IEICE TRANS. FUNDAMENTALS, VOL.E94–A, NO.6 JUNE 2011

PAPER Special Section on Discrete Mathematics and Its Applications

New Concrete Relation between Trace, Definition Field, and Embedding Degree*

Shoujiro HIRASAWA[†], *Nonmember and* **Atsuko MIYAJI**[††a)], *Member*

SUMMARY A pairing over an elliptic curve $E/\mathbb{F}_{p^m}$ to an extension field of $\mathbb{F}_{p^{mk}}$ has begun to be attractive in cryptosystems, from the practical and theoretical point of view. From the practical point of view, many cryptosystems using a pairing, called the pairing-based cryptosystems, have been proposed and, thus, a pairing is a necessary tool for cryptosystems. From the theoretical point of view, the so-called embedding degree k is an indicator of a relationship between the elliptic curve Discrete Logarithm Problem (ECDLP) and the Discrete Logarithm Problem (DLP), where ECDLP over $E(\mathbb{F}_{p^m})$ is reduced to DLP over $\mathbb{F}_{p^{mk}}$ by using the pairing. An elliptic curve is determined by mathematical parameters such as the j-invariant or order of an elliptic curve, however, explicit conditions between these mathematical parameters and an embedding degree have been described only in a few degrees. In this paper, we focus on the theoretical view of a pairing and investigate a new condition of the existence of elliptic curves with pre-determined embedding degrees. We also present some examples of elliptic curves over 160-bit, 192-bit and 224-bit $\mathbb{F}_{p^m}$ with embedding degrees $k < (\log p)^2$ such as $k = 10, 12, 14, 20, 22, 24, 28$.
key words: *elliptic curve, embedding degree*

1. Introduction

The elliptic curve cryptosystem (ECC) chosen appropriately can offer efficient public key cryptosystems [1]. This is why elliptic curve cryptosystems have been desired in various application such as a smart card, whose memory storage and CPU power are very limited. Recently, a pairing over an elliptic curve $E/\mathbb{F}_{p^m}$ has begun to be attractive in cryptosystems from the practical and theoretical point of view. For example, it can achieve an ID-based cryptosystem [5], short signature [2], etc. The cryptosystems using a pairing are called the pairing-based cryptosystems. On the other hand, a pairing is originally used to solve the Elliptic Curve Discrete Logarithm Problem (ECDLP) by reducing ECDLP on $E(\mathbb{F}_{p^m})$ to Discrete Logarithm Problem (DLP) on $\mathbb{F}_{p^{mk}}$ [8], [12], where k is called the embedding degree. The embedding degree k can be considered to be an indicator of the security of ECDLP. Then, the security level of ECDLP over $E(\mathbb{F}_{p^m})$ is the same as that of DLP over $\mathbb{F}_{p^{mk}}$ by using a pairing from $E(\mathbb{F}_{p^m})$ to $\mathbb{F}_{p^{mk}}$.

An elliptic curve $E/\mathbb{F}_{p^m}$ can be determined by parameters of j-invariant or order $\sharp E(\mathbb{F}_{p^m})$. This is one of mathematical facts on elliptic curves. On the other hand, from the point of view of cryptology, we are curious about the relation between an embedding degree and these mathematical parameters of j-invariant or $\sharp E(\mathbb{F}_{p^m})$. The relationship, however, between them has been described only in a few degrees such as $k = 3, 4, 6, 10$, or 12. It is an open problem to describe an embedding degree of an elliptic curve $E/\mathbb{F}_{p^m}$ explicitly by its j-invariant or $\sharp E(\mathbb{F}_{p^m})$. Generally, the embedding degree k for a prime-order elliptic curve is $k \approx n$ where $n = \sharp E(\mathbb{F}_{p^m})$ [3].

A lot of studies to construct elliptic curves having small embedding degrees, such as $k = 2$, 3, 4, 5, 6, 10 and 12, have been investigated. Miyaji, Nakabayashi and Takano [13] have proposed ordinary elliptic curves with embedding degrees $k = 3$, 4 and 6. Galbraith, Valenca, Mackee [9] have presented the factorization of cyclotomic polynomials with degrees 5, 10 and 12, and applied the results [13] to a hyperelliptic curve. Freeman [6] and Barretto and Naehrig [4] have constructed ordinary elliptic curves with embedding degree $k = 10$ and $k = 12$ using the factorization of cyclotomic polynomials in [9], respectively.

Hitt [11] has investigated a Jacobian of hyperelliptic curve $J_C/\mathbb{F}_{2^m}$ and discussed the way to decide an embedding degree k of $J_C(\mathbb{F}_{2^m})$ from order of p in $\mathbb{Z}_n$, where n is the largest prime divisor of $\sharp J_C(\mathbb{F}_{2^m})$. Hitt also gave some examples of $\sharp J_C(\mathbb{F}_{2^m})$ with embedding degrees $k < (\log p^m)^2$. Unfortunately, by her approach, it is not easy to give concrete $J_C/\mathbb{F}_{2^m}$ themselves. However, her approach sheds additional light on the relations between $\sharp J_C(\mathbb{F}_{2^m})$ and the embedding degree of J_C by the simple discussion based on the elementary number theory. There might be still room for further improvement in the following points:

1. Her result cannot construct $\sharp J_C(\mathbb{F}_{2^m})$ with $\rho = \frac{\sharp J_C(\mathbb{F}_{2^m})}{n} \approx 1$. Her results restrict the relation between trace, definition field, and the largest prime divisor. As a result, $\rho > 1$.
2. Her results cannot decide an embedding degree of k of $\sharp J_C(\mathbb{F}_p)$ in the case of a prime field $\mathbb{F}_p$. This means that they suffer from reduction to the actual minimum embedding degree. In fact, the actual security level of her examples is reduced to $\frac{1}{19}$ of their original security level at the minimum and its $\frac{1}{3}$ at the maximum.

In this paper, we investigate the case of elliptic curves by improving the approach to a Jacobian of hyperelliptic curve

Manuscript received October 1, 2010.
Manuscript revised January 11, 2011.
[†]The author was with JAIST.
[††]The author is with Japan Advanced Institute of Science and Technology, Nomi-shi, 923-1292 Japan.
*This study is partly supported by Grant-in-Aid for Exploratory Research (19650002) and the Mitsubishi Foundation. A preliminary version was presented at ISIT 2009 [10].
a) E-mail: miyaji@jaist.ac.jp
DOI: 10.1587/transfun.E94.A.1368

[11]. We prove the new concrete relations between $\mathbb{F}_{p^m}$, $\sharp E(\mathbb{F}_{p^m})$ and the embedding degree of E, which resolves the above her drawbacks. In fact, we improve Hitt's results from the point of view of ρ-value and the actual minimum security. As for ρ-value, we do not place any restriction on the relation between trace and definition field. As a result, we can construct elliptic curves with $\rho = 1$. Furthermore, we can enjoy the case of prime field $\mathbb{F}_p$, and, thus, our results do not suffer from reduction to the minimum embedding degree. We also present some examples of prime orders of elliptic curves over 160-bit, 192-bit and 224-bit $\mathbb{F}_p$ with embedding degrees $k < (\log p)^2$ such as $k = 10, 12, 14, 20, 22, 24, 28$.

This paper is organized as follows. Section 2 summarizes known facts on elliptic curves. In Sect. 3, we review the previous results. Our main contribution appears in Sect. 4, where we show how to decide order of elliptic curves with pre-determined embedding degree. In Sect. 5, we present some experimental results based on Sect. 4. Section 6 compares our results with Hitt's results. Conclusion follows in Sect. 7.

2. Preparation

This section summarizes the known facts on elliptic curves. Let p be a prime, m be a positive integer, and E be an elliptic curve defined over a finite field $\mathbb{F}_{p^m}$. The trace t is defined as $t = p^m + 1 - \sharp E(\mathbb{F}_{p^m})$. The embedding degree is defined as follows.

Definition 1: Let E be an elliptic curve over a finite field $\mathbb{F}_{p^m}$ with $\sharp E(\mathbb{F}_{p^m})$, and n be the largest prime divisor of $\sharp E(\mathbb{F}_{p^m})$. The embedding degree of E is defined as the smallest positive integer k such that $n \mid p^{mk} - 1$.

The k-th cyclotomic polynomial, $\Phi_k(X)$, is defined as the minimum polynomial of k-th root of unity, which satisfies the following features:

$$X^k - 1 = \prod_{d|k} \Phi_d(X).$$

By using the k-th cyclotomic polynomial, we can say that k is the minimal integer such that $n \mid \Phi_k(p^m)$. Further, the following 4 conditions on the embedding degree k of E are equivalent to each other:

1. ECDLP over a subgroup with order n of $E(\mathbb{F}_{p^m})$ is reduced to DLP over that of $\mathbb{F}_{p^{mk}}$.
2. k is the smallest positive integer such that
$$n \mid p^{mk} - 1.$$
3. $\Phi_k(p^m) \equiv 0 \pmod{n}$.
4. $\Phi_k(t-1) \equiv 0 \pmod{n}$.

In this paper, we need the condition that, for a given order n, an elliptic curve $E/\mathbb{F}_{p^m}$ with order n exists. The following Waterhouse's theorem [14] gives conditions that an elliptic curve defined over $\mathbb{F}_{p^m}$ of order $p^m + 1 - t$ exists.

Table 1 Elliptic curves with small embedding degrees.

	k	p^m	t
MNT-Curve[13]	3	$12x^2 - 1$	$-1 \pm 6x$
	4	$x^2 + x + 1$	$-x$ or $x + 1$
	6	$4x^2 + 1$	$1 \pm 2x$
Freeman[6]	10	$25x^4 + 25x^3 + 25x^2 + 10x + 3$	$10x^2 + 5x + 3$
BN-Curve[4]	12	$36x^4 + 36x^3 + 24x^2 + 6x + 1$	$6x^2 + 1$

Theorem 1 ([14]): An elliptic curve defined over $\mathbb{F}_{p^m}$ of order $p^m + 1 - t$ exists if and only if one of the following conditions holds:

1. $t \not\equiv 0 \pmod{p}$ and $t^2 \le 4p^m$.
2. m is odd and one of the following holds:
   - $t = 0$,
   - $t^2 = 2p^m$ and $p = 2$,
   - $t^2 = 3p^m$ and $p = 3$.
3. m is even and one of the following holds:
   - $t^2 = 4p^m$,
   - $t^2 = p^m$ and $p \not\equiv 1 \pmod{3}$,
   - $t = 0$ and $p \not\equiv 1 \pmod{4}$.

3. Previous Results

We summarize previous results that determine the embedding degree explicitly by trace [4], [6], [13] and Hitt's results [11] in detail. Table 1 presents relations between traces t of elliptic curves over $\mathbb{F}_{p^m}$ and their embedding degrees k, where x are integers.

Hitt [11] investigates Jacobians of genus 2 curves J_C over $\mathbb{F}_{2^m}$ and showed that the embedding degree k of $J_C(\mathbb{F}_{2^m})$ is decided from the order of 2 in $\mathbb{Z}_n$ (where n is the largest prime divisor of $\sharp J_C(\mathbb{F}_{2^m})$), and that $k < (\log 2^m)^2$. The order of $a \in \mathbb{Z}$ in $\mathbb{Z}_n$ is denoted by $\mathrm{ord}_n(a)$. Here we present Hitt's results.

Theorem 2 ([11]): Let $n = \dfrac{2^{2^r L} + 1}{2^{2^r} + 1}$ be a prime for $^\exists r \ge 0$, let $L \ge 5$ be odd, and let k be the embedding degree of $J_C(\mathbb{F}_{2^m})$ with respect to the largest prime divisor n of $\sharp J_C(\mathbb{F}_{2^m})$, where $1 \le m \le 2^r(L-1) - 1$ or $(m, r) = (\dfrac{L+1}{2}, 0)$. Then, $k = 2^{r+1-i}$ when $\gcd(\mathrm{ord}_n(2), m) = 2^i L$ $(0 \le^\exists i \le r-1)$, and $k = 2^{r+1-i}L$ when $\gcd(\mathrm{ord}_n(2), m) = 2^i$ $(0 \le^\exists i \le r+1)$.

Let us present Lemma shown in [11] that we will use later.

Lemma 1 ([11]): Let m be a positive integer, let p and $n \ne p$ be primes, and let k be the smallest positive integer such that $p^{mk} \equiv 1 \pmod{n}$. Then $k = \dfrac{\mathrm{ord}_n(p)}{\gcd(\mathrm{ord}_n(p), m)}$.

4. The New Relations

We present the new concrete relations between $\mathbb{F}_{p^m}$, $\sharp E(\mathbb{F}_{p^m})$

and the embedding degree of E. The embedding degree of $E(\mathbb{F}_{p^m})$ is determined by order of p in $\mathbb{Z}_n$, where $n = \sharp E(\mathbb{F}_{p^m})$ is a prime and m is a positive integer. Our approach is to find such a condition that order of an element in $\mathbb{Z}_n$ can be determined. In fact, we will show that order of an element a in $\mathbb{Z}_n$ can be determined when $n = \dfrac{a^{2^r L}+1}{\lambda(a^{2^r}+1)}$ holds for r, a, $\lambda \in \mathbb{Z}$ $(r,\ \lambda \geq 0)$ and an odd prime L. We will, then, set $a = p$ or $a = t-1$ for a definition field $\mathbb{F}_{p^m}$ of an elliptic curve and the trace t of $E(\mathbb{F}_{p^m})$ when we apply the following lemmas to decide order of an elliptic curve.

The following lemma determines order of an element a over $\mathbb{Z}_n$.

Lemma 2: Let $r, a, \lambda \in \mathbb{Z}$ $(r,\ \lambda \geq 0)$ and L be an odd prime. If $n = \dfrac{a^{2^r L}+1}{\lambda(a^{2^r}+1)}$ and $a^{2^r} \not\equiv -1 \pmod{n}$, then $\mathrm{ord}_n(a) = 2^{r+1}L$.

proof: From $n = \dfrac{a^{2^r L}+1}{\lambda(a^{2^r}+1)}$, we have $\lambda(a^{2^r}+1)n = a^{2^r L}+1$. Thus, we get $a^{2^r L} \equiv -1 \pmod{n}$. This implies $a^{2^{r+1}L} \equiv 1 \pmod{n}$, and, thus, $\mathrm{ord}_n(a) \mid 2^{r+1}L$. Since L is prime, we get that either $\mathrm{ord}_n(a) = 2^j$ or $\mathrm{ord}_n(a) = 2^j L$ $(0 \leq^{\exists} j \leq r+1)$.

Suppose that $\mathrm{ord}_n(a) = 2^j L$ $(0 \leq^{\exists} j \leq r)$. Then, $a^{2^j L} \equiv 1 \pmod{n}$, so $a^{(2^j L)2^{r-j}} \equiv 1 \pmod{n}$ and, thus, $a^{2^r L} \equiv 1 \pmod{n}$. However, this contradicts the above fact that $a^{2^r L} \equiv -1 \pmod{n}$. Therefore, $\mathrm{ord}_n(a) \neq 2^j L$ $(0 \leq {}^{\forall} j \leq r)$. Similarly, we easily get $\mathrm{ord}_n(a) \neq 2^j$ $(0 \leq {}^{\forall} j \leq r)$.

Suppose that $\mathrm{ord}_n(a) = 2^{r+1}$. From the above fact that $a^{2^r L} \equiv -1 \pmod{n}$, we get the following sequences: $-1 \equiv a^{2^r L} \equiv a^{2^{r+1}} a^{2^r(L-2)} \equiv a^{2^r(L-2)} \equiv a^{2^{r+1}} a^{2^r(L-4)} \equiv \cdots \equiv a^{2^r} \pmod{n}$ since L is an odd prime. However this contradicts $a^{2^r} \not\equiv -1 \pmod{n}$.

Therefore, we have proved $\mathrm{ord}_n(a) = 2^{r+1}L$. ∎

From Lemmas 1 and 2, we get the following Lemma.

Lemma 3: Let r, m, λ, and $a \in \mathbb{Z}$ $(r,\ m,\ \lambda \geq 0)$, let L and n be odd primes, and let k be the smallest positive integer such that $a^{mk} \equiv 1 \pmod{n}$. If $n = \dfrac{a^{2^r L}+1}{\lambda(a^{2^r}+1)}$ and $a^{2^r} \not\equiv -1 \pmod{n}$, then $k = 2^{r+1-i}$ when $\gcd(\mathrm{ord}_n(a), m) = 2^i L$ $(0 \leq^{\exists} i \leq r+1)$, and $k = 2^{r+1-i}L$ when $\gcd(\mathrm{ord}_n(a),\ m) = 2^i$ $(0 \leq^{\exists} i \leq r+1)$.

proof: From the assumption of $n = \dfrac{a^{2^r L}+1}{\lambda(a^{2^r}+1)}$ and $a^{2^r} \not\equiv -1 \pmod{n}$, we get $\mathrm{ord}_n(a) = 2^{r+1}L$ by Lemma 2. Thus, $\gcd(\mathrm{ord}_n(a),\ m) \mid \mathrm{ord}_n(a)$ and, therefore, $\gcd(\mathrm{ord}_n(a),\ m) = 2^i L$ or 2^i $(0 \leq^{\exists} i \leq r+1)$. Lemma 1 says that $k = \dfrac{\mathrm{ord}_n(a)}{\gcd(\mathrm{ord}_n(a),\ m)}$. Therefore, we get $k = 2^{r+1-i}$ if $\gcd(\mathrm{ord}_n(a),\ m) = 2^i L$ $(0 \leq^{\exists} i \leq r+1)$; and $k = 2^{r+1-i}L$ else if $\gcd(\mathrm{ord}_n(a),\ m) = 2^i$ $(0 \leq^{\exists} i \leq r+1)$. ∎

By applying Lemmas 2 and 3 to a prime p of a definition field $\mathbb{F}_{p^m}$ and trace t of an elliptic curve $E(\mathbb{F}_{p^m})$, we prove the following theorem that describes the relation between embedding degree and order.

Theorem 3: Let $r, m, \lambda, a \in \mathbb{Z}$ $(r,\ m,\ \lambda \geq 0)$, let L be an odd prime, $D = \gcd(\mathrm{ord}_n(p), m)$, and let k be the embedding degree of $E(\mathbb{F}_{p^m})$. Then, the following two results hold:

1. if $\sharp E(\mathbb{F}_{p^m}) = \dfrac{p^{2^r L}+1}{\lambda(p^{2^r}+1)} = n$ is a prime and $p^{2^r} \not\equiv -1 \pmod{n}$, then
   - $k = 2^{r+1-i}L$ when $D = 2^i$ $(0 \leq i \leq r+1)$; and
   - $k = 2^{r+1-i}$ when $D = 2^i L$ $(0 \leq i \leq r+1)$;
2. if $\sharp E(\mathbb{F}_{p^m}) = \dfrac{(t-1)^{2^r L}+1}{\lambda((t-1)^{2^r}+1)} = n$ is a prime and $(t-1)^{2^r} \not\equiv -1 \pmod{n}$, then $k = 2^{r+1}L$.

proof: (1). Apply $a = p$ and $\sharp E(\mathbb{F}_{p^m}) = n = \dfrac{p^{2^r L}+1}{\lambda(p^{2^r}+1)}$ to Lemma 3. Then k in Lemma 3 is the smallest positive integer such that $p^{mk} \equiv 1 \pmod{n}$. Therefore, the embedding degree k of $E(\mathbb{F}_{p^m})$ is $k = 2^{r+1-i}L$ when $D = 2^i$, and $k = 2^{r+1-i}$ when $D = 2^i L$.

(2). Apply $a = t-1$, and $\sharp E(\mathbb{F}_{p^m}) = n = \dfrac{(t-1)^{2^r L}+1}{\lambda((t-1)^{2^r}+1)}$ to Lemma 2. In this case, $t = p^m + 1 - n$, and, thus $t - 1 \equiv p^m \pmod{n}$, which implies that $(t-1)^k \equiv p^{mk} \equiv 1 \pmod{n}$. Thus, we get the embedding degree $k = \mathrm{ord}_n(p^m) = \mathrm{ord}_n(t-1) = 2^{r+1}L$. ∎

In the next section, we give two algorithms to find elliptic curve parameters such as a definition field $\mathbb{F}_p$, order of $\sharp E(\mathbb{F}_p) = n$, and trace t, which have a pre-determined embedding degree by using Theorem 3 and satisfy Waterhouse's theorem.

5. Searching Algorithm

We give two algorithms that search elliptic-curve parameters satisfying Theorem 3. We also present our experimental results. All experiments were done by using MATHEMATICA.

5.1 The Basic Algorithm

Let $n = \sharp E(\mathbb{F}_{p^m}) = \dfrac{p^{2^r L}+1}{\lambda(p^{2^r}+1)}$ be a prime, where p and L are odd primes, and r, m and λ are non negative integers. This means that n is a factor of $\Gamma = \dfrac{p^{2^r L}+1}{p^{2^r}+1}$. Before showing the concrete algorithm, we will prove that a non-negative integer m can be restricted by the following Proposition.

Proposition 1: Let $n = \sharp E(\mathbb{F}_{p^m})$ for an odd prime p and a positive integer m. If $|t|$ satisfies the condition of Waterhouse, then $m = \lfloor \log_p n \rfloor$ or $\lfloor \log_p n \rfloor + 1$.

proof: Let $m' = \lfloor \log_p n \rfloor$. Then $m' + 1 > \log_p n \geq m'$, and, thus, $p^{m'+1} > n \geq p^{m'}$ holds.

First we assume that $m > m' + 1$. Then, $m - 1 > m'$ and, thus, $m - 1 \geq m' + 1$ holds since both m and m' are integers. Then, we get the following since $p \geq 3$ and $m \geq 1$:

$$|t| = |p^m + 1 - n| \geq |p^m - p^{m-1} + 1|$$

$$= (p-1)p^{m-1} + 1 \geq 2\sqrt{p^m} + 1$$
$$> 2\sqrt{p^m}.$$

Next we assume that $m' > m$. Then, in the same way as the above, $m' - 1 \geq m$. Then, the following holds:

$$|t| = |n - p^m - 1| \geq |n - p^{m'-1} - 1|$$
$$\geq p^{m'} - p^{m'-1} - 1 = (p-1)p^{m'-1} - 1$$
$$\geq p^m(p-1) - 1 > 2\sqrt{p^m}$$

since $p \geq 3$ and $m \geq 1$.

This contradict the condition of Waterhouse. From this, we get $m = m'$ or $m' + 1$. ∎

Here we present Algorithm 1, which applies $a = p$ to Theorem 3.

Algorithm 1:

Input: An odd prime L and a non negative integer r.
Output: The embedding degree k, order n, definition field p^m, and the trace t.
1. Set an odd prime p.
2. Set $\Gamma = \dfrac{p^{2^r L} + 1}{p^{2^r} + 1}$.
3. Set a large prime factor of Γ to n.
4. If $p^{2^r} \equiv -1 \pmod{n}$, then return to Step 1.
5. Set $m' = \lfloor \log_p n \rfloor$.
6. If $m' + 1/2 < \log_p n$, then $m = m' + 1$. Else $m = m'$.
7. Set $t = p^m + 1 - n$.
8. If (p^m, n) does not satisfy the condition of Waterhouse, then return to Step 1.
9. Set $k = \dfrac{2^{r+1}L}{\gcd(2^{r+1}L, m)}$.
10. Output $\{k,\ n,\ p^m,\ t\}$.

Remark 1: Step 3 of Algorithm 1 excludes all small prime factors[†] from Γ and checks whether the rest is prime or not.

Table 2 presents elliptic-curve parameters of p^m, n, t which satisfy Theorem 3 and the condition of Waterhouse. They are constructed by Algorithm 1 for $0 \leq r \leq 1$, $3 \leq L \leq 7$ and all 16-bit primes p. The total number of 16-bit primes are to 1649.

Algorithm 1 does not work well, since it often fails in Step 8 for the following reason: In order to execute Step 3,

$$\Gamma = \frac{p^{2^r L} + 1}{p^{2^r} + 1} = p^{2^r(L-1)} - p^{2^r(L-2)} + \cdots + 1$$

has to be almost prime with a prime factor n, which implies that $n \approx \Gamma$. On the other hand, $p^m \approx n$ due to the condition of Waterhouse. Therefore, $2^r(L-1) \approx m$. By combining these facts that $n \approx \Gamma$ and $p^m \approx p^{2^r(L-1)}$, we get that

$$|t| = |p^m + 1 - n| \approx p^{m\frac{L-2}{L-1}} + O(p^{m\frac{L-3}{L-1}}),$$

which induces $t^2 > 4p^m$ if L is large. Therefore, it fails in Step 8. As a result, only limited small L can be used, as we have shown in Table 2.

Table 2 The elliptic-curve parameters and k (Algorithm 1).

p	r	L	k	n	m	t	ρ
71993	0	5	10	72341	1	−347	1
74167	0	5	10	74531	1	−363	1
76207	0	5	10	76441	1	−233	1
81023	0	5	10	81401	1	−377	1
65963	1	3	12	66373	1	−409	1
81119	0	7	14	81677	1	−557	1
81847	0	7	14	82223	1	−375	1
75223	1	5	20	75721	1	−497	1
78031	1	5	20	78121	1	−89	1
83579	1	5	20	83621	1	−41	1

5.2 The Improved Algorithm

In order to resolve the problem of Algorithm 1, we apply $a = t - 1$ to Theorem 3. Then, the condition of Waterhouse usually holds for the following reason. In this case, $\log n \approx \log t^{2^r(L-1)}$, thus any n, p^m and t satisfy $n \approx t^{2^r(L-1)} \geq t^2$, which roughly implies that $2\sqrt{n} > \sqrt{n} \geq t$. The equality in $t^{2^r(L-1)} \geq t^2$ holds if and only if $(r,\ L) = (0,\ 3)$. In this case of $(r,\ L) = (0,\ 3)$, we get $\Gamma = t^2 - 3t + 3$, and, thus, $p^m \approx \Gamma + t - 1 = t^2 - 2t + 2 > \left(\frac{t}{2}\right)^2$ always holds.

Algorithm 2:

Input: An odd prime L and a non negative integer r. (i.e. an embedding degree $k = 2^{r+1}L$.)
Output: Order n, a power of prime p^m, and trace t.
1. Set an odd integer[††] t as a candidate of trace, where the range of t is defined by the size of elliptic curves that we will need. The range is described below in detail.
2. Set $\Gamma = \dfrac{(t-1)^{2^r L} + 1}{(t-1)^{2^r} + 1}$.
3. If Γ is not almost prime, then return to Step 1.
4. Set the largest prime factor of Γ to n.
5. If $n + t - 1$ is a power of prime[†††], then set $n + t - 1 = p^m$. Else, then return to Step 1.
6. If $(t-1)^{2^r} \equiv -1 \pmod{n}$, then return to Step 1.
7. Output $\{k,\ n,\ p^m,\ t\}$.

Let us investigate the range of t. Algorithm 2 sets $\sharp E(\mathbb{F}_{p^m}) = n = \dfrac{(t-1)^{2^r L} + 1}{\lambda((t-1)^{2^r} + 1)}$, and, thus, $\log p^m \approx 2^r(L -$

[†] The size of small prime factors depend on a system. In our experiment, we set the size of small prime factors to be 16 bits.

[††] Here we consider only a prime-order elliptic curve and a power of an odd prime p. This is why only an odd integer t is dealt.

[†††] It is easy to check whether $n + t - 1$ is prime or not by using primality tests [1]. In our experimental results in Section 5.3, we deal with only this case.

Table 3 The number of parameters satisfying with $(r,\ L,\ k)$ (Algorithm 2).

160−bit prime p			
r	L	k	$\#\{n,\ p^m,\ t\}$
1	3	12	136
2	3	24	84
0	5	10	225
1	5	20	180
0	7	14	135

192−bit prime p			
r	L	k	$\#\{n,\ p^m,\ t\}$
1	3	12	91
2	3	24	57
0	5	10	154
1	5	20	119
0	7	14	90
0	11	22	91

224−bitprime p			
r	L	k	$\#\{n,\ p^m,\ t\}$
1	3	12	73
2	3	24	41
0	5	10	112
1	5	20	85
0	7	14	75
1	7	28	62
0	11	22	70

1) $\log t$. Therefore, t is set to $\frac{160}{2^r(L-1)}$ bits when we construct 160-bit elliptic curves.

5.3 Experimental Results

Experiments are executed for $m = 1$ and $(r,\ L)$ as shown in Table 3. Here we set $m = 1$ since an elliptic curve over a prime field $\mathbb{F}_p$ do not suffer from reduction to the minimum embedding degree.

Then, the range of t is determined by the above discussion in Sect. 5.2, where t runs over 100,000 kinds of random $\frac{\log p}{2^r(L-1)}$-bit integers. We constructed examples with 160, 192, 224-bit primes p.

Table 3 shows the total number of elliptic-curve parameters searched by Algorithm 2 under given values of (m, r, L, k) and each 100,000 kinds of of t.

The following are some examples.

160-bit elliptic curves

(1)

$k = 10$
$t = 1285693206491$
$p = 273243221\ \ 2182434088\ \ 1531032711\ \ 6177600129\ \ 4482681101$
$n = 273243221\ \ 2182434088\ \ 1531032711\ \ 6177600000\ \ 8789474611$
$\rho = 1$

(2)

$k = 20$
$t = 1712607$
$p = 180499429\ \ 2421198963\ \ 8284539265\ \ 0495241704\ \ 2967749987$
$n = 180499429\ \ 2421198963\ \ 8284539265\ \ 0495241704\ \ 2966037381$
$\rho = 1$

192-bit elliptic curves

(1)

$k = 14$
$t = 7223820963$
$p = 1912551\ \ 0159002005\ \ 2219431877\ \ 1995972452\ \ 4321251430\ \ 5346292063$
$n = 1912551\ \ 0159002005\ \ 2219431877\ \ 1995972452\ \ 4321251429\ \ 8122471101$
$\rho = 1$

(2)

$k = 28$
$t = -66881$
$p = 24447\ \ 5068599953\ \ 5868940457\ \ 2401483697\ \ 7022909801\ \ 1541952959$
$n = 24447\ \ 5068599953\ \ 5868940457\ \ 2401483697\ \ 7022909801\ \ 1542019841$
$\rho = 1$

224-bit elliptic curves

(1)

$k = 12$
$t = -9924312\ 9329168669$
$p = 1328859\ \ 1151679357\ \ 6485698850\ \ 6600860828\ \ 7715683196\ \ 7144571636\ \ 9719292167$
$n = 1328859\ \ 1151679357\ \ 6485698850\ \ 6600860828\ \ 7715683196\ \ 7154495949\ \ 9048460837$
$\rho = 1$

(2)

$k = 20$
$t = -419108453$
$p = 15605638\ \ 2326675970\ \ 2773190814\ \ 4467543753\ \ 5277124105\ \ 2130428296\ \ 5529550667$
$n = 15605638\ \ 2326675970\ \ 2773190814\ \ 4467543753\ \ 5277124105\ \ 2130428296\ \ 5948659121$
$\rho = 1$

6. Comparison between Our Results and Previous Results

Let us compare our results with previous results. First we discuss our advantage over Hitt's results [11]. Table 4 shows the comparison between our results and [11]. Hitt has investigated Jacobians of genus 2 curves J_C over $\mathbb{F}_{2^m}$ and some examples of the parameters for such curves over $\mathbb{F}_{2^m}$ with embedding degrees $k = 8, 13, 16, 23, 26, 37, 46$, and 52. However, Hitt's results cannot construct $\rho = 1$ because the results restrict the relation between trace, definition field, and the largest prime divisor. Furthermore, the results suffer from reduction to the actual minimum embedding degree

Table 4 Comparison of [11] and our results.

	[11]								Ours						
genus	2								1						
definition field $\mathbb{F}_q$	$q = 2^m$								$q = p^m$ (p : a prime)						
largest prime divisor of $\sharp J_C(\mathbb{F}_{2^m})$ or $\sharp E(\mathbb{F}_{p^m})$	$\frac{2^{2^r L}+1}{2^{2^r}+1}$								$\frac{(t-1)^{2^r L}+1}{\lambda((t-1)^{2^r}+1)}$						
trace	$(-1,\ 2^m + 2^{2^m+2^{2m-2^r L}})$								$^\forall \mid t \mid \leq q^{1/2^r(L-1)}$						
ρ-value	$\frac{4L}{3(L-1)} \leq \rho \leq 2 - \frac{2}{2^r(L-1)}$								1						
constructed embedding degree k	8	13	16	23	26	37	46	52	10	12	14	20	22	24	28
actual embedding degree (highest case)	$\frac{8}{3}$	$\frac{13}{5}$	$\frac{16}{7}$	$\frac{23}{8}$	$\frac{26}{9}$	$\frac{37}{13}$	$\frac{46}{17}$	$\frac{52}{19}$	10	12	14	20	22	24	28

since they work only in the case of $\mathbb{F}_{2^m}$. As a result, the actual security level of all results is reduced to $\frac{1}{19}$ of the original security level at the minimum and to its $\frac{1}{3}$ at the maximum.

On the other hand, we improve on Hitt's ideas from the point of view of ρ-value, the actual minimum security, and elliptic curves. As for ρ-value, we do not place any restrictions on the relation between trace and definition field. As a result, we can construct elliptic curves with $\rho = 1$. Furthermore, we can enjoy the case of prime field $\mathbb{F}_p$, and, thus, our results do not suffer from reduction to the minimum embedding degree.

Let us compare our results with Cocks-Pinch and Brezing-Weng curves, which are summarized in [7]. In [7], previous results to construct pairing-friendly elliptic curves are investigated from the point of view of embedding degrees k and ρ-value. Embedding degrees of results shown in Section 3 are currently limited to $k \leq 12$ while they achieve $\rho = 1$. On the other hand, Cocks-Pinch and Brezing-Weng curves exist for arbitrary embedding degree k but usually lead to $\rho > 1$. Actually, Cocks-Pinch curve tends to have ρ-value around 2. Brezing-Weng curve improves Cocks-Pinch curve to have ρ-value less than 2 but it still needs $\rho > 1$. Compared with these previous results, our results can deal with both arbitrary embedding degree k and $\rho = 1$.

7. Conclusion

We have investigated the new concrete relation between trace, definition field $\mathbb{F}_{p^m}$, embedding degree k, and the largest prime divisor n of $\#E(\mathbb{F}_{p^m})$ of elliptic curves $E/\mathbb{F}_{p^m}$. Compared with the previous Hitt's result, the new relation discovered by us do not place any restrictions on the relation between trace and definition field. As a result, our result can work even when $\rho = 1$. The case of $\rho = 1$ is the most efficient since the size of definition field $\mathbb{F}_{p^m}$ is equal to that of the largest prime divisor n of $\#E(\mathbb{F}_{p^m})$. We also gave some examples of the new relations in the cases of 160-bit, 192-bit and 224-bit elliptic curves.

Acknowledgments

The authors express our gratitude to anonymous referees for invaluable comments.

References

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman & Hall/CRC, 2006.
[2] D. Boneh and X. Boyen, "Short signatures without random oracles," EUROCRYPT 2004, LNCS 3027, pp.56–73, 2004.
[3] R. Balasubramanian and N. Koblitz, "The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm," J. Cryptol., vol.11, pp.141–145, 1998.
[4] P.S.L.M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order," Proc. SAC'05, LNCS 3897, pp.319–331, Springer-Verlag, 2005.
[5] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," SIAM J. Comput., vol.32, no.3, pp.586–615, 2003.
[6] D. Freeman, "Constructing pairing-friendly elliptic curves with embedding degree 10," Algorithmic Number Theory Symposium — ANTS VII, LNCS 4076, pp.452–465, Springer-Verlag, 2006.
[7] D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing friendly elliptic curves," J. Cryptol., vol.23, no.2, pp.224–280, 2010.
[8] 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, vol.62, pp.865–874, 1994.
[9] S. Galbraith, J. McKee, and P. Valenca, "Ordinary abelian varieties having small embedding degree," Cryptology ePrint Archive, Report 2004/365, 2004, Available from http://eprint.iacr.org/2004/365
[10] S. Hirasawa and A. Miyaji, "Elliptic curves with a pre-determined embedding degree," 2009 IEEE International Symposium on Information Theory (ISIT 2009), pp.2391–2395, 2009.
[11] L. Hitt, "On the minimal embedding field," Pairing 2007, LNCS 4575, pp.294–301, Springer-Verlag, 2007.
[12] A. Menezes, T. Okamoto, and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," IEEE Trans. Inf. Theory, vol.39, no.5, pp.1639–1646, 1993.
[13] A. Miyaji, M. Nakabayashi, and S. Takano, "New explicit conditions of elliptic curve traces under FR-reduction," IEICE Trans. Fundamentals, vol.E84-A, no.5, pp.1234–1243, May 2001.
[14] E. Waterhouse, "Abelian varieties over finite fields," Ann. Sci. Ecole Norm, Sup. 2, pp.521–560, 1969.

Shoujiro Hirasawa received the B.Sc. degree from Gakushuin University in 2007 and the M. Info. Sc. degree from the Japan Advanced Institute of Science and Technology in 2009.

Atsuko Miyaji received the B.Sc., the M.Sc., and the Dr. Sci. degrees in mathematics from Osaka University, Osaka, Japan in 1988, 1990, and 1997 respectively. She joined Panasonic Co., LTD from 1990 to 1998 and engaged in research and development for secure communication. She was an associate professor at the Japan Advanced Institute of Science and Technology (JAIST) in 1998. She has joined the computer science department of the University of California, Davis since 2002. She has been a professor at the Japan Advanced Institute of Science and Technology (JAIST) since 2007 and the director of Library of JAIST since 2008. Her research interests include the application of number theory into cryptography and information security. She received Young Paper Award of SCIS'93 in 1993, Notable Invention Award of the Science and Technology Agency in 1997, the IPSJ Sakai Special Researcher Award in 2002, the Standardization Contribution Award in 2003, Engineering Sciences Society: Certificate of Appreciation in 2005, the AWARD for the contribution to CULTURE of SECURITY in 2007, IPSJ/ITSCJ Project Editor Award in 2007, 2008, 2009, and 2010, the Director-General of Industrial Science and Technology Policy and Environment Bureau Award in 2007, Editorial Committee of Engineering Sciences Society: Certificate of Appreciation in 2007, DoCoMo Mobile Science Awards in 2008, Advanced Data Mining and Applications (ADMA 2010) Best Paper Award, and The chief of air staff: Letter of Appreciation Award. She is a member of the International Association for Cryptologic Research, the Information Processing Society of Japan, and the Mathematical Society of Japan.