous referees for invaluable comments.

References

[1] R. Anderson and R. Needham, "Robustness principles for public key protocols", *Advances in Cryptology-Proceedings of CRYPTO'95*, Lecture Notes in Computer Science, **963**(1995), Springer-Verlag, 236-247.

[2] A. O. L. Atkin and F. Morain, "Elliptic curves and primality proving", *Math. of Computation*, **61**(1993), 29-68.

[3] K. Araki and T. Satoh "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves", *Commentarii Math. Univ. St. Pauli.*, vol. **47** (1998), 81-92.

[4] R. Balasubramanian and N. Koblitz, "The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm", J. Cryptology, **11** (1998), 141-145.

[5] J. Chao, O. Nakamura, K. Sobataka, and S. Tsujii, "Construction of secure elliptic curves with CM tests and lifting", *Advances in Cryptology-Proceedings of ASIACRYPT'98*, Lecture Notes in Computer Science, **1514**(1998), Springer-Verlag, 95-109.

[6] J. Chao, M. Hosoya, K. Sobataka, and S. Tsujii, "Construction of Elliptic Cryptosystems Using Ordinary Lifting", *Proceeding of the 1999 Symposium on Cryptography and Information Security*, 163-166.

[7] J. M. Couveignes and F. Morain, "Schoof's algorithm and isogeny cycles", *Proceedings of the ANTS-I*, Lecture Notes in Compute Science, **877** (1994), Springer-Verlag, 43-58.

[8] T. Denny, O. Schirokauer and D. Weber, "Discrete logarithms: the effectiveness of the index calculus method", *Proceedings of ANTSII* , Lecture Notes in Computer Science, **1122**(1996), Springer-Verlag, 337-361.

[9] M. Deuring, "Die typen der multiplikatorenringe elliptischer funktionenkörper", *Abh. Math. Sem. Hamburg*, **14**(1941), 197-272.

[10] N. D. Elkies, "Explicit isogenies", Preprint, 1991

[11] G. Frey and H. G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of computation*, **62**(1994), 865-874.

[12] "Proposed federal information processing standard for digital signature standard (DSS)", *Federal Register*, **56** No. 169, 30 Aug 1991, 42980–42982.

[13] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Trans. Inform. Theory*, **IT-31** (1985), 469–472.

[14] D. M. Gordon, "Discrete logarithms in $GF(p)$ using the number field sieve", *SIAM J. on Discrete Math.*, **6**(1993), 124-138.

[15] R. Harasawa, H. Imai, J. Shikata, J. Suzuki, "Comparing the MOV and FR Reductions in Elliptic Curve Cryptography", *Advances in Cryptology-Proceedings of EUROCRYPT '99*, Lecture notes in Computer Science, **1592** (1999), 190-205.

[16] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, GTM 84, Springer-Verlag, New-York, 1982.

[17] *IEEE P1363 Working Draft*, June 16, 1998.

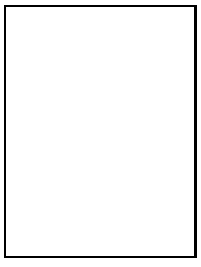
[18] N. Kanayama, T. Kobayashi, T. Saito, and S. Uchiyama "Remarks on elliptic curve discrete logarithm problems" , *IEICE Trans.*, Fundamentals. vol. E83-A, No.1(2000), 17-23.

[19] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, **48** (1987), 203–209.

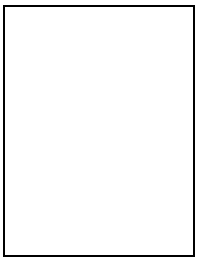
[20] N. Koblitz, "An elliptic curve implementation of the finite field digital signature algotirhm", *Advances in Cryptology-Proceedings of CRYPTO'98*, Lecture Notes in Computer Science, **1462**(1998), Springer-Verlag, 327-337.

[21] M. Kasahara, K. Ohgishi, and R. Sakai "Notes on ID-based key sharing systems on elliptic curve", *IEICE Japan Tech. Rep.*, **ISEC99-57**(1999-11), 37-42.

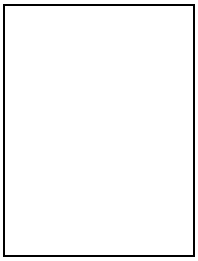
[22] M. Kasahara, K. Ohgishi, and R. Sakai "Cryptosystems based on pairing", *The 2000 Symposium on Cryptography and Information Security*, **SCIS2000-C20**, Jan. 2000.
[23] S. Lang, *Elliptic Functions*, GTM112, Springer-Verlag, New York, 1987.
[24] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing* (1991), 80–89.
[25] V. S. Miller, "Use of elliptic curves in cryptography", *Advances in Cryptology-Proceedings of Crypto'85*, Lecture Notes in Computer Science, **218** (1986), Springer-Verlag, 417-426.
[26] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance", *IEEE Trans. Inf. Theory*, **IT-24** (1978), 106–110.
[27] J. Pollard, "Monte Carlo methods for index computation (mod p)", *Mathematics of Computation*, **32** (1978), 918–924.
[28] R. Rivest, A. Shamir and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, **21** No. 2 (1978), 120–126.
[29] T. Saitoh and S. Uchiyama, "A Note on the Discrete Logarithm Problem on Elliptic Curves of Trace Two", *Technical Report of IEICE*, ISEC98-27(1998), 51-57.
[30] R. Schoof, "Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p", *Mathematics of computation*, **44** (1985), 483–494.
[31] R. Schoof, "Nonsingular plane cubic curves over finite fields", *Jornal of Combination Theory*, vol. A. **46** (1987), 183-211.
[32] R. Schoof, "Counting points on elliptic curve over finite fields", *Journal de Théorie des Nombres de Bordeux*, **7** (1995), 219–254.
[33] I. A. 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.
[34] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag, New York, 1986.
[35] N. P. Smart "The discrete logarithm problem on elliptic curves of trace one", J. Cryptology, **12** (1999), 193–196.
[36] T. Takagi, *Syotou seisuuronn kougi*, Kyouritu Syuppan, 1971, (in Japanese).
[37] Torbjorn Granlund, THE GNU MP LIBRARY, version 3.1, August 2000. ftp://ftp.gnu.org/gnu/gmp/gmp-3.1.tar.gz



Atsuko Miyaji received the B. Sc., the M. Sc., and Dr. Sci. degrees in mathematics from Osaka University, Osaka, Japan in 1988, 1990, and 1997 respectively. She joined Matsushita Electric Industrial Co., LTD from 1990 to 1998 and engaged in research and development for secure communication. She has been an associate professor at JAIST(Japan Advanced Institute of Science and Technology) since 1998. Her research interests include the application of projective varieties theory into cryptography and information security. She is a member of the International Association for Cryptologic Research and the Information Processing Society of Japan.



Masaki Nakabayashi received the B.E. in industrial engineering from Waseda University in 1999. He has been a student at JAIST since 1999. His research interest is the security of elliptic curve cryptosystems.



Shunzou Takano received the B. Sc. in mathematics from Kanazawa University and the M. info. Sc. from JAIST in 1998 and 2000 respectively. He had researched the security of elliptic curve cryptosystems. He has joined Matsushita Communication Industrial Co., Ltd since 2000 and engages in standardization and development for the mobile internet and electronic technologies.