Elliptic Curves with a Pre-determined Embedding Degree

Shoujirou Hirasawa
Japan Advanced Institute of
Science and Technology
1-1 Asahidai, Nomi, Ishikawa 923-1292 Japan

Atsuko Miyaji
Japan Advanced Institute of
Science and Technology
1-1 Asahidai, Nomi, Ishikawa 923-1292 Japan
Email: miyaji@jaist.ac.jp

***Abstract*—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, where k is called the embedding degree. The cryptosystems using a pairing are called the pairing-based cryptosystems. The embedding degree k is also an indicator of the 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 $\mathbb{F}_{p^{mk}}$. An elliptic curve is determined by j-invariant or order, however the explicit condition between these parameters and an embedding degree has been described only in some degrees. In this paper, we investigate a new condition of the existence of elliptic curves with pre-determined embedding degrees, and present some examples of the elliptic curves over 160-bit, 192-bit and 224-bit $\mathbb{F}_{p^m}$.**

I. Introduction

A pairing over an elliptic curve $E(\mathbb{F}_{p^m})$ to an extension field of $\mathbb{F}_{p^{mk}}$ 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 $\mathbb{F}_{p^{mk}}$ [7], where k is called the embedding degree. The embedding degree k is an indicator of the security of ECDLP, where the security level of ECDLP over $E(\mathbb{F}_{p^m})$ is the same as that of DLP over $\mathbb{F}_{p^{mk}}$. Recently, the pairing over an elliptic curve $E(\mathbb{F}_{p^m})$ has begun to be attractive in cryptosystems since it can achieve an ID-based cryptosystem [3] or etc. The cryptosystems using a pairing are called the pairing-based cryptosystems.

The elliptic curve $E(\mathbb{F}_{p^m})$ is determined by j-invariant or order $\sharp E(\mathbb{F}_{p^m})$. The relationship, however, between j, $\sharp E(\mathbb{F}_{p^m})$ and the embedding degree k has been described only in some degrees such as $k = 3, 4, 6, 10$, or 12. Generally, the embedding degree k for a prime-order elliptic curve is $k \approx n$ where $n = \sharp E(\mathbb{F}_{p^m})$ [1].

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 [8] have proposed ordinary elliptic curves with embedding degrees $k = 3$, 4 and 6. Galbraith, Valenca, Mackee [5] have presented the factorization of cyclotomic polynomials with degrees 5, 10 and 12, and applied the results [8] to a hyperelliptic curve. Freeman [4] and Barretto and Naehrig [2] have constructed ordinary elliptic curves with embedding degree $k = 10$ and $k = 12$ using [5], respectively. In addition, Hitt [6] has investigated a Jacobian of hyperelliptic curve $J_C/\mathbb{F}_{2^m}$ and discussed the way to decide the embedding degree k of $J_C(\mathbb{F}_{2^m})$ from the 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 the embedding degree $k < (\log p^m)^2$, but did not give concrete $J_C/\mathbb{F}_{2^m}$ themselves This result cannot construct $\sharp J_C(\mathbb{F}_{2^m})$ with $\rho = \frac{\sharp J_C(\mathbb{F}_{2^m})}{n} \approx 1$. Because this results restrict the relation between trace, definition field, and the largest prime divisor. Furthermore, this result suffers from reduction to the actual minimum embedding degree. As a result, the actual security level of all this results is reduced to $\frac{1}{23} - \frac{1}{3}$ of their original security level.

In this paper, we apply [6] to the case of elliptic curves, and prove the existence of elliptic curves with pre-determined embedding degrees and resolves the above problem. 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 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. We also present some examples of prime orders of elliptic curves over 160-bit, 192-bit and 224-bit $\mathbb{F}_p$ and embedding degrees.

This paper is organized as follows. Section II summarizes known facts on elliptic curves. In Section III, we review the previous results. Our main contribution appears in Section IV, where we show how to give orders of elliptic curves with pre-determined embedding degree. with pre-determined embedding degree. In Section V, we present some experimental results based on Section IV. Section VI compares our results with Hitt's results. Conclusion follows in Section VII.

II. 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 $\mathbb{F}_{p^m}$, where the trace t is defined $t = p^m + 1 - \sharp E(\mathbb{F}_{p^m})$. The embedding degree is defined as follows.

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

In other words, k is the minimal integer such that $n \mid \Phi_k(p^m)$, where $\Phi_k(X)$ is the k-th cyclotomic polynomial. As

978-1-4244-4313-0/09/$25.00 ©2009 IEEE

for the embedding degree k of E, the following 4 conditions are equivalent to each other:

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

Waterhouse's theorem [9] shows that 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 $p \not\equiv 1 \pmod{4}$.

III. Previous research

We summarize previous results that determine the embedding degree explicitly by trace [8], [4], [2] and Hitt's results [6] in detail. Table 1 presents traces t of elliptic curves over $\mathbb{F}_{p^m}$ with embedding degree k, where x are integers.

A. The hyperelliptic curve of $k < (\log p^m)^2$ [6]

Hitt investigates Jacobians of genus 2 curves J_C over $\mathbb{F}_{2^m}$. Hitt has shown 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 $k < (\log 2^m)^2$. Here we present Hitt's results.

Theorem 1 ([6]): Let $n = \frac{2^{2^r L}+1}{2^{2^r}+1}$ be 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 $(m,\ r) = (\frac{L+1}{2},\ 0)$. 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 [6] that we will use later.

Lemma 1 ([6]): Let m be a positive integer, p and $n \ne p$ be primes, and let k be the smallest positive integer such that $p^{mk} \equiv 1 \pmod{n}$. Then $k = \frac{\mathrm{ord}_n(p)}{\gcd(\mathrm{ord}_n(p),m)}$.

IV. The proposed method

We propose a method to construct an elliptic curve with a pre-determined embedding degree k. 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 prime. We will show that order of p in $\mathbb{Z}_n$ is determined when $n = \frac{a^{2^r L}+1}{\lambda(a^{2^r}+1)}$ for $r,\ a,\ \lambda \in \mathbb{Z}$ $(r,\ \lambda \ge 0)$ and an odd prime L. We will set $a=p$ or $a=t-1$ when we apply the following lemmas to decide the order of an elliptic curve.

The following lemma determines the order of a prime p over $\mathbb{Z}_n$.

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

Proof: From $n = \frac{a^{2^r L}+1}{\lambda(a^{2^r}+1)}$, 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 $\mathrm{ord}_n(a) = 2^j L$ $(0 \le^\exists j \le r+1)$. Suppose $\mathrm{ord}_n(a) = 2^j L$ $(0 \le^\exists j \le r)$. 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, $\mathrm{ord}_n(a) \ne 2^j L$ $(0 \le^\forall j \le r)$. Similarly, we easily get $\mathrm{ord}_n(a) \ne 2^j$ $(0 \le^\forall j \le r)$. 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 $r,\ m,\ \lambda$, and $a \in \mathbb{Z}$ $(r,\ m,\ \lambda \ge 0)$, let L and n be odd primes, and let k be the smallest positive integer such that $a^{mk} \equiv 1 \pmod{n}$. If $n = \frac{a^{2^r L}+1}{\lambda(a^{2^r}+1)}$ and $a^{2^r} \not\equiv -1 \pmod{n}$, then $k = 2^{r+1-i}$ when $\gcd(\mathrm{ord}_n(a), m) = 2^i L$ $(0 \le^\exists i \le r+1)$, and $k = 2^{r+1-i}L$ when $\gcd(\mathrm{ord}_n(a),\ m) = 2^i$ $(0 \le^\exists i \le r+1)$.

Proof: From the assumption of $n = \frac{a^{2^r L}+1}{\lambda(a^{2^r}+1)}$ 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 $(0 \le^\exists i \le r+1)$. Lemma 1 says that $k = \frac{\mathrm{ord}_n(a)}{\gcd(\mathrm{ord}_n(a),\ m)}$. Therefore, we get $k = 2^{r+1-i}$ if $\gcd(\mathrm{ord}_n(a),\ m) = 2^i L$ $(0 \le^\exists i \le r+1)$; and $k = 2^{r+1-i}L$ else if $\gcd(\mathrm{ord}_n(a),\ m) = 2^i$ $(0 \le^\exists i \le r+1)$. ∎

Applying Lemmas 2 and 3 on $a=p,\ t-1$ we prove the following theorem that describes the relation between embedding degree and order.

Theorem 2: Let $r,\ m,\ \lambda,\ a \in \mathbb{Z}$ $(r,\ m,\ \lambda \ge 0)$, let L be an odd prime, $D = \gcd(\mathrm{ord}_n(p), m)$, and let k be embedding degree of $E(\mathbb{F}_{p^m})$. Then, the following two results hold:

1) Embedding degree k of $E(\mathbb{F}_{p^m})$ is $k = 2^{r+1-i}L$ when $D = 2^i$ $(0 \le i \le r+1)$ or $k = 2^{r+1-i}$ when $D = 2^i L$ $(0 \le i \le r+1)$ if $\sharp E(\mathbb{F}_{p^m}) = \frac{p^{2^r L}+1}{\lambda(p^{2^r}+1)} = n$ is prime and $p^{2^r} \not\equiv -1 \pmod{n}$;
2) The embedding degree k of $E(\mathbb{F}_{p^m})$ is $k = 2^{r+1}L$ if $\sharp E(\mathbb{F}_{p^m}) = \frac{(t-1)^{2^r L}+1}{\lambda((t-1)^{2^r}+1)} = n$ and $(t-1)^{2^r} \not\equiv -1 \pmod{n}$.

Proof: (1). Apply $a=p$ and $\sharp E(\mathbb{F}_{p^m}) = n = \frac{p^{2^r L}+1}{\lambda(p^{2^r}+1)}$ to Lemma 3. Then k in Lemma 3 is the smallest positive integer such that $p^{mk} \equiv 1 \pmod{n}$. Therefore, 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 $\sharp E(\mathbb{F}_{p^m}) = n = \frac{(t-1)^{2^r L}+1}{\lambda((t-1)^{2^r}+1)}$ to Lemma 2. In this case, $t = p^m+1-n$, and, thus $t-1 \equiv p^m \pmod{n}$, which implies that $(t-1)^k \equiv p^{mk} \equiv 1$

TABLE I
ELLIPTIC CURVES WITH SMALL EMBEDDING DEGREES

	k	p^m	t
MNT-Curve[8]	3	$12x^2-1$	$-1\pm 6x$
	4	x^2+x+1	$-x$ or $x+1$
	6	$4x^2+1$	$1\pm 2x$
Freeman[4]	10	$25x^4+25x^3+25x^2+10x+3$	$10x^2+5x+3$
BN-Curve[2]	12	$36x^4+36x^3+24x^2+6x+1$	$6x^2+1$

$(\mathrm{mod}\ n)$. Thus, we get 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 degrees by using Theorem 2 and satisfy Waterhouse's theorem.

V. CONSTRUCTIONS OF $E/\mathbb{F}_{p^m}$

We give two algorithms to find some of elliptic-curve parameters and experimental results. All experiments were done by using MATHEMATICA on a PC with pentium D 3.0 GHz and memory of 1.0 GB.

A. The Basic Algorithm

Let $n=\sharp E(\mathbb{F}_{p^m})=\frac{p^{2^rL}+1}{\lambda(p^{2^r}+1)}$ 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 $\Gamma=\frac{p^{2^rL}+1}{p^{2^r}+1}$. 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 $m'=\lfloor\log_p n\rfloor$. If $m>m'+1$, then $|t|=p^m+1-n\geq p^m-p^{m-1}=(p-1)p^{m-1}>2\sqrt{p^m}$. If $m<m'$, then $|t|=n-(p^m+1)>p^{m'}-p^{m'-1}-1=(p-1)p^{m'-1}-1>2\sqrt{p^m}$. 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 2.

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 $\Gamma=\frac{p^{2^rL}+1}{p^{2^r}+1}$.
3. Set a large prime factor of Γ to n.
4. If $p^{2^r}\equiv -1\ (\mathrm{mod}\ n)$, 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 $k=\frac{2^{r+1}L}{\gcd(2^{r+1}L,m)}$.
10. Output $\{k,\ n,\ p^m,\ t\}$.

Table II presents elliptic-curve parameters of p^m, n, t which satisfy Theorem 2 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.

Algorithm 1 does not work well, since it often fails in Step 8 for the following reason: In order to execute Step 3, $\Gamma=\frac{p^{2^rL}+1}{p^{2^r}+1}=p^{2^r(L-1)}-p^{2^r(L-2)}+\cdots+1$ 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 $|t|=|p^m+1-n|\approx p^{\frac{L-2}{L-1}m}+\mathcal{O}(p^{\frac{L-3}{L-1}m})$, which induces $t^2>4p^m$ if p^m is large. Therefore, it fails in Step 8. As a result, only small p^m can be constructed, as we have shown in Table II.

TABLE II
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

B. The Improved Algorithm

In order to resolve the problem of Algorithm 1, we apply $a=t-1$ to Theorem 2. 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 implies that $2\sqrt{n}>\sqrt{n}\geq t$, where equality in $t^{2^r(L-1)}\geq t^2$ holds if and only if $(r,\ L)=(0,\ 3)$.

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

[1]The total number of 16-bit primes are to 1649.

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 $\Gamma = \frac{(t-1)^{2^r L}+1}{(t-1)^{2^r}+1}$.
3. If Γ is not almost prime, then return to Step 1.
4. Set the largest prime factor of Γ to n and $p^m = n + t - 1$.
5. If p^m is not a power of prime, 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 $\sharp E(\mathbb{F}_{p^m}) = n = \frac{(t-1)^{2^r L}+1}{\lambda((t-1)^{2^r}+1)}$, and, thus, $\log p^m \approx 2^r(L-1)\log t$. Therefore, t is set to $\frac{160}{2^r(L-1)}$ bits when we construct 160-bit elliptic curves.

C. Experimental results

Experiments are executed for $m = 1$ and $(r,\ L)$ as shown in Table III. 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 Section 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 p.

Table III shows the total number of elliptic-curve parameters constructed by Algorithm 2. The following are some examples.

160-bit elliptic curves

(1) $k = 10$, $t = 1285693206491$
$q = 273243221\ 2182434088\ 1531032711\ 6177600129\ 4482681101$
$r = 273243221\ 2182434088\ 1531032711\ 6177600000\ 8789474611$
$\rho = 1$

(2) $k = 20$, $t = 1712607$
$q = 180499429\ 2421198963\ 8284539265\ 0495241704\ 2967749987$
$r = 180499429\ 2421198963\ 8284539265\ 0495241704\ 2966037381$
$\rho = 1$

192-bit elliptic curves

(1) $k = 14$ $t = 7223820963$
$q = 1912551\ 0159002005\ 2219431877\ 1995972452\ 4321251430\ 5346292063$
$r = 1912551\ 0159002005\ 2219431877\ 1995972452\ 4321251429\ 8122471101$
$\rho = 1$

(2) $k = 28$ $t = -66881$
$q = 24447\ 5068599953\ 5868940457\ 2401483697\ 7022909801\ 1541952959$
$r = 24447\ 5068599953\ 5868940457\ 2401483697\ 7022909801\ 1542019841$
$\rho = 1$

224-bit elliptic curves

(1) $k = 12$, $t = -9924312\ 9329168669$
$q = 1328859\ 1151679357\ 6485698850\ 6600860828\ 7715683196\ 7144571636\ 9719292167$
$r = 1328859\ 1151679357\ 6485698850\ 6600860828\ 7715683196\ 7154495949\ 9048460837$
$\rho = 1$

(2) $k = 20$, $t = -419108453$
$q = 15605638\ 2326675970\ 2773190814\ 4467543753\ 5277124105\ 2130428296\ 5529550667$
$r = 15605638\ 2326675970\ 2773190814\ 4467543753\ 5277124105\ 2130428296\ 5948659121$
$\rho = 1$

VI. Comparison between our results and Hitt's results.

Let us compare our results with Hitt's results. Table IV shows the comparison between our results and [6]. 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 result cannot construct $\rho = 1$ because the results restrict the relation between trace, definition field, and the largest prime divisor. Furthermore, the result suffers from reduction to the actual minimum embedding degree. As a result, the actual security level of all results is reduced to $\frac{1}{23} - \frac{1}{3}$ of the original security level.

On the other hand, we improve on Hitt's ideas from the point of view of ρ-value and the actual minimum security. 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.

VII. Conclusion

We have proposed a method to construct elliptic curves with pre-determined embedding degrees. We also gave some examples of 160-bit, 192-bit and 224-bit elliptic curves.

Acknowledgment

This study is partly supported by Grant-in-Aid for Scientific Research (B) (19650002) and the Mitsubishi Foundation. The authors express gratitude to anonymous referees for invaluable comments.

References

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

TABLE III
THE NUMBER OF ELLIPTIC CURVES WITH A PRE-DETERMINED EMBEDDING DEGREE k (ALGORITHM 2)

p is 160−bit				p is 192−bit				p is 224−bit			
r	L	k	the total numbers	r	L	k	the total numbers	r	L	k	the total numbers
1	3	12	136	1	3	12	91	1	3	12	73
2	3	24	84	2	3	24	57	2	3	24	41
0	5	10	225	0	5	10	154	0	5	10	112
1	5	20	180	1	5	20	119	1	5	20	85
0	7	14	135	0	7	14	90	0	7	14	75
				0	11	22	91	1	7	28	62
								0	11	22	70

TABLE IV
COMPARISON OF [6] AND OUR RESULTS

	[6]								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

[2] P. S. L. M. Barreto and M. Naehrig, "Pairing-friendly elliptic curves of prime order", *In Proceedings of SAC'05*, LNCS **3897**(2005), 319-331, Springer-Verlag.

[3] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing", *SIAM J. of Computing*, Vol. **32**, No. 3 (2003), 586–615.

[4] D. Freeman, "Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10", *Algorithmic Number Theory Symposium- ANTS VII*, LNCS **4076** (2006), 452-465, Springer-Verlag.

[5] 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.

[6] L. Hitt, "On the Minimal Embedding Field", 4575, *Pairing 2007*, LNCS **4575**, 294-301, Springer-Verlag.

[7] 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.

[8] 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(2001), 1234-1243.

[9] E. Waterhouse, "Abelian vaieties over finite fields", Ann. Sci. Ecole Norm. Sup.,2 (1969), 521-560.