Pairing Inversion via Non-degenerate Auxiliary Pairings

Seunghwan Chang[1], Hoon Hong[2], Eunjeong Lee[1], and Hyang-Sook Lee[3]

[1] Institute of Mathematical Sciences, Ewha Womans University, Seoul, S. Korea
schang@ewha.ac.kr, ejlee127@ewha.ac.kr
[2] Department of Mathematics, North Carolina State University, Raleigh, USA
hong@ncsu.edu
[3] Department of Mathematics, Ewha Womans University, Seoul, S. Korea
hsl@ewha.ac.kr

Abstract. The security of pairing-based cryptosystems is closely related to the difficulty of the pairing inversion problem(PI). In this paper, we discuss the difficulty of pairing inversion on the generalized ate pairings of Vercauteren. First, we provide a simpler approach for PI by generalizing and simplifying Kanayama-Okamotos approach; our approach involves modifications of exponentiation inversion(EI) and Miller inversion(MI), via an auxiliary pairing. Then we provide a complexity of the modified MI, showing that the complexity depends on the sum-norm of the integer vector defining the auxiliary pairing. Next, we observe that *degenerate* auxiliary pairings expect to make modified EI harder. We provide a sufficient condition on the integer vector, in terms of its max norm, so that the corresponding auxiliary paring is *non*-degenerate. Finally, we define an infinite set of curve parameters, which includes those of typical pairing friendly curves, and we show that, within those parameters, PI of arbitrarily given generalized ate pairing can be reduced to modified EI in polynomial time.

1 Introduction

Pairings [1, 9, 12, 13, 18, 25, 29] play an important role in cryptography [2–4, 14, 27]. The security of pairing-based cryptosystems is closely related to the difficulty of the pairing inversion problem (PI): for a given pairing $\langle \cdot, \cdot \rangle$, an argument Q(or P) and a pairing value z, compute the other argument P(or Q) such that $z = \langle P, Q \rangle$.

PI on elliptic curves was first recognized by Verheul [26] as a potentially hard cryptographic computational problem. Satoh [23, 24] considered the polynomial interpolations to find the x-coordinate of P for given Q and z, providing evidences that support the difficulty of PI. Galbraith-Hess-Vercauteren [11] defined PI formally and discussed two approaches for PI. (1) Try to solve PI in a single step. (2) Solve PI by inverting exponentiation first and then inverting Miller step - Since pairings on elliptic curves are computed in two steps, namely the Miller step and the exponentiation step, they suggested inverting them in reverse order to solve PI, i.e. exponentiation inversion(EI) and then Miller inversion (MI).

They discussed the possibilities on the reduction of MI to PI (precisely FAPI-1) vice versa for Tate-Lichtenbaum pairing after the observation that the EI for Tate-Lichtenbaum pairing can be defined as returning a random value satisfying its exponentiation relation, which is very easy. They remarked that the situation, of EI, is quite different for the ate pairing. Recently, [17] showed that, when a preimage of Tate-Lichtenbaum pairing was restricted, its PI was equivalent to the PI of the ate pairing. Kanayama-Okamoto [15] studied the PI on the ate$_i$ pairings and suggested a clever idea for a reduction of PI to EI.

In this paper, inspired by significant previous works [26, 22–24, 11, 20, 28, 15, 7], we provide further contributions toward understanding the difficulty of pairing inversion. In order to provide the context and the motivation for the main contributions of this paper, we first review informally some of the previous works particular [11, 15] on PI by recasting them for the generalized ate pairing of Vercauteren [25], which currently is one of the most general constructions of cryptographic pairings.

For a given integer vector ε, the generalized ate pairing $a_\varepsilon : G_2 \times G_1 \to G_3$ takes two points $P \in G_1, Q \in G_2$ and produces a value z. It is carried out in two steps: Miller step (M) [19] and Exponentiation step (E).

1. $[\mathsf{M}_\varepsilon]$ $\gamma_\varepsilon = Z_\varepsilon\,(Q, P)$
2. $[\mathsf{E}_\varepsilon]$ $z = \gamma_\varepsilon^L$

where Z_ε is a certain rational function depending on the integer vector ε and L is a certain natural number. Depending on the choice of ε, one gets a different pairing (see [25] and Section 2.2 for details).

Pairing inversion problems are defined in two types [11]. In this paper, we consider one of them (FAPI-1): for given $Q \in G_2$, $z \in G_3$, find P such that $z = a_\varepsilon(Q, P)$. Following [11, 15], we consider the two-step approach i.e., first inverting the exponentiation step (EI) and then inverting the Miller step (MI).

For the generalized ate pairings, there is a *subtlety* in the formulation of EI, as observed for example in [17], due to the fact that, for a fixed Q, the map $a_\varepsilon(Q, \cdot) : G_1 \to G_3$ is one-to-one, unlike for Tate-Lichtenbaum pairing. One could think of three possible formulations of EI. For a given L and z, find

F1: any γ such that $z = \gamma^L$. (γ might not be γ_ε)
F2: all γ's such that $z = \gamma^L$. (one of them will be γ_ε)
F3: the "right" γ such that $z = \gamma^L$. ($\gamma = \gamma_\varepsilon$)

In [15], it is *not* stated explicitly which formulation of EI is intended. From the context, we conclude that it cannot be F1. If it were F1, then we get into a strange conclusion that PI could be solvable in polynomial time since F1 is obviously solvable in polynomial time (due to fact that L is relatively prime to the order of z) and [15] showed that PI can be reduced to EI. We also conclude that it cannot be F2 either. If it were F2, then one would have to carry out MI for each of the exponentially many γ's, contradicting the claim of [15] that PI can be reduced to EI in polynomial time. Hence, the only formulation of EI which is consistent with the claim of [15] is F3. Therefore, we will use F3 as the formulation of EI. Summarizing, we have the following formulation of PI :

1. $[\mathsf{EI}_{\varepsilon}]$ Find the "right" γ_{ε} from the set $\{\gamma : z = \gamma^L\}$
2. $[\mathsf{MI}_{\varepsilon}]$ Find P from $\gamma_{\varepsilon} = Z_{\varepsilon}(Q, P)$

In [15], Kanayama-Okamoto proposed an interesting modification of the natural approach for PI, which amounts to the following:

1. [Choice] Choose an integer vector e (which might be different from ε), giving rise to another generalized ate pairing, which we will call *an auxiliary pairing*, which may or may not be non-degenerate.
2. $[\mathsf{EI}_{\varepsilon,e}]$ Find the "right" γ_e by carrying out several "related" exponentiation inversions (See Section 2.3).
3. $[\mathsf{MI}_e]$ Find P from $\gamma_e = Z_e(Q, P)$

From now on, we will call $\mathsf{EI}_{\varepsilon,e}$ and MI_e as the *modified* exponentiation inversion and the *modified* Miller inversion, respectively. If $e = \varepsilon$, then $\mathsf{EI}_{\varepsilon,e}$ and MI_e are exactly same as $\mathsf{EI}_{\varepsilon}$ and $\mathsf{MI}_{\varepsilon}$. The key idea is to choose an integer vector e which may be different from ε, but which may be better for PI. Specifically, Kanayama-Okamoto suggested that the integer vector e is chosen from either coefficients of cyclotomic polynomials or $(1, \ldots, 1)$, because such e yields Z_e of low degree, making MI_e easy.

This concludes the informal review of the previous works on PI (recast for the generalized ate pairing). Finally we are ready to describe informally the main contributions of this paper.

1. In Section 3, we provide another approach for pairing inversion (Approach 1), by simplifying the step $\mathsf{EI}_{\varepsilon,e}$ of Kanayama-Okamoto's approach. The simplicity of the proposed approach significantly facilitates the subsequent investigation. We prove its correctness (Theorem 1), and then compare the two approaches with respect to the search spaces(Theorem 2).
2. In Section 4, we provide a complexity analysis of MI_e (Theorem 3). It essentially says that the complexity is bounded by $||e||_1^2$ where $||e||_1$ stands for the sum norm of the chosen integer vector e. Hence, in order to reduce the complexity of MI_e, one needs to choose e with small sum norm.
3. In Section 5, we provide an incremental result toward the understanding of the complexity of $\mathsf{EI}_{\varepsilon,e}$. We begin by observing that the degeneracy of the auxiliary pairing has a potential impact on the difficulty of $\mathsf{EI}_{\varepsilon,e}$ (Proposition 1 and Remark 2). More precisely, if the auxiliary paring defined by the choice of e is degenerate, then the exponential relation in $\mathsf{EI}_{\varepsilon,e}$ step becomes independent of the input z, that is, the exponential relation does not capture any information about the input. As a result, $\mathsf{EI}_{\varepsilon,e}$ is expected to be harder than $\mathsf{EI}_{\varepsilon}$, when such e is chosen. If the auxiliary pairing corresponding to e is non-degenerate, then $\mathsf{EI}_{\varepsilon,e}$ is likely as hard as $\mathsf{EI}_{\varepsilon}$. Hence, in order to reduce the complexity of $\mathsf{EI}_{\varepsilon,e}$, one better choose e such that the auxiliary paring defined by e is non-degenerate. We provide a sufficient condition on e, in terms of the max norm of e, so that the pairing corresponding to e is non-degenerate (Theorem 4).

4. In Section 6, we discuss when pairing inversion can be reduced to modified exponentiation inversion $\mathsf{EI}_{\varepsilon,e}$. This was inspired by Kanayama-Okamoto [15] where pairing inversion was reduced to several (unmodified) exponentiation inversions. Specifically we are looking for a condition on e so that MI_e is easy. As explained above, we need to find *small* e. Thus, one might be naturally tempted to choose the integer vector e from either coefficients of cyclotomic polynomials or $(1, \ldots, 1)$. However such e makes the corresponding auxiliary pairing degenerate. Hence the modified exponentiation inversion $\mathsf{EI}_{\varepsilon,e}$ is expected to be hard. Therefore, in order to meaningfully reduce pairing inversion to modified exponentiation inversion, one needs find e such that it is *small* and the corresponding auxiliary pairing is *non-degenerate*. In this section, we investigate the existence of such e in various cases. In particular, we define an infinite set of curve parameters (Definition 1), which includes those of typical pairing friendly curves as in Table 1 of [10] and show that, within those parameters, pairing inversion of an arbitrarily given pairing can be reduced to modified exponentiation inversion in polynomial time (Theorem 5). We furthermore provide tighter upper bounds on the number of bit operations needed by such reductions for several concrete cases (Table 1).

2 Preliminaries

In this section, we briefly review elliptic curves, the generalized ate pairings due to Vercauteren [25] and an approach to pairing inversion due to Kanayama-Okamoto [15]. We encourage all the readers to skim through them, as the notations and the assumptions therein will be extensively used throughout the subsequent sections.

2.1 Elliptic curves

We fix the basic notations for elliptic curves. Let q be a power of a prime and let r be a prime such that $\gcd(q, r) = 1$. Let k be the embedding degree defined as the multiplicative order of q in $\mathbb{F}_r^*$, denoted by $k = \mathrm{ord}_r(q)$, and $L = (q^k - 1)/r$. Let E be an elliptic curve defined over $\mathbb{F}_q$ such that $r \mid \#E(\mathbb{F}_q)$. Let $G_1 = E[r] \cap \ker(\pi_q - [1])$ and $G_2 = E[r] \cap \ker(\pi_q - [q])$ where $\pi_q : E \to E$ denotes the q-power Frobenius endomorphism.

2.2 Vercauteren's generalized ate pairings

We review the generalized ate pairings [25]. Let $\mu_r = \left\{ u \in \mathbb{F}_{q^k}^{\times} : u^r = 1 \right\}$. Let $f_{n,Q}, l_{P,Q}$ and v_P be the normalized functions with divisors $n(Q) - ([n]Q) - (n-1)(O)$, $(P)+(Q)+(-(P+Q))-3(O)$ and $(P)+(-P)-2(O)$ respectively, where O denotes the identity element of the group E. Let

$$g(X) = X^k - 1, \quad \lambda_\varepsilon(X) = \sum_{j=0}^{k-1} \varepsilon_j X^j, \quad W_\varepsilon(X) = \det \begin{pmatrix} g(X) & \lambda_\varepsilon(X) \\ g'(X) & \lambda'_\varepsilon(X) \end{pmatrix}$$

for $\varepsilon = (\varepsilon_0, \ldots, \varepsilon_{k-1}) \in \mathbb{Z}^k$. Vercauteren [25] defined a map $a_\varepsilon : G_2 \times G_1 \to \mu_r$ such that, for all $P \in G_1, Q \in G_2$,

$$a_\varepsilon(Q,P) = Z_\varepsilon\left(Q,P\right)^L, \quad \text{where}$$
$$Z_\varepsilon\left(Q,P\right) = \prod_{j=0}^{k-1} f_{\varepsilon_j, q^j Q}(P) \prod_{j=0}^{k-2} \frac{l_{\varepsilon_j q^j Q,\ (\varepsilon_{j+1} q^{j+1} + \cdots + \varepsilon_{k-1} q^{k-1})Q}(P)}{v_{(\varepsilon_j q^j + \cdots + \varepsilon_{k-1} q^{k-1})Q}}$$

and showed that it is a well-defined bilinear map if $r \mid \lambda_\varepsilon\left(q\right)$, $r^2 \nmid \lambda_\varepsilon(q)$ and $r^2 \nmid g\left(q\right)$. He also showed that a_ε is non-degenerate if and only if $r^2 \nmid W_\varepsilon(q)$.

From now on, we will assume $r \mid \lambda_\varepsilon\left(q\right)$, $r^2 \nmid \lambda_\varepsilon(q)$, $r^2 \nmid g\left(q\right)$ and $r^2 \nmid W_\varepsilon(q)$, so that a_ε is a non-degenerate pairing. We will also assume, without losing generality, that $\gcd\left(\varepsilon_0, \ldots, \varepsilon_{k-1}\right) = 1$ because the vector ε is selected as small as possible for faster pairing computation. In summary, Vercauteren proposed the following approach for pairings.

In: $P \in G_1, Q \in G_2$
Out: $z = a_\varepsilon(Q,P)$

1. $[\mathsf{M}_\varepsilon]$ $\gamma_\varepsilon \leftarrow Z_\epsilon\left(P,Q\right)$
2. $[\mathsf{E}_\varepsilon]$ $z \leftarrow \gamma_\epsilon^L$

2.3 Kanayama-Okamoto's approach to pairing inversion

We review an approach for pairing inversion due to Kanayama-Okamoto [15]. They proposed the following approach and proved its correctness.

In: $Q \in G_2$, $z \in \mu_r$
Out: $P \in G_1$ such that $z = a_\epsilon(Q,P)$.

1. [Choice] Choose $e \in \mathbb{Z}^k$ such that $r \mid \lambda_e(q)$ and $\gcd\left(e_0, \ldots, e_{k-1}\right) = 1$.
2. $[\mathsf{EI}_{\varepsilon,e}]$ Find γ_e by carrying out the following.
   (a) $T_j \leftarrow \mathrm{rem}\left(q^j, r\right)$, the remainder of q^j modulo r
   (b) $a_j \leftarrow \mathrm{ord}_r(T_j)$
   (c) $n_j \leftarrow \frac{T_j^{a_j}-1}{r}$
   (d) $N_j \leftarrow \gcd(T_j^{a_j}-1, q^k-1)$
   (e) $d_j \leftarrow \sum_{h=0}^{a_j-1} T_j^{a_j-1-h} q^{jh}$
   (f) $c_j \leftarrow \mathrm{rem}(d_j, N_j)$
   (g) $c_j' \leftarrow c_j^{-1} \bmod r$.
   (h) $U_e \leftarrow \frac{1}{r} \sum_{j=0}^{k-1} e_j T_j$
   (i) $U_\varepsilon \leftarrow \frac{1}{r} \sum_{j=0}^{k-1} \varepsilon_j T_j$
   (j) $\psi_\varepsilon \leftarrow U_\varepsilon - \sum_{j=0}^{k-1} \varepsilon_j c_j' n_j$
   (k) $\psi_\varepsilon' \leftarrow \psi_\varepsilon^{-1} \bmod r$.
   (l) Find the "right" τ such that $\tau^L = z^{\psi_\varepsilon'}$
   (m) Find the "right" α_j such that $\alpha_j^L = \tau^{L c_j' n_j}$

(n) $\gamma_e \leftarrow \frac{\tau^{U_e}}{\prod_{j=0}^{k-1} \alpha_j^{e_j}}$.

3. [MI_e] Find P from $\gamma_e = Z_e(P, Q)$.

By the "right" τ and the "right" α_j, we mean the ones satisfying the condition $\tau = f_{r,Q}(P)$ and $\alpha_j = f_{T_j,Q}(P)$ for some $P \in G_1$.

Remark 1. The above description is a bit different from the original one by Kanayama-Okamoto [15] in three ways.

- They used the quantity $\frac{\prod_{j=0}^{k-1} \alpha_j^{e_j}}{\tau^{U_e}}$ for γ_e, which is the reciprocal of the quantity shown above. We changed it in the current form, because it is more consistent with the notation used in Vercauteren's generalized pairings [25].
- They elaborated their idea for ate_i pairing (corresponding to a particular class of ε) and indicated that it could be extended to the generalized ate pairing of Vercauteren [25] (corresponding to a general class of ε). Indeed, such an extension is straightforward. The above description allows arbitrary ε.
- They elaborated their idea for particular choices of e such as coefficients of cyclotomic polynomials or $(1, \ldots, 1)$. The extension to arbitrary e is also straightforward. The above description allows arbitrary e.

3 A Simpler Approach for Paring Inversion

In this section, we describe an approach for inverting the generalized ate pairing of Vercauteren (Approach 1). We will use the notations introduced in Section 2.2. Comparing to Kanayama-Okamoto's approach (See Section 2.3), one sees that the modified exponentiation inversion step $\mathsf{EI}_{\varepsilon,e}$ is simplified. The simplicity of the proposed approach facilitates the subsequent investigation. We prove its correctness (Theorem 1). Then we compare the simpler approach with Kanayama-Okamoto's approach (Theorem 2). We let $a \equiv_n b$ abbreviate $a \equiv b \pmod{n}$ for simplicity.

Approach 1 Pairing Inversion

In: $Q \in G_2$, $z \in \mu_r$
Out: $P \in G_1$ such that $z = a_\varepsilon(Q, P)$.

1. [Choice] Choose $e \in \mathbb{Z}^k$ such that $r \mid \lambda_e(q)$ and $\gcd(e_0, \ldots, e_{k-1}) = 1$.
2. [$\mathsf{EI}_{\varepsilon,e}$] Find the "right" γ_e from $\Gamma_{\varepsilon,e,z} = \left\{\gamma \in \mathbb{F}_{q^k}^\times : \gamma^L = z^{\delta_{\varepsilon,e}}\right\}$, where $\delta_{\varepsilon,e} \equiv_r w_e/w_\varepsilon$ and $w_\eta = \frac{1}{r} W_\eta(q)$.
3. [MI_e] Find P from $\gamma_e = Z_e(P, Q)$.

By the "right" γ_e, we mean the ones satisfying the condition $\gamma_e = Z_e(Q, P)$ for some $P \in G_1$.

Theorem 1 (Correctness). *If $\gamma_e = Z_e(Q, P)$, then $\gamma_e^L = z^{\delta_{\varepsilon,e}}$.*

Proof. Recall that $\gamma_e^L = a_e(Q,P)$ and $z = a_\varepsilon(Q,P)$. Hence we need to show that

$$a_e(Q,P) = a_\varepsilon(Q,P)^{\delta_{\varepsilon,e}}.$$

Recall, from the proof of Theorem 4 in [25], that

$$f_{q,Q}(P)^{L\frac{\lambda_e(q)}{r}g'(q)\left(\frac{g(q)}{r}\right)^{-1}} = f_{q,Q}(P)^{L\lambda_e'(q)} \cdot a_e(Q,P).$$

and thus

$$a_e(Q,P) = f_{q,Q}(P)^{L\left(\frac{\lambda_e(q)}{r}g'(q)\left(\frac{g(q)}{r}\right)^{-1}-\lambda_e'(q)\right)} = f_{q,Q}(P)^{L\left(-\left(\frac{g(q)}{r}\right)^{-1}w_e\right)}.$$

Similarly, one gets

$$a_\varepsilon(Q,P) = f_{q,Q}(P)^{L\left(-\left(\frac{g(q)}{r}\right)^{-1}w_\varepsilon\right)}.$$

Thus,

$$a_e(Q,P) = f_{q,Q}(P)^{L\left(-\left(\frac{g(q)}{r}\right)^{-1}w_e\right)} = a_\varepsilon(Q,P)^{w_e w_\varepsilon^{-1}} = a_\varepsilon(Q,P)^{\delta_{\varepsilon,e}}. \qquad \square$$

One may wonder how the above approach compares to the approach of Kanayama-Okamoto. Since the MI_e steps are the same, we only need to compare $\mathsf{EI}_{\varepsilon,e}$ steps. Since $\mathsf{EI}_{\varepsilon,e}$ is essentially a search problem (finding the "right" elements), we need to compare the search spaces. Recall that the search space of Approach 1 is $\Gamma_{\varepsilon,e,z}$ when "brute-force" search is used. Likewise, the search space for the approach of Kanayama-Okamoto (see Section 2.3) amounts to

$$\Theta_{\varepsilon,e,z} = \left\{ \frac{\tau^{U_e}}{\prod_{j=0}^{k-1}\alpha_j^{e_j}} \;:\; \exists \tau, \alpha_j \in \mathbb{F}_{q^k}^\times \quad \alpha_j^L = \tau^{Lc_j'n_j} \;\wedge \tau^L = z^{\psi_\varepsilon'} \right\}$$

The following theorem states that the two "brute-force" search spaces are the same.

Theorem 2. *We have*

$$\Gamma_{\varepsilon,e,z} = \Theta_{\varepsilon,e,z}.$$

Proof. We will prove the inclusion in both directions.

Claim 1: $\Theta_{\varepsilon,e,z} \subset \Gamma_{\varepsilon,e,z}$

Let $\tau \in \mathbb{F}_{q^k}^\times$ and $\alpha_j \in \mathbb{F}_{q^k}^\times$ be such that $\alpha_j^L = \tau^{Lc_j'n_j}$ and $\tau^L = z^{\psi_\varepsilon'}$. Let $\theta = \frac{\tau^{U_e}}{\prod_{j=0}^{k-1}\alpha_j^{e_j}}$. We need to show that $\theta^L = z^{\delta_{\varepsilon,e}}$. Note

$$\theta^L = \left(\frac{\tau^{U_e}}{\prod_{j=0}^{k-1}\alpha_j^{e_j}}\right)^L = \frac{\tau^{LU_e}}{\prod_{j=0}^{k-1}\alpha_j^{Le_j}} = \frac{\tau^{LU_e}}{\prod_{j=0}^{k-1}\tau^{Le_jc_j'n_j}} = \tau^{L\left(U_e-\sum_{j=0}^{k-1}e_jc_j'n_j\right)} = \tau^{L\psi_e}$$

As $z = \tau^{L\psi_\varepsilon}$, we have $\theta^L = z^{\psi_e\psi_\varepsilon'}$. Since $Z_e(Q,P) \in \Theta_{e,z}$ as [15] showed, we also have $Z_e(Q,P)^L = z^{\psi_e\psi_\varepsilon'}$. Recall $Z_e(Q,P)^L = a_\varepsilon(Q,P)^{w_e w_\varepsilon'} = z^{w_e w_\varepsilon'}$. Thus,

$$\theta^L = z^{\psi_e\psi_\varepsilon'} = Z_e(Q,P)^L = a_\varepsilon(Q,P)^{w_e w_\varepsilon'} = z^{w_e w_\varepsilon'} = z^{\delta_{\varepsilon,e}}.$$

Claim 2: $\Gamma_{\varepsilon,e,z} \subset \Theta_{\varepsilon,e,z}$

Let $\gamma \in \mathbb{F}_{q^k}^{\times}$ be such that $\gamma^L = z^{\delta_{\varepsilon,e}}$. We need to find τ and α_j such that $\alpha_j^L = \tau^{Lc'_j n_j}$ and $\tau^L = z^{\psi'_\varepsilon}$ and $\gamma = \frac{\tau^{U_e}}{\prod_{j=0}^{k-1} \alpha_j^{e_j}}$. Let $P \in G_1$ and $Q \in G_2$ be such that $z = a_\varepsilon(Q,P)$. Such P, Q exist because the map $G_1 \to \mu_r, P \mapsto a_\varepsilon(Q,P)$ is bijective if $Q \in G_2 - \{O\}$. Let $\tilde{\tau} = f_{r,Q}(P)$ and $\tilde{\alpha}_j = f_{T_j,Q}(P)$ and $\tilde{\gamma} = \frac{\tilde{\tau}^{U_e}}{\prod_{j=1}^{k-1} \tilde{\alpha}_j^{e_j}}$. Let $h \in \mathbb{Z}^k$ be such that $\sum_{j=0}^{k-1} h_j e_j = 1$. Such h exists because $\gcd(e_0, \ldots, e_{k-1}) = 1$. Let

$$\tau = \tilde{\tau}, \qquad \alpha_j = \tilde{\alpha}_j \left(\frac{\tilde{\gamma}}{\gamma}\right)^{h_j}$$

Then we have

$$\tau^L = \tilde{\tau}^L = z^{\psi'_\varepsilon}$$

$$\alpha_j^L = \left(\tilde{\alpha}_j \left(\frac{\tilde{\gamma}}{\gamma}\right)^{h_j}\right)^L = \tilde{\alpha}_j^L \left(\frac{\tilde{\gamma}}{\gamma}\right)^{Lh_j} = \tilde{\alpha}_j^L \left(\frac{z^{\delta_{\varepsilon,e}}}{z^{\delta_{\varepsilon,e}}}\right)^{h_j} = \tilde{\tau}^{Lc'_j n_j} = \tau^{Lc'_j n_j}$$

$$\gamma = \tilde{\gamma}\frac{\gamma}{\tilde{\gamma}} = \frac{\tilde{\tau}^{U_e}}{\prod_{j=0}^{k-1} \tilde{\alpha}_j^{e_j}} \prod_{j=0}^{k-1} \left(\frac{\gamma}{\tilde{\gamma}}\right)^{h_j e_j} = \frac{\tilde{\tau}^{U_e}}{\prod_{j=0}^{k-1} \left(\tilde{\alpha}_j \left(\frac{\tilde{\gamma}}{\gamma}\right)^{h_j}\right)^{e_j}} = \frac{\tau^{U_e}}{\prod_{j=1}^{k-1} \alpha_j^{e_j}}$$

□

4 Complexity of Modified Miller Inversion

In this section, we provide a bit-complexity of the modified Miller inversion step MI_e. It essentially says that, when q and k are fixed, the complexity is bounded by $||e||_1^2$ where $||e||_1$ stands for the sum norm of the integer vector e. Hence in order to reduce the complexity of MI_e, one needs to choose e with small sum norm. This result can be viewed as an adaptation of the results/ideas [11] to the generalized ate pairing.

Theorem 3 (Complexity of MI_e). *There exists an algorithm for MI_e requiring at most*

$$2^8 \; ||e||_1^2 \; k^2 \; (\log_2 q)^3$$

bit operations.

In the remainder of this section, we will prove Theorem 3. We will divide the proof into several lemmas that are interesting on their own. We begin with a slight reformulation of the expression for the generalized ate pairing [25], because it greatly simplifies the derivation of the above upper bound.

Lemma 1. *Let $e^{(+)}, e^{(-)} \in \mathbb{Z}^k$ be*

$$e_i^{(+)} = \begin{cases} e_i \text{ if } e_i > 0 \\ 0 \quad \text{else} \end{cases} \qquad \text{and} \qquad e_j^{(-)} = \begin{cases} e_j \text{ if } e_j < 0 \\ 0 \quad \text{else} \end{cases}$$

Then, for all $Q \in G_2$ and all $P \in G_1$, we have

$$Z_e(Q,P) = \frac{Z_{e^{(+)}}(Q,P)}{Z_{-e^{(-)}}(Q,P)}$$

Proof. See the Appendix. □

Lemma 2. *For every $Q \in G_2$, $\theta \in \mathbb{F}_{q^k}^*$ and $e \in \mathbb{Z}^\ell$, there exists a bivariate polynomial h over $\mathbb{F}_{q^k}$ such that*

(a) $\forall (x,y) \in G_1 \quad \theta = Z_e(Q,(x,y)) \implies h(x,y) = 0$
(b) $\deg_X(h) \le ||e||_1$
(c) $\deg_Y(h) \le 2\max\{s,t\}$, *where* $s := \#\{j : e_j > 0\}$ *and* $t := \#\{j : e_j < 0\}$.

Proof. See the Appendix.. □

Proof (Proof of Theorem 3). To solve MI_e for given $Q \in G_2$ and $e \in \mathbb{Z}^\ell$, we have to find $P = (x,y) \in G_1$ such that

$$\theta = Z_e(Q,(x,y)), \qquad y^2 = x^3 + ax + b \tag{1}$$

Let h be a bivariate polynomial over $\mathbb{F}_{q^k}$ satisfying the three conditions in Lemma 2 and let, for the h,

$$F(X,Y) = Y^2 - X^3 - aX - b$$
$$u(X) = \mathrm{res}_Y(h(X,Y), F(X,Y)).$$

Note, for all $(x,y) \in G_1$, if $\theta = Z_e(Q,(x,y))$, then $u(x) = 0$ and

$$\deg u \;\le\; \deg_Y F \deg_X h + \deg_Y h \deg_X F \;\le\; 2 \cdot ||e||_1 + 2||e||_1 \cdot 3 \;=\; 8\,||e||_1 .$$

From [11], there exists an algorithm for solving a polynomial of degree d in $\mathbb{F}_q$ whose complexity is $O(d^2k^2(\log q)^3)$. In fact, a more detailed analysis shows that the algorithm requires at most $4\ d^2\ k^2\ (\log_2 q)^3$ bit operations. Since solving $u(X) = 0$ is enough to solve the system of equations (1), we see that MI_e can be solved within

$$4\,(8\,||e||_1)^2\,k^2\,(\log_2 q)^3 = 2^8\ ||e||_1^2\ k^2\ (\log_2 q)^3 .$$

bit operations. □

5 Toward Complexity of Modified Exponentiation Inversion

It would be nice to have a complexity estimate for the modified exponentiation inversion $\mathsf{EI}_{\varepsilon,e}$, just as for the modified Miller inversion MI_e (Theorem 3). Unfortunately, we do *not* have a result on it. We are not aware of any results

in the literature either. We expect it to be a very non-trivial task, most likely requiring patient and long arduous efforts of many researchers, each making an incremental contribution. In this section, we report on an incremental finding toward complexity of $\mathsf{EI}_{\varepsilon,e}$.

Recall that $\mathsf{EI}_{\varepsilon,e}$ asks to find the "right" γ_e from the search space $\Gamma_{\varepsilon,e,z}$. Hence it is reasonable to begin with the study of the relationship between the search space $\Gamma_{\varepsilon,e,z}$ and the chosen vector e.

Proposition 1. *We have*

1. *If the auxiliary pairing a_e is degenerate, then $\Gamma_{\varepsilon,e,z} = \Gamma_{\varepsilon,\varepsilon,1} = \mu_L$.*
2. *If the auxiliary pairing a_e is non-degenerate, then $\Gamma_{\varepsilon,e,z} = \Gamma_{\varepsilon,\varepsilon,z^{\delta_{\varepsilon,e}}}$.*

Proof. Note that $\delta_{\varepsilon,\varepsilon} = 1$. Recall that $\delta_{\varepsilon,e} \equiv_r w_e/w_\varepsilon$ and $w_e = \frac{1}{r}W_e(q) \in \mathbb{Z}$. Therefore we have

$$a_e \text{ is degenerate } \iff r^2 | W_e(q) \iff w_e \equiv_r 0 \iff \delta_{\varepsilon,e} \equiv_r 0$$

If a_e is degenerate, then we have

$$\Gamma_{\varepsilon,e,z} \;=\; \left\{\gamma \in \mathbb{F}_{q^k}^\times : \gamma^L = z^0\right\} \;=\; \left\{\gamma \in \mathbb{F}_{q^k}^\times : \gamma^L = 1^{\delta_{\varepsilon,\varepsilon}}\right\} \;=\; \Gamma_{\varepsilon,\varepsilon,1} = \mu_L$$

If a_e is non-degenerate, then we have

$$\Gamma_{\varepsilon,e,z} = \left\{\gamma \in \mathbb{F}_{q^k}^\times : \gamma^L = z^{\delta_{\varepsilon,e}}\right\} \;=\; \left\{\gamma \in \mathbb{F}_{q^k}^\times : \gamma^L = \left(z^{\delta_{\varepsilon,e}}\right)^{\delta_{\varepsilon,\varepsilon}}\right\} \;=\; \Gamma_{\varepsilon,\varepsilon,z^{\delta_{\varepsilon,e}}}$$

□

Remark 2. From the above proposition, we observe the followings:

- If a_e is degenerate then the search space of $\mathsf{EI}_{\varepsilon,e}$ is *independent* of the input z, that is, the exponential relation in $\mathsf{EI}_{\varepsilon,e}$ does not capture any information about the input. Thus the modified exponentiation inversion $\mathsf{EI}_{\varepsilon,e}$ will be most likely *harder* when a_e is degenerate than when a_e is non-degenerate.
- If a_e is non-degenerate then the search space of $\mathsf{EI}_{\varepsilon,e}$ for an input z is the same as that of EI_ε for *another* input $z^{\delta_{\varepsilon,e}}$. Thus the modified exponentiation inversion $\mathsf{EI}_{\varepsilon,e}$ is likely as hard as the original exponentiation inversion EI_ε.

Therefore, as a first step toward finding an efficient method for $\mathsf{EI}_{\varepsilon,e}$, we better ensure that a_e is non-degenerate. The following theorem (Theorem 4) gives a sufficient condition on e, in terms of the max norm of e, for the non-degeneracy of a_e. We will use the following lemma in the proof of the theorem, hence we state it first.

Lemma 3. *Let s be a primitive k-th root of unity modulo r^2 and $s \equiv q \mod r$. Then $r^2 \nmid \lambda_e(s)$ iff a_e is non-degenerate.*

Proof. The claim follows easily from the proof of [12, Theorem 3]. See the Appendix for a detailed proof in terms of our terminologies.

Theorem 4. *Let $e \in \mathbb{Z}^k$ be such that $r \mid \lambda_e(q)$ and $\Phi_k(X) \nmid \lambda_e(X)$. Let $m_e = [\mathbb{Q}(\zeta_k) : \mathbb{Q}(\lambda_e(\zeta_k))]$. If*

$$||e||_\infty < \frac{r^{2m_e/\varphi(k)}}{\varphi(k)}$$

then a_e is non-degenerate.

Proof. We will prove the contra-positive. Assume that a_e is degenerate. We claim

$$||e||_\infty \geq \frac{r^{2m_e/\varphi(k)}}{\varphi(k)}.$$

Let $s \in \mathbb{Z}$ be such that $s \equiv q \pmod{r}$ and $\mathrm{ord}_{r^2}(s) = k$. To prove the claim, we will use the fact that a_e is degenerate if and only if $r^2 \mid \lambda_e(s)$ (Lemma 3). Note $r^2 \mid (s^k - 1) = \prod_{d|k} \Phi_d(s)$. Since $r \mid \Phi_d(s) = \Phi_d(q + \iota r)$ implies $r \mid \Phi_d(q)$, r divides only $\Phi_k(s)$ and $r \nmid \Phi_d(s)$ for all $d < k$. Therefore, $r^2 \mid \Phi_k(s)$.

Let $\mu_e(X) = \mathrm{rem}(\lambda_e(X), \Phi_k(X))$ and $\zeta_k \in \mathbb{C}$ be a primitive k-th root of unity. Note that $\mu_e \neq 0$ from the assumption. Let $v(X) \in \mathbb{Q}[X]$ be the minimal polynomial of $\mu_e(\zeta_k)$ over $\mathbb{Q}$. Note that $v(x) \in \mathbb{Z}[x]$ as $\mu_e(\zeta_k) \in \mathbb{Z}[\zeta_k]$, the ring of integers of $\mathbb{Q}(\zeta_k)$. Since $v(\mu_e(X))$ is zero at ζ_k and $\Phi_k(x)$ is monic, we have

$$v(\mu_e(X)) = \Phi_k(X)h(X) \quad \text{for some} \quad h(X) \in \mathbb{Z}[X].$$

From $r^2 \mid \lambda_e(s)$ and $r^2 \mid \Phi_k(s)$, we have $r^2 \mid \mu_e(s)$ and

$$v(0) \equiv_{r^2} v(\mu_e(s)) \equiv_{r^2} \Phi_k(s)h(s) \equiv_{r^2} 0$$

Therefore, we have either $v(0) = 0$ or $|v(0)| \geq r^2$. Noting that, by [6, Proposition 4.3.2] and the fact that v is monic,

$$|v(0)| = |\mathrm{Norm}(\mu_e(\zeta_k))| = \left|\mathrm{Norm}_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\mu_e(\zeta_k))\right|^{\frac{1}{m_e}} = \left|\prod_{\gcd(j,k)=1} \mu_e(\zeta_k^j)\right|^{\frac{1}{m_e}},$$

we conclude that $v(0) \neq 0$. Indeed if $v(0) = 0$, then $\Phi_k \mid \lambda_e$, a contradiction to $\mu_e \neq 0$. Thus, we have

$$r^2 \leq |v(0)| = \left|\prod_{\gcd(j,k)=1} \mu_e(\zeta_k^j)\right|^{\frac{1}{m_e}} \leq \left(\prod_{\gcd(j,k)=1} \varphi(k)||e||_\infty\right)^{\frac{1}{m_e}} = (\varphi(k)||e||_\infty)^{\frac{\varphi(k)}{m_e}}$$

Therefore, we finally have the claim. □

6 Reducing Paring Inversion to Modified Exponentiation Inversion

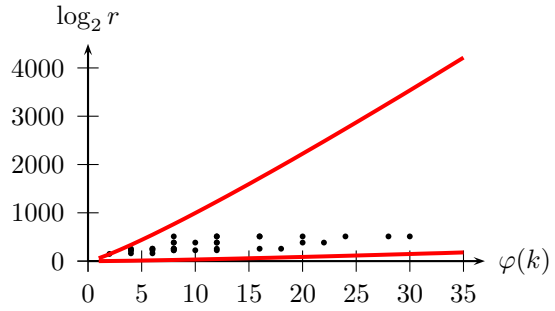
In this section, we discuss when pairing inversion can be reduced to modified exponentiation inversion $\mathsf{EI}_{\varepsilon,e}$.

Specifically we are looking for a condition on e so that MI_e is easy. According to Theorem 3, we need to find *small* e. One might be naturally tempted to choose the integer vector e from either coefficients of cyclotomic polynomials or $(1, \ldots, 1)$. However according to Corollary 6 of Vercauteren [25], such e makes the corresponding auxiliary pairing degenerate. Hence, from Proposition 1, the modified exponentiation inversion $\mathsf{EI}_{\varepsilon,e}$ is expected to be hard because the search space does *not* depend on z. Therefore, in order to meaningfully reduce pairing inversion to modified exponentiation inversion, one needs find e such that it is *small* and the corresponding auxiliary pairing is *non-degenerate*. In this section, we investigate the existence of such e in various cases (Theorem 5 and the subsequent examples in Table 1). We begin by introducing a definition that was inspired by the discussions in[11].

Definition 1. *Let C_α be the set of all $(r, k) \in \mathbb{Z}^2_{>0}$ satisfying*

C1: $r^{1/\varphi(k)} > \varphi(k)$
C2: $r^{1/\varphi(k)} \leq (\log_2 r)^\alpha$

Remark 3. In the following figure, the bottom curve is from the condition C1 in Definition 1 and the top curve is from the condition C2 when $\alpha = 10$. Thus, the regions between the two curves is the set C_{10}, The black dots represent typical pairing friendly curves from Table 1 in [10]. Note that the parameters for the typical pairing friendly curves belong to C_{10}.



Lemma 4. *If $\alpha > 1$, then C_α is an infinite set.*

Proof. See the Appendix. □

Theorem 5. *Let $\alpha > 1$, $(r, k) \in C_\alpha$ and $r \geq \sqrt{q}$. Then the inversion of every generalized ate pairing can be reduced to modified exponentiation inversion in polynomial time in $\log_2 r$. Specifically, there exists e such that the auxiliary pairing a_e is non-degenerate and MI_e can be carried out in at most*

$$2^{13} \quad (\log_2 r)^{8\alpha+3}$$

bit operations.

Proof. Let $(q, r) \in C_\alpha$ and $r \geq \sqrt{q}$. We need to find a "witness" e such that a_e is non-degenerate and MI_e can be carried out in the claimed number of bit operations. From Minkowski's theorem (see III.C of [25]), there exists $e \in \mathbb{Z}^k$ with $r \mid \lambda_e(q)$ such that the last $k - \varphi(k)$ elements of e are zero and

$$||e||_\infty \leq r^{1/\varphi(k)}$$

We will take it as the witness.

First we show that a_e is non-degenerate. Since the last $k - \varphi(k)$ elements of e are zero, we have $\lambda_e(X) \nmid \Phi_k(X)$. From the condition that $r^{1/\varphi(k)} > \varphi(k)$, we have

$$\frac{r^{(2m_e-1)/\varphi(k)}}{\varphi(k)} \geq \frac{r^{1/\varphi(k)}}{\varphi(k)} > 1$$

and thus

$$||e||_\infty \leq r^{1/\varphi(k)} < r^{1/\varphi(k)} \frac{r^{(2m_e-1)/\varphi(k)}}{\varphi(k)} = \frac{r^{2m_e/\varphi(k)}}{\varphi(k)}$$

Therefore, by Theorem 4, a_e is non-degenerate.

Next we show that MI_e can be carried out in the claimed number of bit operations. Let N be the number of bit operations for MI_e. Note that $||e||_1 \leq \varphi(k)\,||e||_\infty$. Hence $||e||_1 \leq \varphi(k) r^{1/\varphi(k)}$. Therefore, from Theorem 3, we have

$$N \leq 2^8 \ \left(\varphi(k) r^{1/\varphi(k)}\right)^2 \ k^2 \ (\log_2 q)^3$$

From the condition $r \geq \sqrt{q}$, we have

$$N \leq 2^8 \ \left(\varphi(k) r^{1/\varphi(k)}\right)^2 \ k^2 \ (2\log_2 r)^3 = 2^{11} \ \varphi(k)^2 \ r^{2/\varphi(k)} \ k^2 \ (\log_2 r)^3$$

Since $\sqrt{k} \leq \sqrt{2}\varphi(k)$ and $\varphi(k) < r^{1/\varphi(k)}$, we have

$$N \leq 2^{11} \ \varphi(k)^2 \ r^{2/\varphi(k)} \ 4\ \varphi(k)^4 \ (\log_2 r)^3 = 2^{13} \ r^{8/\varphi(k)} \ (\log_2 r)^3$$

Since $r^{1/\varphi(k)} \leq (\log_2 r)^\alpha$, we have

$$N < 2^{13} \ (\log_2 r)^{8\alpha} \ (\log_2 r)^3 = 2^{13} \ (\log_2 r)^{8\alpha+3}$$ □

The upper bound in Theorem 5 is not tight. In Table 1, we provide tighter upper bounds for several examples. For each example, the first row of the table shows $k, \varphi(k), \log_2 r, \alpha$ with which we can estimate an upper bound of the bit complexity for reducing PI to $\mathsf{EI}_{\varepsilon,e}$, using Theorem 5. The next rows show actual parameters q, r and a vector $e \in \mathbb{Z}^{\varphi(k)}$. The vector e is the one with smallest sum norm among the LLL reduced vectors for the lattice with respect to q, r, k [25]. The vector e is verified to yield non-degenerate a_e. For the vector e, the last row has been calculated using Theorem 3, which estimates the bit complexity of MI_e on the curve more precisely. The estimated upper bounds on the computing

times are based on the assumption that one uses the currently fastest supercomputer [8], which can perform about $17 \cdot 10^{15}$ flops $\times 1000 \frac{\text{bops}}{\text{flops}} = 2^{64}$bops (bit operations per second).

The first example BN is the smallest value taken from Table 1 in [21]. Since $\varphi(k)$ for the BN curves [5] are small ($\varphi(k) = 4$), they easily satisfy the condition C1 in Definition 1 but large α values are needed to satisfy C2. Therefore, from Theorem 5, we expect that it will be difficult to reduce PI to $\mathsf{EI}_{\varepsilon,e}$ for BN curves. The tighter upper bound on the bit operation on the last row, based on Theorem 3, supports the observation. Next two examples are the KSS curves described in Example 4.6 and Example 4.7 in [16]. The parameters are obtained by evaluating the polynomials in the Examples in [16] at $x_0 = -188$ for KSS1 and $x_0 = 107$ for KSS2. The example CP1 is constructed by Cocks-Pinch method to have small α and "typical" parameters $(k, \log_2 r)$ in Table 1 in [10]. The example C6.6 is obtained from evaluating the polynomials in Construction 6.6 with $k = 33$ in [10] at $x_0 = -9727$, which is also a pairing-friendly curve (Definition 2.3 in [10]). The $\varphi(k)$ for these curves are small enough to satisfy C1, and big enough for small α values to satisfy C2. Therefore, from Theorem 5, we expect that it will be relatively easy to reduce PI to $\mathsf{EI}_{\varepsilon,e}$ for these curves. The tighter upper bound on the bit operations on the last row, based on Theorem 3, supports the observation.

Acknowledgement

The authors would like to thank Steven Galbraith and anonymous referees for their insightful and helpful comments.

References

1. Barreto, P., Galbraith, S., Ó hÉigeartaigh, C., Scott, M. : Efficient Pairing Computation on Supersingular Abelian Varieties. Designs, Codes and Cryptography 42, no. 3, pp.239-271 (2007)
2. Boneh, D., Franklin, M. : Identity-based encryption from the Weil pairing. SIAM J. of Computing 32, no. 3, pp.586-615 (2003)
3. Boneh, D., Goh, E., Nissim, K. : Evaluating 2-DNF formulas on ciphertexts. In Proceedings of Theory of Cryptography (TCC)'05, LNCS 3378, pp.325-341 (2005)
4. Boneh, D., Lynn, B., Shacham, H. : Short signatures from the Weil pairing. J. of Cryptology 17, no 4, pp.297-319 (2004)
5. Barreto, P., Naehrig, M. : Pairing-friendly elliptic curves of prime order. In Proceedings of SAC 2005, LNCS 3897, pp.319-331 (2006)
6. Cohen, H. : A Course in Computational Algebraic Number Theory. Springer, Heidelberg (2000)
7. Duc, A., Jetchev, D. : Hardness of Computing Individual Bits for One-way Functions on Elliptic Curves. In Proceedings of Advances in Cryptography CRYPTO 2012, LNCS 7417, pp.832-849 (2012)
8. Cray Titan: olcf.ornl.gov/titan/, en.wikipedia.org/wiki/Titan_(supercomputer)

Table 1. Estimates on time needed for reducing pairing inversion to exponentiation inversion

BN	$k,\ \varphi(k),\ \log_2 r,\ \alpha$	12, 4, 158, 6
	q	206327671360737302491015800744139033450591027219
	r	2063276713607373024910153465110806135606083584 13
	e	$[-550292684801, 0, -550292684802, 1]$
	$\|\|e_1\|\|$	$\approx 2^{41}$
	bit ops	$< 2^{118} \approx 5.7 \times 10^8$ years
KSS1	$k,\ \varphi(k),\ \log_2 r,\ \alpha$	40, 16, 270, 3
	q	178326709713245217260627572968724387343855332468581993976702897877627555783690964596151952604627173843429620177224588 89
	r	1033360998958592639176333946764816221704441278553743659647994766150169434118209921
	e	$[-89353, -1, 0, 0, 0, 0, 0, 0, 0, 0, -178706, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$
	$\|\|e_1\|\|$	$\approx 2^{19}$
	bit ops	$< 2^{81} \approx 1.5$ days
KSS2	$k,\ \varphi(k),\ \log_2 r,\ \alpha$	36, 12, 169, 2
	q	27515431606313682600546511947515923267058275939278041592973834669
	r	70570852702852842087313563225319458709272845667 3193
	e	$[644, 966, 2899, -2255, 8697, 10307, 12562, -2577, 5798, 0, 6120, 2577, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$
	$\|\|e_1\|\|$	$\approx 2^{16}$
	bit ops	$< 2^{74} \approx 17.1$ minutes
CP1	$k,\ \varphi(k),\ \log_2 r,\ \alpha$	23, 22, 257, 2
	q	145811957602744608340173404592073971131183909622716668761512762300485126800359788580000631375404539994870728043984894024890668938268039944103589738865779 3
	r	171162823577658908923577123057263396229244166914410717458536445501121285956693
	e	$[-196, -527, -851, -89, -648, 115, 1086, -14, 547, -1053, 409, -611, 680, -1368, -891, -1808, -3226, -1664, 577, 22, 213, 15, 0]$
	$\|\|e_1\|\|$	$\approx 2^{15}$
	bit ops	$< 2^{73} \approx 8.5$ minutes
C6.6	$k,\ \varphi(k),\ \log_2 r,\ \alpha$	33, 20, 265, 2
	q	171560529093254543159492466399817736252453023032471929261478201236234936574795328339355710502059
	r	5748223778236752251949820353441114077317933366192134035319178177655578384 3120129
	e	$[0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, -9727, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$
	$\|\|e_1\|\|$	$\approx 2^{14}$
	bit ops	$< 2^{70} \approx 1.1$ minutes

9. Duursma, I., Lee, H.-S. : Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. In Proceedings of Advances in Cryptography AsiaCrypt 2003, LNCS 2894, pp.111-123 (2003)
10. Freeman, D., Scott, M., Teske, E. : A taxonomy of pairing-friendly elliptic curves. J. of Cryptology 23, pp.224-280 (2010)
11. Galbraith, S., Hess, F., Vercauteren, F. : Aspects of Pairing Inversion. IEEE Trans. Information Theory 54, pp.5719-5728 (2008)
12. Hess, F. : Pairing Lattices. In Proceedings of Pairing 2008, LNCS 5209, pp.18-38 (2008)
13. Hess, F., Smart, N., Vercauteren, F. : The Eta Pairing Revisited. IEEE Trans. Information Theory 52, pp.4595-4602 (2006)
14. Joux, A. : A one round protocol for tripartite Diffie-Hellman. J. of Cryptology 17, no. 4, pp.263-276 (2004)
15. Kanayama, N., Okamoto, E. : Approach to Pairing Inversions Without Solving Miller Inversion. IEEE Trans. Information Theory 58, pp.1248-1253 (2012)
16. Kachisa, E., Schaefer, E., Scott, M. : Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic elements. In Proceedings of Pairing 2008, LNCS 5209, pp.126-135 (2008)
17. Kim, S., Cheon, J. : Fixed Argument Pairing Inversion on Elliptic Curves, preprint (2012). Available at http://eprint.iacr.org/2012/657
18. Lee, E., Lee, H.-S., Park, C. : Efficient and Generalized Pairing Computation on Abelian Varieties. IEEE Trans. Information Theory 55, no. 4, pp.1793-1803 (2009)
19. Miller, V. : The Weil pairing and its efficient calculation. J. of Cryptology 17, pp.235-261 (2004)
20. El Mrabet, N. : What about Vulnerability to a Fault Attack of the Millers Algorithm During an Identity Based Protocol?. In Proceedings of ISA 2009, LNCS 5576, pp.122-134 (2009)
21. Pereira, G., Simplício, M., Naehrig, M., Barreto, P. : A Family of Implementation-Friendly BN Elliptic Curves. J. of Systems and Software 84, Issue 8, pp.1319-1326 (2011)
22. Page, D., Vercauteren, F. : A Fault Attack on Pairing Based Cryptography. IEEE Trans. Computers 55, no. 9, pp.1075-1080 (2006)
23. Satoh, T. : On polynomial interpolations related to Verheul homomorphisms. J. Comput. Math. 9, pp.135-158 (2006)
24. Satoh, T. : On pairing inversion problems. In Proceedings of Pairing 2007, LNCS 4575, pp.317-328 (2007)
25. Vercauteren, F. : Optimal Pairings. IEEE Trans. Information Theory 56, no. 1, pp.455-461 (2010)
26. Verheul, E. : Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. J. Cryptology 17, no. 4, pp.277-296 (2004)
27. Waters, B. : Efficient Identity-Based Encryption Without Random Oracles. In Proceedings of Advances in Cryptology EUROCRYPT 2005, LNCS 3494, pp.114-127 (2005)
28. Weng, J., Dou, Y., Ma, C. : Fault Attacks against the Miller Algorithm in Hessian Coordinates. In Proceedings of InsCrypt 2011: Information and Cryptology, LNCS 7537, pp.102-112 (2012)
29. Zhao, C., Zhang, F., Huang, J. : A Note on the Ate Pairing. International J. of Information Security 7, no. 6, pp.379-382 (2008)

Appendix

In this appendix, we provide proofs of several technical lemmas.

Proof (Proof of Lemma 1). Let $e_{m_1}, \ldots, e_{m_s} > 0$ and $e_{n_1}, \ldots, e_{n_t} < 0$ and all other components of e are zero. Then we have

$$e^{(+)}_{m_i} = e_{m_i} \qquad\qquad e^{(-)}_{n_j} = e_{n_j}$$

and all other components of $e^{(+)}$ and $e^{(-)}$ are zero. Note

$$U_e r - e_{n_1} q^{n_1} - \cdots - e_{n_t} q^{n_t} = e_{m_1} q^{m_1} + \cdots + e_{m_s} q^{m_s}$$

Thus

$$\begin{aligned}
&f_{e_{m_1} q^{m_1} + \cdots + e_{m_s} q^{m_s}, Q} \\
&= \prod_{i=1}^{s} f^{e_{m_i}}_{q^{m_i}, Q} \prod_{i=1}^{s} f_{e_{m_i}, q^{m_i} Q} \prod_{i=1}^{s-1} \frac{l_{e_{m_i} q^{m_i} Q, \left(e_{m_{i+1}} q^{m_{i+1}} + \cdots + e_{m_s} q^{m_s}\right) Q}}{v_{\left(e_{m_i} q^{m_i} + \cdots + e_{m_s} q^{m_s}\right) Q}} \\
&= \prod_{i=1}^{s} f^{e_{m_i}}_{q^{m_i}, Q}(P) \cdot Z_{e^{(+)}}(Q, P) \\
&f_{U_e r - e_{n_1} q^{n_1} - \cdots - e_{n_t} q^{n_t}, Q} \\
&= f_{U_e r, Q} f_{-e_{n_1} q^{n_1} - \cdots - e_{n_t} q^{n_t}, Q} \\
&= f^{U_e}_{r,Q}(P) \prod_{j=1}^{t} f^{-e_{n_j}}_{q^{n_j}, Q}(P) \cdot Z_{-e^{(-)}}(Q, P)
\end{aligned}$$

Hence

$$f^{U_e}_{r,Q}(P) \prod_{j=1}^{t} f^{-e_{n_j}}_{q^{n_j}, Q}(P) \cdot Z_{-e^{(-)}}(Q, P) = \prod_{i=1}^{s} f^{e_{m_i}}_{q^{m_i}, Q} \cdot Z_{e^{(+)}}(Q, P)$$

and, from [25], we have

$$Z_e(Q, P) = \frac{f^{U_e}_{r,Q}(P)}{\prod_{i=0}^{k-1} f^{e_i}_{q^i, Q}(P)} = \frac{Z_{e^{(+)}}(Q, P)}{Z_{-e^{(-)}}(Q, P)}$$

□

Proof (Proof of Lemma 2). Let $Q \in G_2$, $\theta \in \mathbb{F}^*_{q^k}$ and $e \in \mathbb{Z}^\ell$. We will construct a witness for the existentially quantified h. From Lemma 14 of [11], we have

$$f_{\mu,\, \nu Q}(X, Y) = \begin{cases} 1 & \mu = 1 \\ \frac{f_{\mu,\nu,1}(X) + Y f_{\mu,\nu,2}(X)}{v_{\mu\nu Q}} & \mu > 1 \end{cases}$$

where $f_{\mu,\nu,1}, f_{\mu,\nu,2} \in \mathbb{F}_{q^k}[X]$ such that

$$\deg(f_{\mu,\nu,1}) \leq \left\lfloor \frac{\mu+1}{2} \right\rfloor, \qquad \deg(f_{\mu,\nu,2}) \leq \left\lfloor \frac{\mu}{2} - 1 \right\rfloor$$

From Lemma 1, we have

$$Z_e\left(Q,(x,y)\right) = \frac{Z_{e^{(+)}}(x,y)}{Z_{-e^{(-)}}(x,y)} =: \frac{A(x,y)}{B(x,y)} \quad \text{for all} \quad (x,y) \in G_1$$

where

$$\begin{aligned}
A = & \prod_{\substack{1\leq i\leq s \\ e_{m_i}\geq 2}} \left(f_{e_{m_i},q^{m_i},1} + Y f_{e_{m_i},q^{m_i},2}\right) \prod_{\substack{1\leq j\leq t \\ e_{n_j}\leq -2}} v_{-e_{n_j}q^{n_j}Q} \\
& \prod_{i=1}^{s-1} l_{e_{m_i}q^{m_i}Q,\left(e_{m_{i+1}}q^{m_{i+1}}+\cdots+e_{m_s}q^{m_s}\right)Q} \prod_{j=1}^{t-1} v_{\left(-e_{n_{j+1}}q^{n_{j+1}}-\cdots-e_{n_t}q^{n_t}\right)Q} \\
B = & \prod_{\substack{1\leq j\leq t \\ e_{n_j}\leq -2}} \left(f_{-e_{n_j},q^{n_j},1} + Y f_{-e_{n_j},q^{n_j},2}\right) \prod_{\substack{1\leq i\leq s \\ e_{m_i}\geq 2}} v_{e_{m_i}q^{m_i}Q} \\
& \prod_{j=1}^{t-1} l_{-e_{n_j}q^{n_j}Q,\left(-e_{n_{j+1}}q^{n_{j+1}}-\cdots-e_{n_t}q^{n_t}\right)Q} \prod_{i=1}^{s-1} v_{\left(e_{m_i}q^{m_i}+\cdots+e_{m_s}q^{m_s}\right)Q}
\end{aligned}$$

Finally, we propose the following h as a witness for the existential quantification:

$$h = A - \theta B.$$

We will show that h is indeed a witness satisfying the three conditions.

(a) $\forall (x,y) \in G_1, \quad Z_e(Q,(x,y)) = \theta \implies h(x,y) = 0$.: Let $(x,y) \in G_1$. Assume that $\theta = Z_e(Q,(x,y))$. Then Obviously $\theta = \frac{A(x,y)}{B(x,y)}$. Thus $h(x,y) = A(x,y) - \theta B(x,y) = 0$.

(b) $\deg_X(h) \le ||e||_1$: Note

$$\begin{aligned}
\deg_X(A) &\le \sum_{e_i \ge 2} \left\lfloor \frac{e_i+1}{2} \right\rfloor + \sum_{e_i \le -2} 1 + \sum_{e_i \ge 1} 1 + \sum_{e_i \le -1} 1 \\
&= \sum_{e_i \ge 2} \left\lfloor \frac{e_i+3}{2} \right\rfloor + \sum_{e_i \le -2} 2 + \sum_{e_i = 1} 1 + \sum_{e_i = -1} 1 \\
&\le \sum_{e_i \ge 2} |e_i| + \sum_{e_i \le -2} |e_i| + \sum_{e_i = 1} |e_i| + \sum_{e_i = -1} |e_i| \\
&= ||e||_1 \\
\deg_X(B) &\le \sum_{e_i \le -2} \left\lfloor \frac{-e_i+1}{2} \right\rfloor + \sum_{e_i \ge 2} 1 + \sum_{e_i \le -1} 1 + \sum_{e_i \ge 1} 1 \\
&= \sum_{e_i \le -2} \left\lfloor \frac{-e_i+3}{2} \right\rfloor + \sum_{e_i \ge 2} 2 + \sum_{e_i = -1} 1 + \sum_{e_i = 1} 1 \\
&\le \sum_{e_i \le -2} |e_i| + \sum_{e_i \ge 2} |e_i| + \sum_{e_i = -1} |e_i| + \sum_{e_i = 1} |e_i| \\
&= ||e||_1
\end{aligned}$$

Hence $\deg_X(h) \le ||e||_1$.

(c) $\deg_Y(h) \le 2\max\{s,t\}$: Note

$$\deg_Y(A) \le s + s \le 2s, \qquad \deg_Y(B) \le t + t \le 2t$$

Hence $\deg_Y(h) \le 2\max\{s,t\}$.

□

Proof (Proof of Lemma 3). Note

$$f_{r,Q}^{\frac{s^k-1}{r}} = f_{s^k-1,Q} = f_{s^k,Q} = f_{s,Q}^{s^{k-1}} f_{s,sQ}^{s^{k-2}} \cdots f_{s,s^{k-1}Q}$$

Since $s \equiv q \pmod r$ and $f_{s,sQ} = f_{s,qQ} = f_{s,Q}^q$, we have

$$f_{r,Q}^{\frac{s^k-1}{r}} = f_{s,Q}^{s^{k-1}} f_{s,Q}^{qs^{k-2}} \cdots f_{s,s^{k-2}Q}^{q} = f_{s,Q}^{s^{k-1}+qs^{k-2}+\cdots+q^{k-1}} \tag{2}$$

Let $u = s^{k-1} + qs^{k-2} + \cdots + q^{k-1}$. Then $u \equiv kq^{k-1} \bmod r$. Raising Eq. (2) to the power $(q^k-1)/r$, we have

$$t(Q,P)^{\frac{s^k-1}{r}} = f_{s,Q}(P)^{\frac{(q^k-1)}{r}\cdot u}.$$

Since $r \mid \frac{s^k-1}{r}$, we have

$$t(Q,P)^{\frac{s^k-1}{r}} = 1$$

$$f_{s,Q}(P)^{\frac{(q^k-1)}{r}} = 1.$$

Therefore, $f_{s^i,Q}(P)^{\frac{q^k-1}{r}} = f_{s,Q}^{(s^{i-1}+s^{i-2}q+\ldots+q^{i-1})\frac{q^k-1}{r}} = 1$ for $0 \le i \le k-1$. Note

$$\begin{aligned}
t(Q,P)^{\frac{\lambda_e(s)}{r}} &= f_{r,Q}(P)^{\frac{\lambda_e(s)}{r}\frac{q^k-1}{r}} \\
&= f_{\lambda_e(s),Q}(P)^{\frac{q^k-1}{r}} \\
&= f_{e_0+\cdots+e_{k-1}s^{k-1},Q}\left(P\right)^{\frac{q^k-1}{r}} \\
&= \prod_{j=0}^{k-1} f_{e_j s^j,Q}\left(P\right)^{\frac{q^k-1}{r}} \left(\prod_{j=0}^{k-2} \frac{\ell_{e_j s^j Q,(e_{j+1}s^{j+1}+\cdots+e_{k-1}s^{k-1})Q}\left(P\right)}{v_{(e_j s^j+\cdots+e_{k-1}s^{k-1})Q}\left(P\right)}\right)^{\frac{q^k-1}{r}} \\
&= \prod_{j=0}^{k-1} f_{s^j,Q}\left(P\right)^{e_j\frac{q^k-1}{r}} \prod_{j=0}^{k-1} f_{e_j,q^jQ}\left(P\right)^{\frac{q^k-1}{r}} \left(\prod_{j=0}^{k-2} \frac{\ell_{e_j q^j Q,(e_{j+1}q^{j+1}+\cdots+e_{k-1}q^{k-1})Q}\left(P\right)}{v_{(e_j q^j+\cdots+e_{k-1}q^{k-1})Q}\left(P\right)}\right)^{\frac{q^k-1}{r}} \\
&= \prod_{j=0}^{k-1} 1^{e_j} \left(\prod_{j=0}^{k-1} f_{e_j,Q}^{q^j}\left(P\right) \prod_{j=0}^{k-2} \frac{\ell_{e_j q^j Q,(e_{j+1}q^{j+1}+\cdots+e_{k-1}q^{k-1})Q}\left(P\right)}{v_{(e_j q^j+\cdots+e_{k-1}q^{k-1})Q}\left(P\right)}\right)^{\frac{q^k-1}{r}} \\
&= Z_e\left(Q,P\right)^{\frac{q^k-1}{r}} = a_e(Q,P)
\end{aligned}$$

The claim follows immediately from the relation $t(Q,P)^{\frac{\lambda_e(s)}{r}} = a_e(Q,P)$. □

Proof (Proof of Lemma 4). We first observe that $r = 9$ and $\varphi(k) = 2$ satisfy the above two conditions. We will show that the two curves defined by

$$r^{1/\varphi(k)} = \varphi(k), \qquad r^{1/\varphi(k)} = (\log_2 r)^{\alpha}$$

do not meet when $\varphi(k) > 2$. The above system is equivalent to

$$\begin{aligned}
r^{1/\varphi(k)} &= \varphi(k) \\
(\log_2 r)^{\alpha} &= \varphi(k)
\end{aligned}$$

The first equation is equivalent to

$$\log_2 r = \varphi(k)\log_2\varphi(k)$$

By substituting it into the second equation, we have

$$\varphi(k)^{\alpha}\left(\log_2\varphi(k)\right)^{\alpha} = \varphi(k),$$

which does not have a solution when $\varphi(k) > 2$. Thus the above two curves do not meet when $\varphi(k) > 2$. Therefore, we conclude that C_α is an infinite set. □