Approach to pairing inversions without solving Miller inversion

Naoki Kanayama, *Member, IEEE,* and Eiji Okamoto, *Member, IEEE*

***Abstract*—In the present paper, we show that the pairing inversion problem of Ate$_i$ pairing can be solved under the assumption that we have a generic algorithm for solving "exponentiation inversion" problem. With such an algorithm, the inversion problem of Ate$_i$ pairing can be solved without solving the Miller inversion. Thus, the pairing inversion problem of Ate$_i$ pairing is reduced to the exponentiation inversion problem.**

***Index Terms*—Ate$_i$ pairing, exponentiation inversion, Miller inversion, pairing inversion, Tate pairing**

I. Introduction

A pairing e_r is a map from $G_1 \times G_2$ to G_T, where G_1 and G_2 are additive groups of order r and G_T is a multiplicative group of order r, which satisfies the following properties:

$$e_r(P_1 + P_2, Q) = e_r(P_1, Q)e_r(P_2, Q),$$
$$e_r(P, Q_1 + Q_2) = e_r(P, Q_1)e_r(P, Q_2).$$

These are referred to collectively as bilinearity.

In the present paper, we consider the case in which G_1 and G_2 are subgroups of points of order r on an elliptic curve E over a finite field $\mathbb{F}_q$, and G_T is a subgroup of the multiplicative group of $\mathbb{F}_{q^k}$, where k is a positive integer determined by q and r. We refer to pairings from $G_1 \times G_2$ to G_T as pairings on elliptic curves. Pairings on elliptic curves, first, attracted attention in cryptography to attack elliptic curve cryptosystems based on the elliptic curve discrete logarithm problem (ECDLP). We can reduce the ECDLP to the discrete logarithm problem (DLP) on G_T using pairings on elliptic curves and attack elliptic curve cryptosystems in sub-exponential time (see [17], [8]). Around 2000, Sakai et al. [25] and Boneh et al. [4] independently proposed ID-based cryptosystems using pairings on elliptic curves. Furthermore, many excellent schemes based on pairing have been proposed, including one-round DH key exchange for tripartite proposed by Joux [15] and short signature proposed by Boneh et al. [5]. At present, pairing-based cryptography is a subject of great interest in cryptography.

The security of most of pairing-based cryptosystems is based on the difficulty in solving the ECDLP, the DLP, and the pairing inversion problem. For cryptographic use, we consider two pairings: Weil pairing and Tate pairing. Currently, Tate pairing is widely used, and numerous improved versions of Tate pairing, such as η_T pairing and Ate pairing, have been proposed (see Section 2). In the present paper, we consider the inversion problem of Tate pairing. The following is a natural approach to the pairing inversion problem of Tate pairing:

Step 1: Find a $\frac{q^k-1}{r}$-th root β of the input $\alpha \in G_T$.

Step 2: For the solution β of **Step 1**, find a point $P \in E$ (or $Q \in E$ or the pair (P, Q)) with $\beta = f_{S,P}(Q)$ if such a point or pair exists (see Section 2 for an explanation of the notation $f_{S,P}(Q)$).

At first glance, this approach would seem to be infeasible because attackers need to try **Step 2** for all $\frac{q^k-1}{r}$ roots of **Step 1**. However, as shown in [11], it suffices to choose a random $\frac{q^k-1}{r}$ root to solve the inversion problem of the Tate pairing $e(P, Q)$.

Step 2 is referred to in [11] as the Miller inversion. The difficulty of the Miller inversion is related to the degree of the function $f_{S,P}(X, Y)$. Generally, the degree of $f_{S,P}(X, Y)$ is very large. So, the Miller inversion is generally a difficult problem. Galbraith et al. [12] discuss the difficulty of Miller inversion of pairings over small characteristic fields. Although some examples of "easy" Miller inversion are shown in [11], solving the Miller inversion does not need to be made difficult to guarantee the difficulty of solving the pairing inversion problem because **Step 1**, namely inverting the final exponentiation, is generally difficult.

On the other hand, a very interesting approach to solve pairing inversion was shown by Page and Vercauteren [24]. Their method, fault attack on pairings, does not require solving Miller inversion. The basic approach of their attack is to use the structure of Miller's algorithm, which is currently a standard algorithm for pairing computation. Let $\alpha := f_{s,P}(Q)$ be the target pairing for attackers, that is, attackers try to find Q from P and α. If attackers are able to access the value $\alpha' := f_{s+1,P}(Q)$, they can obtain the value of $l_{[s-1]P,P}(Q)/v_{[s]P}(Q)$ from α and α'(see Section 2 for the notation l and v). In [24], the authors considered several types of pairing. Vercauteren [28] considered general cases by introducing the hidden root problem.

The main result of the present paper provides another approach to solve pairing inversion without solving Miller inversion. Our method assumes that we have an efficient algorithm for solving *exponentiation inversion* (EI), which is formulated in Section 2.

We consider pairing inversion of the Ate$_i$ pairings proposed in [27]. Ate$_i$ pairings are variants of the Ate pairing proposed by Hess et al. [14]. Ate$_i$ pairings shorten the length of the Miller loop by $1/\phi(k)$ for certain types of pairing-friendly el-

Manuscript received January 1, 2010; revised October 19, 2010. This work was supported by Grants-in-Aid for Scientific Research 19700005, 21650011, 22500005 and 22300002.

N. Kanayama and E. Okamoto are with Department of Risk Engineering, Faculty of Systems and Information Engineering, University of Tsukuba, 1-1-1, Ten-nohdai, Tsukuba-shi, Ibaraki-ken, 305-8573 Japan.

liptic curves (where $\phi(k)$ is the Euler function of k). However, the structure of Ate$_i$ pairings is "too good" and provides some information to attackers. In the present paper, we demonstrate that the pairing inversion problems of Ate$_i$ pairings can be reduced to the EI using this information.

The results of the present study do not demonstrate that pairing inversion is easy, because the EI is generally hard. However, it is interesting that pairing inversion can be reduced to such a simple (but not necessarily *easy*) problem.

The remainder of the present paper is organized as follows. Section 2 presents a brief mathematical description of pairings and the pairing inversion problem. Section 3 presents the solution of the pairing inversion problem of Ate$_i$ pairings, which is the main result of the present study. Finally, conclusions are presented in Section 4.

II. Preliminaries

A. Pairings

Let $\mathbb{F}_q$ be a finite field of characteristic p, and let E:$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ be an elliptic curve over $\mathbb{F}_q$. We denote the point at infinity of E as O. Let $E(\mathbb{F}_{q^j})$ ($j \geq 1$) be the group of $\mathbb{F}_{q^j}$-rational points on E. The trace of E is denoted as t. Then, $\#E(\mathbb{F}_q) = q+1-t$. Let r be a large prime number with $r|\#E(\mathbb{F}_q)$ and $(r, q) = 1$. The embedding degree k with respect to q and r is the smallest positive integer with $r|(q^k - 1)$. We assume that $r^2 \nmid (q^k - 1)$.

1) Rational functions on curves: Before introducing pairings, we briefly review divisors and rational functions on curves. For details, see, e.g., [18].

A divisor on E is a formal sum of finite numbers of points on E: $D = \Sigma m_P(P), m_P \in \mathbb{Z}$. Here, m_P is referred to as the order of D on P, and we write $\mathrm{ord}_P(D) = m_P$. The degree of D, denoted by $\mathrm{deg}D$, is defined as $\mathrm{deg}D := \Sigma_{P\in E} m_P$.

When a rational function $h(X, Y)$ on E has zeros P_i of order m_i and poles Q_i of order n_i, the divisor $D = \Sigma m_i(P_i) - \Sigma n_i(Q_i)$ is referred to as the divisor of $h(X, Y)$, and we write $D = \mathrm{div}(h)$.

For a point $P \in E(\mathbb{F}_{q^k})$ and an integer s, we define a rational function on E, denoted by $f_{s,P}(X, Y)$ or simply $f_{s,P}$, over $\mathbb{F}_{q^k}$ as a function with $\mathrm{div}(f_{s,P}) = s(P) - ([s]P) - (s-1)(O)$, where $[s]P$ is the s-multiplication of P. The function $f_{s,P}$ is uniquely determined, up to non-zero scalar multiples, from the ground field of $P = (x_P, y_P)$.

To compute $f_{s,P}$, we use the following properties of $f_{s,P}$ (see, e.g., [21] and [22]).

- $f_{-n,P} = \frac{1}{f_{n,P} \cdot v_{[n]P}}$ for a positive integer n,
- $f_{a+b,P} = f_{a,P} \cdot f_{b,P} \cdot \frac{l_{[a]P,[b]P}}{v_{[a+b]P}}$ for integers a and b,
- $f_{ab,P} = f_{a,P}^b \cdot f_{b,[a]P} = f_{b,P}^a \cdot f_{a,[b]P}$ for integers a and b,

where the line through $A, B \in E$ is denoted as $l_{A,B}$, and the vertical line through A is denoted as v_A. We define $f_{0,P} = f_{1,P} = 1$.

2) Tate pairing : Let $P \in E(\mathbb{F}_{q^k})[r] := \{P_0 \in E(\mathbb{F}_{q^k}) : [r]P_0 = O\}$ and $Q \in E(\mathbb{F}_{q^k})$. Choose a point $R \in E(\mathbb{F}_{q^k})$ such that $\mathrm{div}(f_{r,P})$ and $D = (Q+R)-(R)$ are disjoint. Then, the Tate pairing is defined by

$$\langle \cdot, \cdot \rangle_r : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^\times/(\mathbb{F}_{q^k}^\times)^r,$$
$$(P, Q) \mapsto \langle P, Q \rangle_r := f_{r,P}(D).$$

It is shown that $\langle P, Q \rangle_r$ is bilinear and non-degenerate.

In cryptographic applications, it is convenient to define pairings in which the outputs are unique values rather than equivalent classes. Therefore, we usually consider the reduced Tate pairing defined by

$$e : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r,$$
$$e(P, Q) = \langle P, Q \rangle_r^{(q^k-1)/r},$$

where μ_r denotes the group of r-th roots of unity. We refer to the operation $z \mapsto z^{(q^k-1)/r}$ as the final exponentiation. Numerous improved versions of Tate pairing have been proposed. In 2004, Barreto et al. [1] proposed the η_T pairing, which is a generalization of a method proposed by Duursma et al. [6] for supersingular curves. In 2006, Hess et al. [14] proposed the Ate and twisted Ate pairing as generalizations of the η_T pairing. These can be applied to both supersingular curves and ordinary elliptic curves. In 2007, Zhao et al. [27] proposed the Ate$_i$ and twisted Ate$_i$ pairings.

We review only the Ate$_i$ pairing because we will consider the inversion problem of Ate$_i$ pairings.

3) Ate$_i$ and twisted Ate$_i$ pairings: The q-Frobenius endomorphism on E is denoted as π_q, i.e., $\pi_q : (x, y) \mapsto (x^q, y^q)$. We consider the following two groups: $\mathbb{G}_1 = E(\mathbb{F}_q)[r] = E[r] \cap \mathrm{Ker}(\pi_q - 1)$ and $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi_q - q)$.

Let $T_i := q^i \bmod r$ for $i = 1, 2, \cdots, k-1$. For each i, we define the following quantities in a manner similar to that for Ate pairing. Let a_i be the smallest positive integer such that $T_i^{a_i} \equiv 1 \pmod r$. In addition, $N_i := \gcd(T_i^{a_i} - 1, q^k - 1)$, and L_i is a positive integer such that $T_i^{a_i} - 1 = L_i N_i$.

As with Ate pairing, Ate$_i$ pairing has two versions: the pairing defined on $\mathbb{G}_2 \times \mathbb{G}_1$ and the pairing on $\mathbb{G}_1 \times \mathbb{G}_2$. The Ate$_i$ pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ is defined by $\alpha_i(Q, P) := f_{T_i,Q}^{\mathrm{norm}}(P)$ ($Q \in \mathbb{G}_2$ and $P \in \mathbb{G}_1$), where E may be either supersingular or ordinary. Here, $f_{T_i,Q}^{\mathrm{norm}}$ is the normalization of $f_{T_i,Q}$. As mentioned at the beginning of this section, the rational function with $\mathrm{div}(f_{T_i,Q}) = T_i(Q) - ([T_i]Q) - (T_i - 1)(O)$ is uniquely determined up to non-zero scalar multiples. When the point Q is in $E(\mathbb{F}_{q^k})$, the multiples are in $\mathbb{F}_{q^k}$ and will not be annihilated by final exponentiation. Therefore, we need to consider the normalization. We can use the normalization function $f_{T_i,Q}^{\mathrm{norm}} = f_{T_i,Q}/\gamma$, where $\gamma := (z^{T_i-1} f_{T_i,Q})(O)$ and z is called a uniformizer of E on O (see, e.g., [18]).

On $\mathbb{G}_1 \times \mathbb{G}_2$, we must consider whether E is supersingular. When E is supersingular, the Ate$_i$ pairing is defined by $\alpha_i(P, Q) := f_{T_i,P}(Q)$ ($P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$). If E is ordinary, $f_{T_i,P}(Q)$ does not have bilinearity on $\mathbb{G}_1 \times \mathbb{G}_2$, the same as for Ate pairings (see [14]). In this case, we must use the twist of E.

Let E and E' be ordinary elliptic curves over $\mathbb{F}_q$. We refer to the curve E' as a twist of degree d of E if there exists an isomorphism $\psi : E' \to E$ defined over $\mathbb{F}_{q^d}$ and d is minimal with this property. We hereafter consider $\mathbb{F}_q$ with characteristic $p \geq 5$. Then, only $d = 2, 3, 4$, and 6 are possible (see [14] for

explicit forms of twists of elliptic curves with characteristic $p \geq 5$).

We define Ate$_i$ pairing on $\mathbb{G}_1 \times \mathbb{G}_2$ for ordinary elliptic curves. Let $m := \gcd(k, d)$, and let $e := k/m$ for an ordinary elliptic curve E with embedding degree k. Put $S_{e,i} := T_i^e \bmod r = q^{ie} \bmod r$. Then, the Ate$_i$ pairing on $\mathbb{G}_1 \times \mathbb{G}_2$, referred to as the twisted Ate$_i$ pairing, is defined by $\alpha_i^{\text{twist}}(P, Q) := f_{S_{e,i},P}(Q)$ ($P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$). Note that normalization is not required in this case because P is in $E(\mathbb{F}_q)$ and constants of $f_{T_i,P}$ or $f_{S_{e,i},P}$ are in $\mathbb{F}_q$.

The Tate and the Ate$_i$ (and also twisted Ate$_i$) pairings are connected by a power relationship, i.e., one pairing is a power function of the other. This relationship makes the Ate$_i$ and twisted Ate$_i$ pairings bilinear and non-degenerate. (The η_T and Ate pairings also have similar relations.) In the present paper, we refer to this type of relationship as an *exponential relationship*.

Let

$$c_i := \begin{cases} \sum_{j=0}^{m-1} T_i^{e(m-1-j)} q^{(ei)j} \equiv mq^{m-1} \pmod{N_i} \\ (\mathbb{G}_1 \times \mathbb{G}_2,\ E : \text{ordinary}), \\ \sum_{j=0}^{k-1} T_i^{k-1-j} q^j \equiv kq^{k-1} \pmod{N_i} \\ (\text{otherwise}). \end{cases}$$

Then,

$$e(Q,P)^{L_i} = \alpha_i(Q,P)^{c_i(q^k-1)/N_i},$$

$$e(P,Q)^{L_i} = \begin{cases} \alpha_i(P,Q)^{c_i(q^k-1)/N_i} \\ (E\text{: supersingular}), \\ \alpha_i^{\text{twist}}(P,Q)^{c_i(q^k-1)/N_i} \\ (E\text{: ordinary}). \end{cases}$$

Thus, the Ate$_i$ and twisted Ate$_i$ pairings are non-degenerate if and only if $(r, L_i) = 1$.

The reduced Ate$_i$ and twisted Ate$_i$ pairings are denoted as $\hat{\alpha}_i(Q, P)$ (or $\hat{\alpha}_i(P, Q)$) and $\hat{\alpha}_i{}^{\text{twist}}(P, Q)$:

$$\hat{\alpha}_i(Q,P) := \alpha_i(Q,P)^{\frac{q^k-1}{r}},$$
$$\hat{\alpha}_i(P,Q) := \alpha_i(P,Q)^{\frac{q^k-1}{r}},$$
$$\hat{\alpha}_i{}^{\text{twist}}(P,Q) := \alpha_i^{\text{twist}}(P,Q)^{\frac{q^k-1}{r}}.$$

In Section 3, we use the exponential relationship between the reduced Ate$_i$ pairing $\hat{\alpha}_i(Q, P)$ and the Tate pairing $e(Q, P)$:

$$\hat{\alpha}_i(Q,P)^{c_i} = \alpha_i(Q,P)^{c_i \frac{q^k-1}{N_i} \frac{N_i}{r}} = e(Q,P)^{\frac{L_i N_i}{r}}.$$

Note that the exponent $\frac{L_i N_i}{r}$ is prime to r because $r^2 \nmid (q^k-1)$.

Improvements to Ate$_i$ pairing have been proposed. For example, the R-Ate pairing has been proposed by Lee et al. [20], optimal pairing has been proposed by Vercauteren [29], and a generalization of optimal pairing has been proposed by Hess [13]. However, we do not present further information on these pairings in the present paper because the present approach is applied herein only to Ate$_i$ and twisted Ate$_i$ pairings.

B. Pairing inversion problem

As mentioned in Section 1, the pairing inversion problem consists of finding a point (or a pair of points) on an elliptic curve from the value of a pairing function.

Galbraith et al. [11] and Satoh [26] have already considered the pairing inversion problem theoretically. Satoh [26] discussed the difficulty of the pairing inversion and related problems(e.g., the Weak Diffie-Hellman problem). Galbraith et al. [11] gave a detailed discussion of inverting a final exponentiation and inverting a Miller computation.

In the present paper, we formulate the pairing inversion problem according to [11]. In this subsection, G_1 and G_2 are additive groups of order r. Later, we will consider the case $(G_1, G_2) = (\mathbb{G}_1, \mathbb{G}_2)$ or $(\mathbb{G}_2, \mathbb{G}_1)$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are the groups introduced in Section 2.1. The group of r-th roots of unity is denoted as μ_r, and the pairing function e_r is assumed to be given.

Definition *1:* (FAPI-1, FAPI-2 and GPI)
Fixed Argument Pairing Inversion 1 (FAPI-1): Given a pairing e_r, $P \in G_1$ such that $e_r(P, G_2) = \mu_r$ and $z \in \mu_r$, compute $Q \in G_2$ such that $e_r(P, Q) = z$.
Fixed Argument Pairing Inversion 2 (FAPI-2): Given a pairing e_r, $Q \in G_2$ such that $e_r(G_1, Q) = \mu_r$ and $z \in \mu_r$, compute $P \in G_1$ such that $e_r(P, Q) = z$.
Generalized Pairing Inversion (GPI): Given a pairing e_r and a value $z \in \mu_r$, find $(P, Q) \in G_1 \times G_2$ with $e_r(P, Q) = z$.

As in [26], we consider the FAPI-1 problem in the present paper.

When $e_r(P, Q)$ is a (reduced) Tate pairing, or a variant thereof (e.g., η_T or Ate), it is natural to attempt to invert the pairing $e_r(P,Q) = f_{s,P}(Q)^{\frac{q^k-1}{r}}$ by first inverting the final exponentiation (i.e., by taking $\frac{q^k-1}{r}$-th roots in the finite field) and then inverting the pairing function (Miller inversion). Here, we formulate the Miller inversion.

Definition *2:* Miller inversion (MI): Let D_1 be fixed, and let $\mathcal{S}$ be a set of divisors. Let $z \in \mathbb{F}_{q^k}^*$. Compute a divisor $D_2 \in \mathcal{S}$ such that $z = f_{s,D_1}(D_2)$, or, if no such divisor exists, then output "no solution".

III. Inversion of Ate$_i$ pairing

In this section, we explain the main result of the present paper. First, we give the definition of EI:

Definition *3:* (Exponentiation Inversion, EI) For an unknown element $\beta \in \mathbb{F}_{q^k}^*$, assume that an integer n and the value of $w := \beta^n \in \mathbb{F}_{q^k}^*$ are known. Then, the EI, or (n, w)-EI, is the problem of finding β from the instance (n, w).

When w is a value of a reduced pairing and $n = \frac{q^k-1}{r}$, (n, w)-EI corresponds to inverting the final exponentiation. However, we will deal with (n, w)-EI for general n in the present paper.

We demonstrate that the pairing inversion problem of Ate$_i$ pairings for many cases is reduced to the EI. The basic concept of our approach is to use cyclotomic polynomial $\Phi_k(X)$ for embedding degree k. As in Proposition 2.4 in [9], $\Phi_k(q) \equiv 0 \pmod{r}$ is equivalent to that the embedding degree is k. Therefore, we obtain a relationship among the Tate pairing and a number of Ate$_i$ pairings using $\Phi_k(X)$.

A. FAPI-1 on $\mathbb{G}_2 \times \mathbb{G}_1$

Here, we consider FAPI-1 on $\mathbb{G}_2 \times \mathbb{G}_1$ (Input: $z \in \mu_r \subset \mathbb{F}_{q^k}^*$ and $Q \in \mathbb{G}_2$, Output: $P \in \mathbb{G}_1$ such that $z = e_r(Q,P)$), although the basic strategy does not depend on whether pairings are defined on $\mathbb{G}_2 \times \mathbb{G}_1$ or $\mathbb{G}_1 \times \mathbb{G}_2$.

We first explain the case for which the embedding degree is $k = 12$. The proposed approach can be described very simply for $k = 12$, which is currently the most popular embedding degree for implementation (see e.g., [7], [23]) because good parameterized curves, so-called BN-curves [3], can be obtained with $k = 12$.

1) The $k = 12$ case: The cyclotomic polynomial $\Phi_{12}(X)$ is $X^4 - X^2 + 1$. Therefore, r divides $\Phi_{12}(q) = q^4 - q^2 + 1$, that is, $T_i := q^i \bmod r$ satisfies the following:

$$T_4 - T_2 + 1 \equiv 0 \pmod{r}.$$

We write $T_4 - T_2 + 1 = rU$, where $U \in \mathbb{Z}$. Therefore, we obtain

$$f_{T_4-T_2,Q} = f_{-1+rU,Q}. \tag{1}$$

The right-hand side of (1) can be expressed

$$\begin{aligned} f_{-1+rU,Q} &= f_{rU,Q} f_{-1,Q} \frac{l_{[rU]Q,-Q}}{v_{[rU-1]Q}} \\ &= f_{r,Q}^U f_{U,rQ} \cdot \frac{1}{v_Q} = f_{r,Q}^U \cdot \frac{1}{v_Q}. \end{aligned}$$

The left-hand side of (1) can be expressed

$$\begin{aligned} f_{T_4-T_2,Q} &= f_{T_4,Q} f_{-T_2,Q} \frac{l_{[T_4]Q,[-T_2]Q}}{v_{[T_4-T_2]Q}} \\ &= f_{T_4,Q} \frac{1}{f_{T_2,Q} \cdot v_{[T_2]Q}} \cdot \frac{l_{[T_4]Q,[-T_2]Q}}{v_{-Q}} \\ &= \frac{f_{T_4,Q}}{f_{T_2,Q}} \cdot \frac{l_{[T_4]Q,[-T_2]Q}}{v_{[T_2]Q}} \cdot \frac{1}{v_Q}. \end{aligned}$$

Therefore, by comparing the left- and right-hand sides, we have

$$\frac{f_{T_4,Q}}{f_{T_2,Q} f_{r,Q}^U} = \frac{v_{[T_2]Q}}{l_{[T_4]Q,[-T_2]Q}}.$$

By normalization and evaluation at $P = (x_P, y_P)$, we obtain the relationship among pairings:

$$\frac{\alpha_4(Q,P)}{\alpha_2(Q,P)\tau(Q,P)^U} = \frac{x_P - x_{[T_2]Q}}{ax_P + y_P + b},$$

where $\tau(Q,P) := f_{r,Q}(P)$ and $ax + y + b$ is the normalized function of $l_{[T_4]Q,[-T_2]Q}$.

If attackers obtain values of three pairings $\alpha_4(Q,P)$, $\alpha_2(Q,P)$, and $\tau(Q,P)$, they are able to compute $\beta := \alpha_4(Q,P)\alpha_2(Q,P)^{-1}\tau(Q,P)^{-U}$ and find the point $P = (x_P, y_P)$ by solving $(ax_P + y_P + b)\beta = x_P - x_{[T_2]Q}$ and the defining equation of E, namely, $y_P^2 + a_1 x_P y_P + a_3 y_P = x_P^3 + a_2 x_P^2 + a_4 x_P + a_6$.

We next consider the method of computing the three pairing values. Usually, attackers are assumed to obtain one pairing value. For example, for the case in which we use BN-curves [3] to implement pairings with $k = 12$, the most efficient Ate$_i$ pairing is $\alpha_1(Q,P)$. Therefore, we may assume that the attackers know the value of the (reduced) pairing $\hat{\alpha_1}(Q,P) = \alpha_1(Q,P)^{\frac{q^k-1}{r}}$. Hence, the attackers must obtain values of $\alpha_4(Q,P)$, $\alpha_2(Q,P)$, and $\tau(Q,P)$ from $\hat{\alpha_1}(Q,P)$. However, under the assumption that the EI can be solved efficiently, the attackers can compute $\alpha_4(Q,P)$, $\alpha_2(Q,P)$, and $\tau(Q,P)$ from $\hat{\alpha_1}(Q,P)$. First, the attackers compute $\hat{\alpha_4}(Q,P)$, $\hat{\alpha_2}(Q,P)$, and $e(Q,P)$ by the exponential relationship

$$\hat{\alpha_i}(Q,P)^{c_i} = e(Q,P)^{\frac{L_i N_i}{r}}.$$

(Of course, attackers can easily compute N_i, L_i, and c_i for all i.) Then, attackers compute $\alpha_4(Q,P)$, $\alpha_2(Q,P)$, and $\tau(Q,P)$ by inverting the final exponentiation. Note that $e(Q,P) = \tau(Q,P)^{\frac{q^k-1}{r}}$ (see p. 4596 of [14]).

Therefore, FAPI-1 of the Ate$_i$ pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ is reduced to the EI for the case in which $k = 12$.

2) Other case: The general case is similar to the $k = 12$ case. We show the cyclotomic polynomial $\Phi_k(X)$ and the relationships among pairings for various embedding degrees, $k(> 1)$.

Case 1: $k = 2^\mu 3^\nu$ ($\mu \geq 1$, $\nu \geq 1$)

This is a direct generalization of the $k = 12$ case. The cyclotomic polynomial is $\Phi_k(X) = X^{\frac{k}{3}} - X^{\frac{k}{6}} + 1$. In the same manner as for the $k = 12$ case, we obtain the following relationship

$$\frac{\alpha_{\frac{k}{3}}(Q,P)}{\alpha_{\frac{k}{6}}(Q,P)\tau(Q,P)^U} = \frac{v_{[T_{k/3}]Q}(P)}{l_{[T_{k/3}]Q,-[T_{k/6}]Q}(P)},$$

where $U = \dfrac{T_{k/3} - T_{k/6} + 1}{r}$.

Case 2: $k = 3^\nu$ ($\nu \geq 1$)

The cyclotomic polynomial is $\Phi_k(X) = X^{\frac{2k}{3}} + X^{\frac{k}{3}} + 1$, and the pairing relationship is

$$\frac{\alpha_{\frac{2k}{3}}(Q,P)\alpha_{\frac{k}{3}}(Q,P)}{\tau(Q,P)^U} = \frac{1}{l_{[T_{2k/3}]Q,[T_{k/3}]Q}(P)},$$

where $U = \dfrac{T_{2k/3} + T_{k/3} + 1}{r}$.

Case 3: $k = 2^\mu (\mu \geq 1)$

The cyclotomic polynomial is $\Phi_k(X) = X^{\frac{k}{2}} + 1$. In this case, at first it might appear that no pairing relationship exists. However, multiplying by the polynomial $X + 1$, we obtain

$$T_{k/2+1} + T_{k/2} + T_1 + 1 \equiv 0 \pmod{r}.$$

Thus, we obtain the following relationship:

$$\begin{aligned} &\frac{\alpha_{\frac{k}{2}+1}(Q,P)\alpha_{\frac{k}{2}}(Q,P)\alpha_1(Q,P)}{\tau(Q,P)^U} \\ &= \frac{x_P - x_{[T_{\frac{k}{2}}+T_1]Q}}{l_{[T_{\frac{k}{2}}]Q,Q}(P) \cdot l_{[T_{\frac{k}{2}+1}]Q,[T_{\frac{k}{2}}+T_1]Q}(P)}, \end{aligned}$$

where $U = \dfrac{T_{k/2+1} + T_{k/2} + T_1 + 1}{r}$.

For general k, $\sum_{i=0}^{k-1} T_i \equiv 0 \pmod{r}$ holds because the cyclotomic polynomial $\Phi_k(X)$ satisfies $\Phi_k(X) | \sum_{i=0}^{k-1} X^i$. Therefore, we obtain the following relationship:

$$\tau(Q,P)^{-U} \prod_{i=1}^{k-1} \alpha_i(Q,P) = \prod_{i=2}^{k-1} \frac{v_{[W_i]Q}(P)}{l_{[T_i]Q,[W_i]Q}(P)},$$

where $U = \frac{\sum_{i=1}^{k-1} T_i}{r}$ and $W_i := \sum_{j=0}^{i-1} T_j$ $(i \geq 2)$. Thus, we obtain a pairing relationship using all of the Ate$_i$ pairings $\alpha_i(Q, P)$ $(i = 1, 2, \cdots, k-1)$.

We estimate the running cost of reduction from the pairing inversion to the EI. We assume the use of pairing-friendly elliptic curves. Then, it may be assumed that $k \leq \log_2(q)$ because the embedding degrees of pairing-friendly elliptic curves are less than $\log_2(r)/8$ (see Section 2 of [9]). Thus, the number of using an algorithm for solving the EI to compute $\alpha_i(P, Q)$ is less than $2\log_2(q)$. The complexity of finding $P = (x_P, y_P)$, namely solving $\beta = \prod_{i=2}^{k-1} \frac{v_{[W_i]Q}(P)}{l_{[T_i]Q,[W_i]Q}(P)}$ and the defining equation of E, is $O(k)$ because the degree of the former equation is $O(k)$. Therefore, the reduction from the pairing inversion to the EI can be performed in polynomial time in $\log(q)$.

B. FAPI-1 on $\mathbb{G}_1 \times \mathbb{G}_2$

Next, we consider FAPI-1 on $\mathbb{G}_1 \times \mathbb{G}_2$ (Input: $z \in \mu_r \subset \mathbb{F}_{q^k}^*$ and $P \in \mathbb{G}_1$, Output: $Q \in \mathbb{G}_2$ such that $z = e_r(P, Q)$). In this case, the definitions of Ate and Ate$_i$ pairings depend on whether E is supersingular or ordinary. When E is supersingular, the Ate$_i$ pairing on $\mathbb{G}_1 \times \mathbb{G}_2$ is defined by $f_{T_i,P}(Q)$. Therefore, we consider the case for $\mathbb{G}_2 \times \mathbb{G}_1$ in a similar manner. The exponential relationship between the Ate$_i$ pairing and the Tate pairing also holds in the $\mathbb{G}_1 \times \mathbb{G}_2$ case. Therefore, we can solve FAPI-1 on $\mathbb{G}_1 \times \mathbb{G}_2$ if the EI can be solved efficiently.

Next, we consider the case in which E is ordinary. In this case, the target pairing is the twisted Ate$_i$ pairing $f_{T_i^e,P}(\psi(Q'))$, where $e = k/\gcd(k, d)$. Therefore, we must consider the values of both k and d. Since $m := \gcd(k, d) = 1, 2, 3, 4, 6$, we classify the results according to m.

When $m = 3, 4, 6$, then $q^k - 1 = q^{me} - 1$ is factored as

$$q^{6e} - 1 = (q^e - 1)(q^e + 1)(q^{2e} + q^e + 1)(q^{2e} - q^e + 1),$$
$$q^{4e} - 1 = (q^e - 1)(q^{3e} + q^{2e} + q^e + 1),$$
$$q^{3e} - 1 = (q^e - 1)(q^{2e} + q^e + 1).$$

Thus, we have the following relationships among $S_{e,i} = q^{ie} \bmod r$:

$$S_{e,2} - S_{e,1} + 1 \equiv 0 \pmod{r} \quad (\text{if } m = 6),$$
$$S_{e,3} + S_{e,2} + S_{e,1} + 1 \equiv 0 \pmod{r} \quad (\text{if } m = 4),$$
$$S_{e,2} + S_{e,1} + 1 \equiv 0 \pmod{r} \quad (\text{if } m = 3).$$

By setting $S_{e,2} - S_{e,1} + 1 = rU$ and performing computations similar to those performed in the previous cases, we have

$$\frac{f_{S_{e,2},P}}{f_{S_{e,1},P} f_{r,P}^U} = \frac{v_{[S_{e,1}]P}}{l_{[S_{e,2}]P,[-S_{e,1}]P}}.$$

After substituting $Q = (x_Q, y_Q)$, we obtain the following relationship among pairings:

$$\frac{\alpha_2^{\text{twist}}(P, Q)}{\alpha_1^{\text{twist}}(P, Q)\tau(P, Q)^U} = \frac{v_{[S_{e,1}]P}(Q)}{l_{[S_{e,2}]P,[-S_{e,1}]P}(Q)}$$

for $m = 6$ and

$$\frac{\prod_{i=1}^{3} \alpha_i^{\text{twist}}(P, Q)}{\tau(P, Q)^U} = \frac{v_{[S_{e,2}+S_{e,1}]P}(Q)}{l_{[S_{e,2}]P,[S_{e,1}]P}(Q) \cdot l_{[S_{e,3}]P,[S_{e,2}+S_{e,1}]P}(Q)},$$
$$\frac{\alpha_4^{\text{twist}}(P, Q)\alpha_2^{\text{twist}}(P, Q)}{\tau(P, Q)^U} = \frac{1}{l_{[S_{e,2}]P,[S_{e,1}]P}(Q)}$$

for $m = 4$ and 3, respectively.

When $m = 2$, then $q^k - 1 = q^{me} - 1 = q^{2e} - 1 = (q^e - 1)(q^e + 1)$. Thus, unlike the cases in which $m = 3, 4, 6$, no relationship among pairings is obtained. Finally, we consider the case in which $m = 1$, where $S_{e,i} = q^{ie} \bmod r = q^{ik} \bmod r = 1$, because $e = k$. Thus, the proposed approach cannot be applied in these cases.

We assume that $\mathbb{F}_q$ is a prime field, i.e., $q = p$. Then, $\mathbb{F}_{q^k}$ is a pairing-friendly field if $p \equiv 1 \pmod{12}$ and $k = 2^\mu 3^\nu$ is even (see [19]). We present examples in which $m = 1, 2$ for $k = 2^\mu 3^\nu$ $(\mu \geq 1)$. When $k = 2^\mu$ $(\mu \geq 1)$, if $d = 3$, then $m = 1$, and if $(k, d) = (2^\mu, 2), (2, 4)$, or $(2^\mu, 6)$, then $m = 2$. Finally, when $k = 2^\mu 3^\nu$ $(\mu, \nu \geq 1)$, if $(k, d) = (2^\mu 3^\nu, 2)$ or $(2 \cdot 3^\nu, 4)$, then $m = 2$.

Usually, we choose elliptic curves with large d (i.e., $d = 4, 6$) so that point compress techniques, which are analogous to techniques using distortion maps in the case of supersingular curves, can be used. Therefore, the number of examples to which the proposed approach cannot be applied is not large in the case of pairing-friendly fields.

Thus, the proposed approach can be applied to FAPI-1 of the twisted Ate$_i$ pairing on $\mathbb{G}_1 \times \mathbb{G}_2$ in numerous practical cases.

IV. Conclusion

In the present paper, we have demonstrated that, in several cases, FAPI-1 of the Ate$_i$ pairing is reduced to solving the EI.

The proposed approach can be applied to other pairings, the R-Ate pairing [20] and the optimal pairing [29] (and the generalization by Hess [13]), by converting the inversion problem of these pairings to that of the Ate$_i$ pairing since these pairings also have exponential relationships with the Tate pairing. Thus, similar results can be obtained for these pairings.

However, our approach is not practical because the EI is not easy. So, these results do not demonstrate that pairing-based cryptosystems are insecure.

Applying our approach to FAPI-2 is still an open problem.

Acknowledgement

The authors would like to thank the anonymous referees for various improvements and thank Professor Tsuyoshi Takagi and Doctors Katsuyuki Takashima and Katsuyuki Okeya for their valuable comments to an earlier version of the present paper.

REFERENCES

[1] P.S.L.M. Barreto, S. Galbraith, C. ÓhÉigeartaigh, and M. Scott, "Efficient pairing computation on supersingular abelian varieties", Designs, Codes and Cryptography, Vol. 42, No. 3, pp. 239–271, Springer, 2007.

[2] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems", Crypto 2002, LNCS, Vol. 2442, pp. 354–368, Springer-Verlag, Berlin-Heidelberg-New York, 2002.

[3] P.S.L.M. Barreto and M. Naehrig, "Pairing-friendly elliptic curve of prime order", SAC 2005, LNCS, Vol. 3897, pp. 319–331, Springer-Verlag, Berlin-Heidelberg-New York, 2006.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", CRYPTO 2001, LNCS, Vol. 2139, pp. 213–229, Springer-Verlag, Berlin-Heidelberg-New York, 2001.

[5] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from Weil pairing", ASIACRYPT 2001, LNCS, Vol. 2248, pp. 514–532, Springer-Verlag, Berlin-Heidelberg-New York, 2001.

[6] I. Duursma and H.S. Lee, "Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$", ASIACRYPT 2003, LNCS, Vol. 2894, pp.111–123, Springer-Verlag, Berlin-Heidelberg-New York, 2003.

[7] A.J. Devegili, M. Scott, and R. Dahab, "Implementing cryptographic pairings over Barreto-Naehrig curves", Pairing Conference 2007, LNCS, Vol. 4575, pp. 197–207, Springer-Verlag, Berlin-Heidelberg-New York, 2007.

[8] G. Frey and H.G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", Math. Comp., Vol. 62, No. 206, 865–874, 1994.

[9] D. Freeman, M. Scott, and E. Teske, "A taxonomy of pairing-friendly elliptic curves", Journal of Cryptology, Vol. 23, No. 2, pp. 224–280, 2010.

[10] S. Galbraith, K. Harrison, and S. Soldera, "Implementing the Tate pairing," ANTS V, LNCS, Vol. 2369, pp.324–337, Springer-Verlag, Berlin-Heidelberg-New York, 2002.

[11] S. Galbraith, F. Hess, and F. Vercauteren, "Aspects of pairing inversion", IEEE Trans. Information Theory, Vol. 54, No. 12,pp. 5719–5728, 2008.

[12] S. D. Galbraith, C. O hEigeartaigh, and C. Sheedy, "Simplified pairing computation and security implications", J. Mathematical Crypt, Vol. 1, No. 3, pp. 267–281, 2007,

[13] F. Hess, "Pairing lattices", Pairing 2008, LNCS, Vol. 5209, pp. 18–38, Springer-Verlag, Berlin-Heidelberg-New York, 2008.

[14] F. Hess, N.P. Smart, and F. Vercauteren, "The Eta pairing revisited", IEEE Transaction on Information Theory, Vol. 52, No. 10, pp. 4595–4602, October 2006.

[15] A. Joux, "A one round protocol for tripartite Diffie-Hellman", Algorithmic Number Theory Symposium–ANTS IV, LNCS, Vol. 1838, pp. 385–394, Springer-Verlag, Berlin-Heidelberg-New York, 2000.

[16] S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto, "Optimised versions of the Ate and twisted Ate pairings", S. Galbraith, editor, Eleventh IMA International Conference on Cryptography and Coding, LNCS, Vol. 4887, Springer-Verlag, Berlin-Heidelberg-New York, pp. 302–312, 2007.

[17] A.J. Menezes, T. Okamoto, and S.A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", IEEE Trans. Inform. Theory 39, No. 5, pp. 1639–1646, 1993.

[18] A.J. Menezes, Y.H. Wu, and R.J. Zuccherato, "An elementary introduction to hyperelliptic curves", in Algebraic Aspects of Cryptography, - Algorithms and Computation in Mathematics, by N. Koblitz, Springer-Verlag, Berlin-Heidelberg-New York, 1997.

[19] N. Koblitz and A. Menezes, "Pairing-based cryptography at high security level", Cryptography and Coding: 10th IMA International Conference, LNCS, Vol. 3796, pp13-36, Springer-Verlag, Berlin-Heidelberg-New York, 2005.

[20] E. Lee, H.S. Lee, and C.M. Park, "Efficient and generalized pairing computation on abelian varieties", IEEE Transactions on Information Theory, Vol. 55, No. 4, pp. 1793–1803, 2009.

[21] V.S. Miller, "Short programs for functions on curves", 1986. `http://crypto.stanford.edu/miller/miller.pdf`

[22] V.S. Miller. "The Weil pairing and its efficient calculation", Journal of Cryptology, Vol. 17, No. 4, pp. 235–261, 2004.

[23] Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa, "Integer variable χ-based Ate pairing", Pairing 2008, LNCS, Vol. 5209, Springer-Verlag, Berlin-Heidelberg-New York, pp.178–191, 2008.

[24] D. Page and F. Vercauteren, "A fault attack on pairing based cryptography", IEEE Transactions on Computers, Vol. 55, No. 9, pp. 1075–1080, 2006.

[25] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing", SCIS 2000, 2000.

[26] T. Satoh, "On pairing inversion problems", Pairing 2007, LNCS, Vol. 4575, pp. 317-328, Springer-Verlag, Berlin-Heidelberg-New York, 2007.

[27] C.-A. Zhao, F. Zhang and J. Huang "A Note on the Ate pairing", International Journal of Information Security, Vol. 6, No. 7, pp. 379–382, 2008.

[28] F. Vercauteren, "The hidden root problem", Pairing 2008, LNCS, Vol. 5209, pp.89-99, Springer-Verlag, Berlin-Heidelberg-New York, 2008.

[29] F. Vercauteren, "Optimal pairings", IEEE Transactions on Information Theory, Vol. 56, No. 1, pp. 455–461, 2010.

Naoki Kanayama received his B.E, B.S, M.S and D.S degrees from Waseda University, Tokyo, Japan, in 1994, 1996, 1998 and 2003, respectively. In 2003–2006, he was a post-doctoral fellow of the Japan Society for the Promotion of Science. From 2006, he is a research fellow at University of Tsukuba. His research interests are cryptography and information security.

Eiji Okamoto received his B.S., M.S. and Ph.D degrees in electronics engineering from the Tokyo Institute of Technology in 1973, 1975 and 1978, respectively. He worked and studied communication theory and cryptography for NEC central research laboratories since 1978. From 1991 he became a professor at Japan Advanced Institute of Science and Technology, then at Toho University. Now he is a professor at Graduate School of Systems and Information Engineering, University of Tsukuba. His research interests are cryptography and information security. He is a coeditor-in-chief of International Journal of Information Security.