著者 | 答 Counseling Laboratory, School of Information Science, University of Tsukuba, Japan
---|---
タイトル | Approach to pairing inversions without solving Miller inversion
ジャーナル | IEEE Transactions on Information Theory
巻 | 58
号 | 2
ページ | 1248-1253
年 | 2012
著者 | Kanayama Naoki, Okamoto Eiji
権利 | (C) 2012 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works
URL | http://hdl.handle.net/2241/116856
doi | 10.1109/TIT.2011.2173714
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 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 pairing can be solved without solving the Miller inversion. Thus, the pairing inversion problem of Ate pairing is reduced to the exponentiation inversion problem.

Index Terms—Ate, 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 \( \eta_T \) 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 \( 2^{r-1} \)-th root of the input \( \alpha \in G_T \).

**Step 2:** For the solution \( \beta \) 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 \( 2^{r-1} \) roots of **Step 1**. However, as shown in [11], it suffices to choose a random \( \sqrt{\frac{r}{2}} \) 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 \( \alpha \). If attackers are able to access the value \( \alpha' := f_{S+1,P}(Q) \), they can obtain the value of \( \ell_{[S-1],P}(Q)/\ell_{[\alpha],P}(Q) \) from \( \alpha \) and \( \alpha' \)(see Section 2 for the notation \( \ell \) and \( \ell_\cdot \)). 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 pairings are variants of the Ate pairing proposed by Hess et al. [14]. Ate pairings shorten the length of the Miller loop by \( 1/\phi(k) \) for certain types of pairing-friendly el-
lithic 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$_1$ 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 $E(\mathbb{F}_q^*)$ ($j \geq 1$) be the group of $\mathbb{F}_q$-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 $r \nmid E(\mathbb{F}_q)$ 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 $r^2 \not| (q^k - 1)$.

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 $E$: $D = \sum m_i P_i, m_i \in \mathbb{Z}$. Here, $m_i$ is referred to as the order of $D$ on $P_i$, and we write $\text{ord}_P(D) = m_i$. The degree of $D$, denoted by $\deg D$, is defined as $\deg D := \sum_{P \in E} m_P$.

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 $D = \text{div}(h)$.

For a point $P \in E(\mathbb{F}_q^*)$ and an integer $s$, we define a rational function on $E$, denoted by $f_s, P(X,Y)$ or simply $f_s, P$, over $\mathbb{F}_q$, as a function with $\text{div}(f_s, P) = s(P) - (1 - s - 1)(O)$, 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 field ground 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]):

- $f_{-n, P} = f_{-n, P} = f_{n, P}^{-1}$ for a positive integer $n$,
- $f_{a+b, P} = f_{a, P} \cdot f_{b, P}$ for integers $a$ and $b$,
- $f_{a, b, P} = f_{a, P} \cdot f_{b, P}$ 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 $P \in E(\mathbb{F}_q^*)$ such that $[r]P \in \mathbb{O}$ and $Q \in E(\mathbb{F}_q^*)$ such that $\text{div}(f_r, P)$ and $D = (Q + R) - (R)$ are disjoint. Then, the Tate pairing is defined by

$$\langle \cdot, \cdot \rangle_r : E(\mathbb{F}_q^*)[r] \times E(\mathbb{F}_q^*)[r] \rightarrow \mathbb{F}_q^{\times r}/(\mathbb{F}_q^{\times r})^*,$$

$$(P, Q) \mapsto \langle P, Q \rangle_r := f_{r, P} (D).$$

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

$$e : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_q)[r] \rightarrow \mu_r,$$

$$e(P, Q) = \langle P, Q \rangle_r^{q^k - 1}/r,$$

where $\mu_r$ 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 $\eta_	ext{II}$ 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 $\eta_	ext{II}$ pairing. These can be applied to both supersingular curves and ordinary elliptic curves. In 2007, Zhao et al. [27] proposed the Ate$_1$ and twisted Ate$_1$ pairings.

We review here the Ate$_1$ pairing because we will consider the inversion problem of Ate$_1$ pairings.

3) Ate$_1$ and twisted Ate$_1$ pairings: Let $\theta$ be a Frobenius endomorphism on $E$ is denoted as $\pi_q$, i.e., $\pi_q : (x, y) \mapsto (x^q, y^q)$. We consider the following two groups: $G_1 = E(\mathbb{F}_q)[r] = E[\pi_q - \pi_q - 1] - G_2 = E[\pi_q - \pi_q - 1]$. Let $T_i := q^i \bmod r$ for $i = 1, 2, \ldots, k - 1$. 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$_1$ pairing has two versions: the pairing defined on $G_2 \times G_1$ and the pairing on $G_1 \times G_2$. The Ate$_1$ pairing on $G_2 \times G_1$ is defined by $\alpha_1(P, Q) := f_{T_i, Q}^{\text{norm}}(P)$ ($Q \in G_2$ and $P \in G_1$), where $E$ may be either supersingular or ordinary. Here, $f_{T_i, Q}$ is the normalization of $f_{T_i, Q}$. As mentioned at the beginning of this section, the rational function with $\text{div}(f_{T_i, Q}) = T_i(Q) - (T_i - 1)(O)$ is uniquely determined up to non-zero scalar multiples. When the point $Q$ is in $E(\mathbb{F}_q)$, the multiples are in $\mathbb{F}_q$ and will not be annihilated by final exponentiation. Therefore, we need to consider the normalization. We can use the normalization function $f_{T_i, Q}^{\text{norm}} = f_{T_i, Q}/\gamma$, 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 $G_1 \times G_2$, we must consider whether $E$ is supersingular. When $E$ is supersingular, the Ate$_1$ pairing is defined by $\alpha_1(P, Q) := f_{T_i, P}^{\text{norm}}(Q)$ ($P \in G_1$ and $Q \in G_2$). If $E$ is ordinary, $f_{T_i, P}^{\text{norm}}(Q)$ does not have bilinearity on $G_1 \times G_2$, 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 $\psi : E' \rightarrow E$ 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 pairing on $G_1 \times G_2$ for ordinary elliptic 
curves. Let $m := \gcd(d, k)$, and let $e := k/m$ for an ordinary 
elliptic curve $E$ with embedding degree $k$. Put $S_{e,i} := T_i^e \mod r$. Then, the Ate pairing on $G_1 \times G_2$, referred 
to as the twisted Ate pairing, is defined by $\alpha_{i, \text{twist}}(P, Q) := 
\Phi_{s_{e,i}, f}(Q)$ ($P \in G_1$ and $Q \in G_2$). Note that normalization is 
not required in this case because $P$ is in $E(F_q)$ and constants 
of $f_{T_i, P}$ or $f_{S_{e,i}, P}$ are in $F_q$.

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

Let
$$
c_i := \begin{cases} 
\sum_{j=0}^{m-1} T_i^{e(m-1-j)} q^{(e i) j} \equiv mq^{m-1} \quad (\text{mod } N_i) 
\end{cases}
$$

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

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

The reduced Ate, and twisted Ate, pairings are denoted as 
$\alpha_i(Q, P)$ (or $\alpha_i(P, Q)$) and $\alpha_i^{\text{twist}}(P, Q)$:
$$
\hat{\alpha}_i(Q, P) := \alpha_i(Q, P)^{q^{k-1}},
\hat{\alpha}_i(P, Q) := \alpha_i(P, Q)^{q^{k-1}},
\hat{\alpha}_i^{\text{twist}}(P, Q) := \alpha_i^{\text{twist}}(P, Q)^{q^{k-1}}.
$$

In Section 3, we use the exponential relationship between 
the reduced Ate pairing $\hat{\alpha}_i(Q, P)$ and the Tate pairing 
$e(Q, P)$:
$$
\hat{\alpha}_i(Q, P)^{\alpha_i} = \alpha_i(Q, P)^{\alpha_i(q^{k-1}/N_i)} = e(Q, P)^{\frac{L_i N_i}{r}}.
$$

Note that the exponent $\frac{L_i N_i}{r}$ is prime to $r$ because $r^2 \not\equiv 1 (q^{k-1})$.

Improvements to Ate 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 and twisted Ate 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 consid-
 ered 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 
$(G_1, G_2) = (G_1, G_2)$ or $(G_2, G_1)$, where $G_1$ and $G_2$ 
are the groups introduced in Section 2.1. The group of $r$-th roots of 
unity is denoted as $\mu_r$, 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., $\eta_T$ or Ate), it is natural to attempt to invert 
the pairing $e_r(P, Q) = f_{s_{e,i}, f}(Q)$ by first inverting the 
final exponentiation (i.e., by taking $\frac{q^{k-1}}{N_i}$ 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 $S$ be a set of divisors. Let $z \in F_q^*$. Compute a divisor 
$D_2 \in S$ such that $z = f_{s_{e,i}, D_1}(D_2)$, or, if no such divisor exists, 
then output "no solution".

### III. INVERSION OF ATEI 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 $\beta \in F_q^*$, assume that an integer $n$ and the 
value of $w := \beta^n \in F_{q^k}$ are known. Then, the EI, or $(n, w)$-
EI, is the problem of finding $\beta$ 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 
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 pairings using $\Phi_k(X)$.
A. FAPI-I on $\mathbb{G}_2 \times \mathbb{G}_1$

Here, we consider FAPI-I on $\mathbb{G}_2 \times \mathbb{G}_1$ (Input: $z \in \mu_r \subset \mathbb{F}_q^*$ 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, $T_i := q^i \text{ mod } r$ 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

$$f_{T_4 - T_2, Q} = f_{-1 + ru, Q}.$$  

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

$$f_{-1 + ru, Q} = f_{ru, Q}f_{-1, Q} \frac{l_{ru}[u - ru]{Q} - Q}{v[u - 1]Q} = f_{ru, Q}f_{-1, u} \frac{1}{v-Q} = f_{ru, Q} \frac{1}{v-Q}.$$ 

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

$$f_{T_4 - T_2, Q} = f_{T_4, Q}f_{-T_2, Q} \frac{l_{T_2}[Q, -T_2]{Q}}{v[T_2]{Q}} = f_{T_4, Q}f_{-T_2, Q} \frac{1}{v-T_2{Q}} = f_{T_4, Q} \frac{1}{v-Q}.$$ 

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

$$f_{T_4, Q}f_{-T_2, Q} = \frac{v[T_2]{Q}}{v[T_2][Q, -T_2]{Q}}.$$ 

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

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, $y_P^3 + a_1x_Py_P + a_3y_P = x_P^3 + a_2x_P^2 + a_4x_P + a_6$.

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 pairing is $\alpha_1(Q, P)$. Therefore, we may assume that the attackers know the value of the (reduced) pairing $\hat{\alpha}_1(Q, P)$. 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 EL 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 $\alpha_4(Q, P), \alpha_2(Q, P),$ and $e(Q, P)$ by the exponential relationship

$$\hat{\alpha}_1(Q, P)^{ci} = e(Q, P)^{\frac{1}{r}l_{T_2}{Q}}.$$ 

(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 $e(Q, P) = \tau(Q, P)^{\frac{1}{r}l_{T_2}{Q}}$ (see p. 4596 of [14]).

Therefore, FAPI-I of the Ate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ is reduced to the EL 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 $\Phi_k(X) = X^\frac{k}{2} - X^\frac{k}{3} + 1$. In the same manner as for the $k = 12$ case, we obtain the following relationship

$$\frac{\alpha_\frac{k}{2}(Q, P)}{\alpha_\frac{k}{3}(Q, P)\tau(Q, P)^U} = \frac{v[T_i]{Q}}{l[T_i]{Q, -T_i}{Q}}q^{(P)},$$

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

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

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

$$\frac{\alpha_2^3(Q, P)\alpha_\frac{k}{3}(Q, P)}{\tau(Q, P)^U} = 1 \quad \frac{v[T_i]{Q}}{l[T_i]{Q, -T_i}{Q}}q^{(P)},$$

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

**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

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

Thus, we obtain the following relationship:

$$\frac{\alpha_\frac{k}{2}^2(Q, P)\alpha_\frac{k}{2}(Q, P)\alpha_1(Q, P)}{\tau(Q, P)^U} = \frac{x_P - x[T_\frac{k}{2} + T_1]{Q}q^{(P)}}{l[T_\frac{k}{2}]{Q, Q, [T_\frac{k}{2} + T_1]{Q}}q^{(P)}},$$

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

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:

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

for specific $r$. Note that $\alpha_i(Q, P)$ for $i = 1$ is the Ate pairing.
where \( U = \sum_{i=1}^{k-1} \frac{W_i}{r} \) and \( W_i := \sum_{j=0}^{i-1} T_j \) (\( i \geq 2 \)). Thus, we obtain a pairing relationship using all of the Ate, 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 \( \alpha_i(Q, P) \) is less than \( 2 \log_2(q) \). The complexity of finding \( P = (x_P, y_P) \), namely solving \( \beta = \prod_{i=1}^{k-1} \frac{v_{[W_i]q}(P)}{l_{[P],q}[W_i]q(P)} \) 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 \( G_1 \times G_2 \)

Next, we consider FAPI-1 on \( G_1 \times G_2 \) (Input: \( z \in \mu_r \subset \mathbb{F}_q^\times \) and \( P \in G_1 \), Output: \( Q \in G_2 \) such that \( z = e_{P,Q}(P,Q) \)). In this case, the definitions of Ate and Ate, pairings depend on whether \( E \) is supersingular or ordinary. When \( E \) is supersingular, the Ate pairing on \( G_1 \times G_2 \) is defined by \( f_{\psi}^\ast(P) \). Therefore, we consider the case for \( G_2 \times G_1 \) in a similar manner. The exponential relationship between the Ate pairing and the Tate pairing also holds in the \( G_1 \times G_2 \) case. Therefore, we can solve FAPI-1 on \( G_1 \times G_2 \) 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 pairing \( f_{\psi}^\ast(P) \), where \( e = k/\gcd(k,d) \). Therefore, we must consider the values of both \( k \) and \( d \). Since \( \max := \gcd(k,d) = 1, 2, 3, 4, 6 \), we classify the results according to \( m \).

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

\[
q^6 - 1 = (q-1)(q+1)(q^2 + q + 1)(q^2 - q + 1),
\]

\[
q^4 - 1 = (q-1)(q^3 + q^2 + q + 1),
\]

\[
q^3 - 1 = (q-1)(q^2 + q + 1).
\]

Thus, we have the following relationships among \( S_{e,i} = q^i \) mod \( r \):

\[
S_{e,2} - S_{e,1} + 1 \equiv 0 \pmod{r} \quad \text{(if } m = 6),
\]

\[
S_{e,3} + S_{e,2} + S_{e,1} + 1 \equiv 0 \pmod{r} \quad \text{(if } m = 4),
\]

\[
S_{e,2} + S_{e,1} + 1 \equiv 0 \pmod{r} \quad \text{(if } m = 3).
\]

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

\[
\frac{f_{S_{e,2}},P}{f_{S_{e,1},P} f_{u,P}} = \frac{v_{[S_{e,1}]}(P)}{l_{[S_{e,2}]}[P] - [S_{e,1}]p(Q)}.
\]

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

\[
\frac{\alpha_2(P, Q)}{\alpha_1(P, Q)} = \frac{v_{[S_{e,1}]}(P)}{l_{[S_{e,2}]}[P] - [S_{e,1}]p(Q)}.
\]

for \( m = 6 \) and

\[
\frac{\prod_{i=1}^{3} \alpha_1^{\text{twist}}(P, Q)}{\tau(P, Q)^U} = \frac{v_{[S_{e,2}]}(P) - [S_{e,1}]p(Q)}{l_{[S_{e,2}]}[P] - [S_{e,1}]p(Q)}.
\]

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 \( S_{e,i} = q^i \) mod \( r = q^{ik} \) mod \( r = 1 \), 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 \( k = 2^\nu 3^\mu \) is even (see [19]). We present examples in which \( m = 1, 2 \) for \( k = 2^\mu 3^\nu \) (\( \mu \geq 1 \)). When \( k = 2^\mu 3^\nu \) (\( \mu \geq 1 \)), then \( m = 2 \).

Finally, when \( k = 2^\nu 3^\mu \) (\( \nu \geq 1 \)), if \( (k, d) = (2^\mu 2), (2, 4), (2^\mu 6), \) then \( m = 2 \).

Usually, we choose elliptic curves with large \( d \) (\( d = 4, 6 \)) so that point compression 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 pairing on \( G_1 \times G_2 \) in numerous practical cases.

IV. Conclusion

In the present paper, we have demonstrated that, in several cases, FAPI-1 of the Ate 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 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


Eiji Okamoto received his B.S., 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.