Fixed Argument Pairing Inversion on Elliptic Curves

Sungwook Kim and Jung Hee Cheon

ISaC & Dept. of Mathematical Sciences
Seoul National University
Seoul, Korea
{avell7,jhcheon}@snu.ac.kr

Abstract. Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with a power of prime q, r a prime dividing $\#E(\mathbb{F}_q)$, and k the smallest positive integer satisfying $r|\Phi_k(p)$, called embedding degree. Then a bilinear map $t : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mathbb{F}_{q^k}^*$ is defined, called the Tate pairing. And the Ate pairing and other variants are obtained by reducing the domain for each argument and raising it to some power.
In this paper we consider the *Fixed Argument Pairing Inversion (FAPI)* problem for the Tate pairing and its variants. In 2012, considering FAPI for the Ate$_i$ pairing, Kanayama and Okamoto formulated the *Exponentiation Inversion (EI)* problem. However the definition gives a somewhat vague description of the hardness of EI. We point out that the described EI can be easily solved, and hence clarify the description so that the problem does contain the actual hardness connection with the prescribed domain for given pairings.
Next we show that inverting the Ate pairing (including other variants of the Tate pairing) defined on the smaller domain is neither easier nor harder than inverting the Tate pairing defined on the lager domain. This is very interesting because it is commonly believed that the structure of the Ate pairing is so simple and good (that is, the Miller length is short, the solution domain is small and has an algebraic structure induced from the Frobenius map) that it may leak some information, thus there would be a chance for attackers to find further approach to solve FAPI for the Ate pairing, differently from the Tate pairing.

Key words: Pairing Inverision, Fixed Argument Pairing Inversion, Exponentiation Inversion, Tate Pairing, Ate pairing.

1 Introduction

Pairings have played an important role in recent public-key cryptography. Many cryptographic systems and protocols have been proposed using pairings since the identity-based encryption scheme [2], the short signature scheme [3], and the one-round three-way key exchange protocol [10].

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements where p is a prime and E an elliptic curve over $\mathbb{F}_q$. For a large prime r dividing $\#E(\mathbb{F}_q)$, let k be the embedding degree of $E(\mathbb{F}_q)$, which is the smallest positive integer such that r divides $q^k - 1$. Let G_1 and G_2 be two subgroups of $E(\mathbb{F}_{q^k})$ and μ_r the set of r-th roots of unity in $\mathbb{F}_{q^k}^*$. Then a pairing is a bilinear map $e : G_1 \times G_2 \to \mu_r$.

The most widely used pairing is the Tate pairing $t : E(\mathbb{F}_q)[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r$. If $E(\mathbb{F}_{q^k})$ does not contain any points of order r^2, both $E(\mathbb{F}_q)[r]$ and $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$ are identified with the direct sum of 1- and q-eigenspaces $\mathbb{G}_1$ and $\mathbb{G}_2$ of the Frobenius endomorphism π_q. Then simplifying the domain of the Tate pairing to $\mathbb{G}_1 \times \mathbb{G}_2$ or $\mathbb{G}_2 \times \mathbb{G}_1$ and raising it to a power, there have been numerous proposals on variants of the simplified Tate pairing [9, 17, 12, 16, 8].

The security of pairing-based cryptosystems relies on the hardness to solve the DLP on μ_r, ECDLP on G_1 and G_2, and the pairing inversion problem. All the pairing computation is composed of the Miller step which evaluates the Miller function f at two rational points P and Q (or divisors) on the elliptic curve and the final exponentiation step which raises the result value $f(P,Q)$ of the Miller step to some power d. Thus the natural strategy to solve the pairing inversion problem consists of two steps: 1) inverting the final exponentiation step which computes the d-th root $y \in \mathbb{F}_{q^k}^*$ for an element $z \in \mu_r$ and 2) finding points P and Q satisfying $f(P,Q) = y$. We call them the *Exponentiation Inversion (EI)* problem and the *Miller Inversion (MI)* problem, respectively.

In this paper we focus our concern to the *Fixed Argument Pairing Inversion (FAPI)* problem. It asks to find an unknown point when the first or the second argument of pairings are fixed to some point, called FAPI-1 and FAPI-2, respectively. We first discuss EI. Recently considering FAPI on the Ate_i pairing [11], Kanayama and Okamoto formulated EI and mentioned that it is difficult in general.

In Section 3 we point out the describe EI in [11] is somewhat vague to explain the hardness of the problem. Indeed it is generally hard to find a d-th root in a group if d is a divisor of the order of group. However the situation in EI is different from the general case. For example in the Tate pairing the final exponentiation step raises the evaluation of Miller function to a power $\frac{q^k-1}{r}$. We show that one can find a $\frac{q^k-1}{r}$-th root in polynomial time from the fact that $(\frac{q^k-1}{r}, r) = 1$. And we point out the crucial hardness is to find a root which intersects with the image space of the Miller function on the prescribed domain for given pairings, and hence clarify the description of EI.

In Section 4 we investigate the relationship between FAPI of the Tate pairing defined on the extended domain and the Ate pairing including other variants. If two pairings are defined on the same domain, *i.e.*, $\mathbb{G}_1 \times \mathbb{G}_2$ or vice versa, the equivalence is trivial. However as studied in [6], if we consider the Tate pairing with extended domain $t : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q_k}) \to \mu_r$, bottlenecks to invert two pairings are different. In the case of the Tate pairing with larger domain since taking a random $\frac{q^k-1}{r}$-th root is enough, it is easy to solve EI, while hard to invert the Miller function due to its high degree. And the situation becomes reverse in the case of the Ate pairing.

We show that FAPI of the Tate pairing with the extended domain is computationally equivalent to that of the Ate pairing (including other variants). The result implies even if the domain is changed, the total hardness of FAPI is invariant. It is very interesting because it is commonly believed that the structure of the Ate pairing is so simple and good (that is, the Miller length is short, the solution domain is small and has an algebraic structure induced from the Frobenius map) that it may leak some information and hence there would be a chance for attackers to find further approach to solve FAPI for the Ate pairing, differently from the Tate pairing.

Notation. Throughout the paper, for integers a, b, and i, we use the notation $a^i||b$ if $a^i|b$, but $a^{i+1} \nmid b$.

2 Preliminaries

2.1 The Tate Pairing

Let $\mathbb{F}_q$ be a finite field with $q = p^m$ elements where p is a prime, and let E be an elliptic curve over $\mathbb{F}_q$. Consider a large prime r dividing $\#E(\mathbb{F}_q)$. Throughout we assume $r||\#E(\mathbb{F}_q)$. Let k be the embedding degree of $E(\mathbb{F}_q)$, *i.e.*, $r \mid \Phi_k(q)$ where $\Phi_k(x) \in \mathbb{Z}[x]$ is the k-th cyclotomic polynomial. In this case, $E[r]$ is contained in $E(\mathbb{F}_{q^k})$, where $E[r]$ is the set of r-torsion points and isomorphic to $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$ if $\gcd(r, q) = 1$.

We define $f_{s,Q}$ to be a *normalized* $\mathbb{F}_{q^k}$-rational function with divisor $(f_{s,Q}) = s(Q) - ([s]Q) - (s-1)(\mathcal{O})$. For each $m, n \in \mathbb{Z}$, the normalized Miller functions have the following properties [13, 14]. We denote by $l_{R,S}$ the equation of the line through R and S, and by v_R the equation of the vertical line through R.

D1. $f_{a+b,Q} = f_{a,Q} \cdot f_{b,Q} \cdot \frac{l_{[a]Q,[b]Q}}{v_{[a+b]Q}}$
D2. $f_{ab,Q} = f_{b,Q}^a \cdot f_{a,[b]Q}$
D3. $f_{-a,Q}^{-1} = f_{a,Q} \cdot v_{[a]Q}$

The Tate pairing is defined as follows:

$$t : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k}) \to \mu_r \subset \mathbb{F}_{q^k}, \quad t(P, Q) \mapsto f_{r,P}(Q)^{(q^k-1)/r},$$

where μ_r is the set of r torsion elements in $\mathbb{F}_{q^k}^*$. The Miller length of the Tate pairing is $\log r$.

If we do not consider nondegeneracy property of pairings, the second argument of the above Tate pairing is extended to the lager set $E(\mathbb{F}_{q^k})$. Throughout we consider the Tate pairing on extended domain since it is more convenient to deal with the pairing inversion problem.

2.2 Variants of the Tate pairing

Denote by π_q the Frobenius endomorphism $\pi_q : E \to E$; $(x, y) \mapsto (x^q, y^q)$, and define two eigenspaces of π_q to be $\mathbb{G}_1$ and $\mathbb{G}_2$, *i.e.*,

$$\mathbb{G}_1 = E[r] \cap \ker(\pi_q - [1]) = E(\mathbb{F}_q)[r], \quad \mathbb{G}_2 = E[r] \cap \ker(\pi_q - [q]).$$

More efficient pairings over $\mathbb{G}_2 \times \mathbb{G}_1$ have been extensively studied such as the Ate pairing [9], Ate$_i$ pairing [17], R-ate pairing [12], optimal pairings [16, 8], and so on. One of the basic tool is the following lemma.

Lemma 1. *[9, Theorem 1] Let $\lambda \equiv q \bmod r$ and $m = (\lambda^k - 1)/r$, then the reduced Ate pairing*

$$a_\lambda : \mathbb{G}_2 \times \mathbb{G}_1; \quad (Q, P) \mapsto f_{\lambda,Q}(P)^{(q^k-1)/r},$$

defines a bilinear pairing which is non-degenerate for $r \nmid m$ (i.e. $r^2 \nmid \lambda^k - 1$). Further it satisfies $a_\lambda = t(Q, P)^{m(\lambda-q)/(\lambda^k-q^k)}$.

As the case of the Ate pairing, all the variants of the Tate pairing can be obtained by raising the Tate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ (or vice versa) to appropriate power. Further, Vercauteren introduced an optimal pairing [16], whose Miller length is very short.

Lemma 2. *[16, Theorem 4] Let $r \nmid m$ and write $mr = \sum_{i=0}^{\ell} c_i q^i$ and $s_i = \sum_{j=i}^{\ell} c_j q^j$ then*

$$a_{[c_0,\ldots,c_\ell]} : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r; \quad (Q,P) \mapsto \left(\prod_{i=0}^{\ell} f_{c_i,Q}^{q^i}(P) \cdot \prod_{i=0}^{\ell} \frac{l_{[s_{i+1}]Q,[c_i q^i]Q}(P)}{v_{[s_i]Q}(P)} \right)^{(q^k-1)/r}.$$

Furthermore, it is non-degenerate if $m \cdot \frac{d}{dq} q^k \not\equiv \frac{(q^k-1)}{r} \cdot \frac{d}{dq}(\sum_{i=0}^{\ell} c_i q^i) \bmod r$.

In a parallel computing model, the Miller length of the above pairing is $\log \max_i\{|c_i|\}$. Vercauteren gives a method to obtain small c_i using lattice basis reduction algorithm. In brief consider the following $\phi(k)$-dimensional lattice L spanned by rows of

$$L := \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ -q & 1 & 0 & \cdots & 0 \\ -q^2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & & \\ -q^{\phi(k)-1} & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Then $(c_0, \ldots, c_\ell)$ belongs to L and by Minkowski's theorem there exists a short vector V in L with $||V||_\infty \leq r^{1/\phi(k)}$. Thus the Miller length can be reduced to $\log r/\phi(k)$.

2.3 Pairing Inversion Problems

The problems of our interests are formulated as follows :

Definition 1 ([6]). *For subgroups G_1 and G_2 of $E(\mathbb{F}_{q^k})$, let $e : G_1 \times G_2 \to \mu_r \subset \mathbb{F}_{q^k}^*$ be a well-defined, bilinear pairing.*
The **Fixed Argument Pairing Inversion 1 (FAPI-1)** *problem: given a pairing e, $P_1 \in G_1$, and $z \in \mu_r$, find $P_2 \in G_2$ such that $e(P_1, P_2) = z$.*
The **Fixed Argument Pairing Inversion 2 (FAPI-2)** *problem: given a pairing e, $P_2 \in G_2$, and $z \in \mu_r$, find $P_1 \in G_1$ such that $e(P_1, P_2) = z$.*
The **Generalized Pairing Inversion (GPI)** *problem: given a pairing e and $z \in \mu_r$, find $P_1 \in G_1$ and $P_2 \in G_2$ such that $e(P_1, P_2) = z$.*

A pairing is computed by $e(P_1, P_2) = f_{s,P_1}(P_2)^d$ for some integer s and d, where f_{s,P_1} is a normalized $\mathbb{F}_{q^k}$-rational function with divisor $(f_{s,P_1}) = s(P_1) - ([s]P_1) - (s-1)(\mathcal{O})$. Thus a natural way to solve FAPI for a pairing $e(P_1, P_2) = z$ is performed via two steps, *i.e.*, computing a d-th root y of z and then find a point P_2 (or P_1) satisfying the equation $f_{r,P_1}(\cdot) = y$ (or $f_{r,\cdot}(P_2) = y$) when P_1 (or P_2) is fixed. The first and second step are called the *Exponentiation inversion(EI)* problem and the *Miller Inversion (MI)* problem, respectively.

3 Exponentiation Inversion

In this section we consider EI. Dealing with the pairing inversion problem of Ate_i, Kanayama and Okamoto presented the definition for this problem in [11] and mentioned that it is hard in general.

Through this section we explain that the described EI is not hard. We point out where the hardness to invert the final exponentiation step arises concretely and clarify the description of EI.

3.1 The d-th Root Extraction

In [11, Definition 3] Kanayama and Okamoto defined EI as follows:

Definition 2. *[11, Definition 3] For an unknown element $y \in \mathbb{F}_{q^k}^*$, assume that an integer d and the value of $z := y^d \in \mathbb{F}_{q^k}^*$ are known. Then, the EI, or (d, z)-EI, is the problem of finding y from the instance (d, z).*

They mentioned that the above is generally hard. However the description is insufficient to give an explanation for the hardness of EI for relevant parings precisely. In fact one can find a d-th root y in polynomial time for most pairing friendly curves. The follwing lemma is well-known, but we give a proof for the convenience of readers.

Theorem 1. *Let d be the integer such that $d|(q^k - 1)$ and $(d, (q^k - 1)/d) = 1$. Then given $z \in (\mathbb{F}_{q^k}^*)^d$, there exists an algorithm to find a root $y \in \mathbb{F}_{q^k}^*$ of the equation $y^d = z$ in $O(k^3 \log^3 q)$-bit operations.*

Proof. Since $(d, (q^k-1)/d) = 1$, there exist integers a and b such that $a \cdot d - b \cdot (q^k-1)/d = 1$. Then from

$$(z^a)^d = z^{1+b(q^k-1)/d} = z \cdot z^{b(q^k-1)/d} = z \cdot (y^d)^{b(q^k-1)/d} = z,$$

z^a is a d-th root of z. We can compute z^a by executing the extended Euclidean algorithm one time and computing one $\mathbb{F}_{q^k}$-exponentiation. □

Most of pairing friendly curves satisfy $r||q^k - 1$. In this case the exponent $d \left(:= \frac{q^k-1}{r}\right)$ is relatively prime to $\frac{q^k-1}{d} (= r)$. Thus one can find a d-th root of z very efficiently.

Let ζ be a generator of $\mathbb{F}_{q^k}^*$. For a solution y_0 of $y_0^d = z$, $y_0\zeta^{r \cdot i}$ is another solution for each $0 \leq i < d$. A generator ζ of $\mathbb{F}_{q^k}^*$ can be found in $O(k^4 \log^4 q)$- bit operations when the factorization of $q^k - 1$ is known [5]. Thus once one gets a solution y_0 of $y_0^d = z$, one can compute every solution of $y^d = z$, *i.e.*, $\{y_0\zeta^{r \cdot i} : 0 \leq i < d\}$.

We remark that in the case that $d^i|q^k - 1$ for $i > 1$, a d-th root can be computed by means of the Adleman-Manders-Miller altorithm [1] (see also [4, Section 7.3]), which exploits the DLP solver as a subroutine.

3.2 The Hardness of EI

Let us consider the Tate pairing

$$t : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k}) \to \mu_r \subset \mathbb{F}_{q^k}^*; \quad (Q, P) \mapsto f_{r,Q}(P)^{\frac{q^k-1}{r}}.$$

Recall given Q and z, FAPI-1 for the Tate pairing $t(Q, \cdot) = z$ can be done by finding 1) a $\frac{q^k-1}{r}$-th root y of z and then 2) a point $P \in E(\mathbb{F}_{q^k})$ satisfying $f_{r,Q}(P) = y$.

Since there are $\frac{q^k-1}{r}$ candidates for solutions of EI, it seems infeasible to find a proper root. However Galbraith, Hess, and Vercauteren showed that it is enough to work with a random root y, *i.e.*, there exists a point P corresponding to a random root with the high probability [6, Example 18]. Since computing a random $\frac{q^k-1}{r}$ root is easy as discussed previously, FAPI-1 for the Tate pairing is polynomial time reducible to MI. However note

that MI requires to find a root of a higher degree (approximately r) polynomial equation induced from a rational function equation $f_{r,Q}(\cdot) = y$.

For the Ate pairing or other variants of the Tate pairing defined on $\mathbb{G}_2 \times \mathbb{G}_1$, the situation is totally different. As briefly mentioned in [15], taking a random $\frac{q^k-1}{r}$-th root does not help to find a point of $\mathbb{G}_1$ in MI. More precisely these class of pairings can be described as follows:

$$t' : \mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \simeq \mu_r,$$

where the map from $\mathbb{G}_2 \times \mathbb{G}_1$ to $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$ is given by $f_{s,Q}(P)$ for an integer s and the isomorphism is the $\frac{q^k-1}{r}$ power map. Since for a fixed $Q \in \mathbb{G}_2$ the average cardinality of the image set $\{f_{s,Q}(P) : P \in \mathbb{G}_1\}$ is r, the image set forms the set of representatives of the equivalence class $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$. Suppose $P \in \mathbb{G}_1$ is a solution of FAPI-1 for these class of pairings $t'(Q, \cdot) = z$. Then a random $\frac{q^k-1}{r}$-th root of z is of the form $f_{s,Q}(P)\alpha^r$ for a $\alpha \in \mathbb{F}_{q^k}$. And solving the equation $f_{s,Q}(\cdot) = f_{s,Q}(P)\alpha^r$ does not give a point in $\mathbb{G}_1$ in general. Therefore it is required to clarify the definition of EI with regard to the prescribed domain so that it reflects the crucial hardness.

Definition 3 (Reformulation of EI). *Let $e : G_1 \times G_2 \to \mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r \simeq \mu_r$ be a pairing over elliptic curves, where the map from $G_1 \times G_2$ to $\mathbb{F}_{q^k}^*/(\mathbb{F}_{q^k}^*)^r$ is given by $f_{s,Q}(P)$ for an integer s and the isomorphism is the d-powering map. Then given $P_1 \in G_1$ and $z \in \mu_r$, the exponentiation inversion (EI) problem is defined to find the value of $\{y \in \mathbb{F}_{q^k} : y^d = z\} \cap \{f_{s,P_1}(P_2) \in \mathbb{F}_{q^k} : P_2 \in G_2\}$. EI for the fixed second argument is defined analogously.*

In the case of the Tate pairing on $E(\mathbb{F}_q^k)[r] \times E(\mathbb{F}_{q^k})$, the cardinality of the set $\{y \in \mathbb{F}_{q^k} : y^d = z\} \cap \{f_{s,P_1}(P_2) \in \mathbb{F}_{q^k} : P_2 \in G_2\}$ is approximately d. And the value is approximately 1 in the case of its variants on $\mathbb{G}_2 \times \mathbb{G}_1$, which implies that EI for pairings on small domain is hard. Once one solves EI for the variants of the Tate pairing, MI is easier than that of the Tate pairing since the value s can be reduced to $r^{1/\phi(k)}$ [16]. Thus naturally one can expect that the hardness of MI and that of EI are complementary, hence the hardness of the Tate pairing on larger domain and its variants on smaller domain is invariant. We discuss it precisely in the next section.

4 Equivalence of FAPI for the Tate and the Ate Pairings

In this section we investigate the relationship between FAPI of the Tate pairing $t : E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k}) \to \mu_r$ and the Ate pairing. Note that the Ate pairing and other variants can be computed as $\tilde{t} := t^\kappa$ for some integer κ with $r \nmid \kappa$ whose domain is restricted to $\mathbb{G}_2 \times \mathbb{G}_1$. If the domain of the Tate pairing is restricted to $\mathbb{G}_2 \times \mathbb{G}_1$, the equivalence of FAPI among these pairings is trivial. However if the domain of the first argument for the Tate pairing are extended to $E(\mathbb{F}_{q^k})[r]$ (or the second argument to $E(\mathbb{F}_{q^k})$), which is the original space, then the relationship of FAPI between them does not seem obvious any more.

Note that if $E(\mathbb{F}_{q^k})$ has no point of order r^2, $E(\mathbb{F}_{q^k})[r]$ is the set of representatives of $E(\mathbb{F}_{q^k})/rE(\mathbb{F}_{q^k})$. Thus for every $R \in E(\mathbb{F}_{q^k})$, R is written as a sum of some $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, and the r-multiple of $P' \in E(\mathbb{F}_{q^k})$, *i.e.*, $R = P + Q + rP'$. And since $E(\mathbb{F}_{q^k})[r] =$

$\mathbb{G}_1 \oplus \mathbb{G}_2$, every $S \in E(\mathbb{F}_{q^k})[r]$ is written as a sum of some $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. The following lemma is well-known.

Lemma 3. *Let E be an ordinary elliptic curve over F_q, r a prime such that $r|\#E(\mathbb{F}_{q^k})$ and $r \nmid q-1$. Then the maps $t : \mathbb{G}_i \times \mathbb{G}_i \to \mu_r$ for $i = 1$ and 2 are both trivial.*

Now we are in a position to show that the computational equivalence between FAPI for the Tate pairing on a larger domain and the Ate pairing on a smaller domain. Note that a solution of FAPI for the Tate pairing does not belong to the domain of the Ate pairing. Thus it is required to extract a proper point from this intermediate solution.

Theorem 2. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$, r a prime such that $r|\#E(\mathbb{F}_{q^k})$ and $r \nmid q-1$. Suppose that $E(\mathbb{F}_{q^k})$ has no point of order r^2. Then FAPI-1 for the Tate pairing $t : \mathbb{G}_2 \times E(\mathbb{F}_{q^k}) \to \mu_r$ is computationally equivalent to that of the Ate pairing including its variants $\tilde{t} := t^\kappa : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$.*

Proof. Let $z \in \mu_r$ and $Q \in \mathbb{G}_2$ be instances of FAPI-1. Let Σ_t and $\Sigma_{\tilde{t}}$ be oracles of FAPI-1 for t on $\mathbb{G}_2 \times E(\mathbb{F}_{q^k})$ and $\tilde{t}$ on $\mathbb{G}_2 \times \mathbb{G}_1$, respectively. That is, on inputs $z \in \mu_r$ and $Q \in \mathbb{G}_2$, Σ_t and $\Sigma_{\tilde{t}}$ output $P_t \in E(\mathbb{F}_{q^k})$ and $P_{\tilde{t}} \in G_1$ satisfying $t(Q, P_t) = z$ and $\tilde{t}(Q, P_{\tilde{t}}) = z$, respectively.

It is easy to see that FAPI-1 for $\tilde{t}$ on $\mathbb{G}_2 \times \mathbb{G}_1$ implies FAPI-1 for t on $\mathbb{G}_2 \times E(\mathbb{F}_{q^k})$. Taking input (z, Q) to $\Sigma_{\tilde{t}}$ we have $P_{\tilde{t}} \in G_1 \subset E(\mathbb{F}_{q^k})$. Since $t(\cdot,\cdot)^\kappa = \tilde{t}(\cdot,\cdot)$ on $\mathbb{G}_2 \times \mathbb{G}_1$, we have

$$t(Q, \kappa P_{\tilde{t}}) = t(Q, P_{\tilde{t}})^\kappa = \tilde{t}(Q, P_{\tilde{t}}) = z.$$

Hence we can solve FAPI-1 for t on $\mathbb{G}_2 \times E(\mathbb{F}_{q^k})$ by one call of $\Sigma_{\tilde{t}}$.

Conversely, on input (z, Q), suppose Σ_t outputs P_t such that $t(Q, P_t) = z$. Then since $E(\mathbb{F}_{q^k})$ has no point of order r^2,

$$P_t = Q_1 + P + rP' \tag{1}$$

for some $Q_1 \in \mathbb{G}_2$, $P \in \mathbb{G}_1$, and $P' \in E(\mathbb{F}_{q^k})$.

Firstly we claim that $(\kappa^{-1} \bmod r)\cdot P$ is the desired point, *i.e.*, $\tilde{t}(Q, (\kappa^{-1} \bmod r)\cdot P) = z$. This can be verified as follows:

$$\begin{aligned} z^\kappa &= t(Q, Q_1 + P + rP')^\kappa \\ &= t(Q, Q_1)^\kappa \cdot t(Q, P)^\kappa \cdot t(Q, P')^{r\kappa} \\ &= t(Q, Q_1)^\kappa \cdot t(Q, P)^\kappa \\ &= t(Q, Q_1)^\kappa \cdot \tilde{t}(Q, P) \\ &= \tilde{t}(Q, P), \end{aligned}$$

where the last equality comes from Lemma 3.

Now it suffices to extract P from P_t. From $r \nmid q-1$, $r^\delta || \#E(\mathbb{F}_{q^k})$ for some integer $\delta \geq 2$. (In fact, $\delta = 2$ since $E(\mathbb{F}_{q^k})$ is of rank at most 2 and has no point of order r^2.) Then taking $\#E(\mathbb{F}_{q^k})/r^\delta$-multiple to both sides of (1), we have

$$\#E(\mathbb{F}_{q^k})/r^\delta \cdot P_t = \#E(\mathbb{F}_{q^k})/r^\delta \cdot Q_1 + \#E(\mathbb{F}_{q^k})/r^\delta \cdot P + E(\mathbb{F}_{q^k})/r^{\delta-1} \cdot P'.$$

Note that if $E(\mathbb{F}_{q^k})/r^{\delta-1} \cdot P' \neq \mathcal{O}$, r^2 should divide the order of P', which contradicts that $E(\mathbb{F}_{q^k})$ has no point of order r^2. Thus the above equation becomes

$$\#E(\mathbb{F}_{q^k})/r^\delta \cdot P_t = \#E(\mathbb{F}_{q^k})/r^\delta \cdot Q_1 + \#E(\mathbb{F}_{q^k})/r^\delta \cdot P \tag{2}$$

Next we extract the point $\#E(\mathbb{F}_{q^k})/r^\delta \cdot P$ out of (2). The technique is followed from the previous work by Galbraith and Verheul [7, Proposition 1]: taking the q-th power Frobenius map to both sides of (2), we have

$$\#E(\mathbb{F}_{q^k})/r^\delta \cdot \pi_q(P_t) = q \cdot \#E(\mathbb{F}_{q^k})/r^\delta \cdot Q_1 + \#E(\mathbb{F}_{q^k})/r^\delta \cdot P$$

and hence together with (2)

$$(q-1) \cdot \#E(\mathbb{F}_{q^k})/r^\delta \cdot P = \#E(\mathbb{F}_{q^k})/r^\delta \cdot (qP_t - \pi_q(P_t)).$$

Since $(r^\delta, q-1) = 1$, the extended Euclidean algorithm yields two integers α and α' such that $\alpha \cdot (q-1) - \alpha' \cdot r^\delta = 1$. Then

$$\begin{aligned}\#E(\mathbb{F}_{q^k})/r^\delta \cdot P &= (1 + \alpha' r^\delta) \cdot \#E(\mathbb{F}_{q^k})/r^\delta \cdot P \\ &= \alpha(q-1) \cdot \#E(\mathbb{F}_{q^k})/r^\delta \cdot P \\ &= \alpha \cdot \#E(\mathbb{F}_{q^k})/r^\delta \cdot (qP_t - \pi_q(P_t)).\end{aligned}$$

Also since $(\#E(\mathbb{F}_{q^k})/r^\delta, r) = 1$, there exist two integers β and β' such that $\beta \cdot \#E(\mathbb{F}_{q^k})/r^\delta - \beta' \cdot r = 1$. Hence we have

$$\begin{aligned}P &= (1 + \beta' r) \cdot P \\ &= \beta \cdot \#E(\mathbb{F}_{q^k})/r^\delta \cdot P \\ &= \alpha \cdot \beta \cdot \#E(\mathbb{F}_{q^k})/r^\delta \cdot (qP_t - \pi_q(P_t)).\end{aligned}$$

□

Theorem 3. *Let E be an ordinary elliptic curve over $\mathbb{F}_q$, r a prime such that $r|\#E(\mathbb{F}_{q^k})$ and $r \nmid q-1$. Suppose that $E(\mathbb{F}_{q^k})$ has no point of order r^2. Then FAPI-2 for the Tate pairing $t : E(\mathbb{F}_{q^k})[r] \times \mathbb{G}_1 \to \mu_r$ is computationally equivalent to the of the Ate pairing including its variants $\tilde{t} := t^\kappa : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$.*

Proof. Let $z \in \mu_r$ and $P \in \mathbb{G}_1$ be instances of FAPI-2. Let Σ_t and $\Sigma_{\tilde{t}}$ be oracles of FAPI-2 for t on $E(\mathbb{F}_{q^k})[r] \times \mathbb{G}_1$ and $\tilde{t}$ on $\mathbb{G}_2 \times \mathbb{G}_1$, respectively. That is, on inputs $z \in \mu_r$ and $P \in \mathbb{G}_1$, Σ_t and $\Sigma_{\tilde{t}}$ output $Q_t \in E(\mathbb{F}_{q^k})[r]$ and $Q_{\tilde{t}} \in G_2$ satisfying $t(Q_t, P) = z$ and $\tilde{t}(Q_{\tilde{t}}, P) = z$, respectively.

Taking input (z, P) to $\Sigma_{\tilde{t}}$ we have $Q_{\tilde{t}} \in G_2 \subset E(\mathbb{F}_{q^k})[r]$. Since $t(\cdot,\cdot)^\kappa = \tilde{t}(\cdot,\cdot)$ on $\mathbb{G}_2 \times \mathbb{G}_1$, we have

$$t(\kappa Q_{\tilde{t}}, P) = t(Q_{\tilde{t}}, P)^\kappa = \tilde{t}(Q_{\tilde{t}}, P) = z.$$

Hence we can solve FAPI-2 for the Tate pairing on $E(\mathbb{F}_{q^k})[r] \times \mathbb{G}_1$ by one call of $\Sigma_{\tilde{t}}$.

Conversely, suppose, on input (z, P), Σ_t outputs Q_t such that $t(Q_t, P) = z$. Then since $E(\mathbb{F}_{q^k})[r] = \mathbb{G}_1 \oplus \mathbb{G}_2$, we have

$$Q_t = P' + Q \tag{3}$$

for some $P' \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. Then from

$$\begin{aligned} z^\kappa &= t(P'+Q,P)^\kappa \\ &= t(P',P)^\kappa \cdot t(Q,P)^\kappa \\ &= t(P',P)^\kappa \cdot \tilde{t}(Q,P) \\ &= \tilde{t}(Q,P), \end{aligned}$$

where the last equality comes from Lemma 3, $(\kappa^{-1} \bmod r) \cdot Q$ is the desired point.

Now as presented in [7, Proposition 1], one can extract Q from Q_t as follows: taking q-th power Frobenius map to both sides of (3) yields the equation

$$\pi_q(Q_t) = P' + q \cdot Q.$$

Working the above equation together with (3), we have

$$(q-1) \cdot Q = (Q_t - \pi_q(Q_t)).$$

Since $(r, q-1) = 1$, the extended Euclidean algorithm yields two integers α and α' such that $\alpha \cdot (q-1) - \alpha' \cdot r = 1$. Therefore

$$Q = (1 + \alpha' r) \cdot Q = \alpha(q-1) \cdot Q = \alpha(Q_t - \pi_q(Q_t)).$$

□

Thus inverting the Ate pairing (including other variants of the Tate pairing) defined on the smaller domain is neither easier nor harder than inverting the Tate pairing defined on the lager domain. If MI gets easier (harder) with reduced (extended) domain, EI gets harder (easier) to the same extent and vice versa. Therefore the overall hardness is invariant.

5 Conclusion

In this paper we have reformulated the definition of EI given by Kanayama and Okamoto. We pointed out that a random $\frac{q^k-1}{r}$-th root can be computed easily given $z \in \mu_r$ and anlayzed the crucial hardness to invert the final exponentiation step in pairings.

We have also investigated the relationship between the inversion of the Tate pairing defined on $E(\mathbb{F}_{q^k})[r] \times E(\mathbb{F}_{q^k})$ and the Ate pairing on $\mathbb{G}_2 \times \mathbb{G}_1$ and shown that FAPI for the pairings are computationally equivalent. It implies that the hardness of MI and that of EI are complementary in the pairing inversion problem.

However we stress that we currently do not know the precise hardness of FAPI. To the best of our knowledge, there is no known practical attack on FAPI. It is still worth investigating the security of the pairing inversion problem for the Ate or its optimized versions, focusing on the nice algebraic structure they exploit.

References

1. L. M. Adleman, K. Manders, and G. Miller, "On taking Roots in Finite Field," in *Proc. of 18th IEEE Symposium on Foundations of Computer Science*, pp.175–177.
2. D. Boneh and M. Franklin, "Identity-based Encryption from the Weil Pairing," in *Proc. of CRYTO 2001*, vol. 2139, Lecture Notes on Computer Science, pp.213–229, 2001
3. D. Boneh, X. Boyen, and H. Shacham, "Short Group Signatures," in *Proc. of CRYTO 2004*, vol. 3152, Lecture Notes on Computer Science, pp.41–55, 2004.
4. E. Bach and J. Shallit, *Algorithmic Number Theory, Vol. 1*. MIT Press, 1996.
5. S. Galbraith, "Mathematics of Public Key Cryptography," Cambridge University Press, 2012. Available: `http://www.math.auckland.ac.nz/~sgal018/crypto-book/crypto-book.html`.
6. S. Galbraith, F. Hess, and F. Vercauteren, "Aspects of Pairing Inversion," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5719–5728, 2008.
7. S. Galbraith and R. Verheul, "An Analysis of the Vector Decomposition Problem," *Proc. of PKC 2008*, vol. 4939, Lecture Notes on Computer Science, pp.308–327, 2008.
8. F. Hess, "Pairing Lattices," in *Proc. of PAIRING 2008*, vol. 5209, Lecture Notes on Computer Science, pp.18–38, 2008.
9. F. Hess, N. Smart, and F. Vercauteren, "The Eta Pairing Revisited," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4595–4602, 2006.
10. A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman," in *Proc. of ANTS 2000*, vol. 1838, Lecture Notes on Computer Science, pp. 385–393, 2000.
11. N. Kanayama and E. Okamoto, "Approach to Pairing Inversions Without Solving Miller Inversion," *IEEE Trans. Inf. Theory*, vol.58, no.2, pp. 1248–1253, 2012.
12. E. Lee, H. Lee, and C. Park, "Efficient and Generalized Pairing Computation on Abelian Varieties," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1793–1803, 2006.
13. V. S. Miller, "Short programs for functions on curves," unpublished manuscript (1986). Available: http://crypto.stanford.edu/miller/miller.pdf.
14. V. S. Miller, "The Weil Pairing and its efficient calculation," *J. Cryptol.*, vol. 17, no. 4, pp. 235–261, 2004.
15. F. Vercauteren, "The Hidden Root Problem," in *Proc. of PAIRING 2008*, vol. 5209, Lecture Notes on Computer Science, pp.89–99, 2008.
16. F. Vercauteren, "Optimal Pairing," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 455–461, 2010.
17. C. Zhao , F. Zhang, and J. Huang "A note on the Ate pairing", *Int. J. Inf. Security*, vol. 6, no. 7, pp.379–382, 2008.