Miller Inversion is Easy for the Reduced Tate Pairing on Supersingular Curves of Embedding Degree Two and Three

Takakazu Satoh
e-mail: satoh.df603@gmail.com

Abstract

Let q be a power of an odd prime p. Denote the finite field of q elements by $\mathbf{F}_q$. We present a simple algorithm for Miller inversion for the reduced Tate pairing on certain supersingular elliptic curve defined over $\mathbf{F}_q$ with embedding degree 2 or 3. Let d be an embedding degree. Assume we precomputed a generator of the d-Sylow subgroup of $\mathbf{F}_q^{\times}$, which depends only on q and d. Then our algorithm runs deterministically with $O((\log q)^3)$ bit operations.

1. Introduction

Difficulty of pairing inversion is a fundamental assumption in pairing based cryptography. Duc and Jetchev[6, Sect. 5.2] gives explicit description how pairing inversions break Boneh-Franklin's IBE, Hess' IBS and Joux's tripartite key agreement protocol. More interestingly, Verheul[17] proved that the computational Diffie-Hellman problem is reduced to pairing inversion. The result is extended to asymmetric pairings by Karabina, Knapp and Menezes[12].

Galbraith, Hess and Vercauteren[9] proposed a two step pairing inversion framework. The first step is called final exponentiation inversion (FEI), while the second step is called Miller inversion (MI). In general, both steps are considered to be difficult. However, [9, Sect. 6] proposes a family of pairing friendly elliptic curves whose MI are easy. Akagi and Nogami[1] proved that MI are easy for Barreto-Naehrig curves[3] of embedding degree 12, Brezing-Weng[5] curves of embedding degree 8 and Freeman curve[7] of embedding degree 10. Assuming Bateman and Horn conjecture[4] which is plausible but unproved, we see that these families consists of infinitely many elliptic curves. The purpose of this short note is to prove that MI is easy on supersingular curves with embedding degree two or three, which form a family consisting of infinitely many curves.

Another importance of supersingular curves is as follows: Let p be a prime. Let G be a prime order subgroup of the unit group of the algebraic closure of $\mathbf{F}_p$ and let k be the smallest positive integer satisfying $G \subset \mathbf{F}_{p^k}$. Assume $3 \mid k$ and $p \equiv 5 \bmod 6$. Then the computational Diffie-Hellman problem is reduced to the reduced Tate pairing inversion problem of some supersingular curves E of embedding degree 3 over a finite extension of $\mathbf{F}_p$, provided if such E exists. Sufficient conditions for existence of such E and its construction are described in Section 2. Here we observe that a property of a single embedding degree for supersingular curves is applicable to infinitely many k. A similar property holds for the case $2 \mid k$ and $p \equiv 3 \bmod 4$.

Our algorithm and its computational complexity is described in Sections 3 and 4. For the embedding degree three case, we utilize the fact that the Frobenius endomorphism acts trivially on the Y-coordinate of some points, which keeps our algorithm simple. Similar technique is applicable to the embedding degree two case. However, we use a property of the Ate pairing due to Granger et al.[10, Theorem 2], which seems more essential.

If we exclude side-channel attacks (and use of quantum computers), FEI seems to be a very hard problem. See Vercauteren[16]. If FEI is actually a hard problem, our result has probably no impact to real world cryptography. However, Lashermes, Fournier and Goubin[13] gives a fault attack method for FEI. Although their method is intended for ordinary curves, it is also applicable to supersingular curves. Indeed, the method described in Section 4.2 of [13] is sufficient for the embedding degree two case. Thus, if one has concerns about fault attacks, final exponentiation must be so implemented that it is immune to such attacks.

Notation.

Throughout this note, an elliptic curve E is given by the Weierstrass form. The X and Y coordinate functions are denoted by ξ and η, respectively. We use $\tau := -\xi/\eta$ as a local parameter at the point $\mathcal{O}$ at the infinity of E. For a rational function f on E, we denote by $\mathrm{lc}(f)$ the leading coefficient of Laurent series expansion of f at $\mathcal{O}$ w.r.t. τ, i.e.,

$$f = \mathrm{lc}(f)\tau^m + O(\tau^{m+1})$$

where m is a order of zero of f at $\mathcal{O}$ (negative if f has a pole at $\mathcal{O}$). A rational function f is said to be normalized if $\mathrm{lc}(f) = 1$. For $\varrho \in \mathrm{End}(E)$, we define $\mathrm{lc}(\varrho) := \mathrm{lc}(\tau \circ \varrho)$. Note that $\mathrm{lc}(f)$ depends on a choice of a local parameter at $\mathcal{O}$, whereas $\mathrm{lc}(\varrho)$ does not. For an object over a field of characteristic p, we write p^n-th power Frobenius as φ_{p^n}. Finally, for $P \in E$ and $n \in \mathbf{N}$, we denote by $h_{n,P}$ the normalized n-th Miller function for P, i.e., the normalized rational function satisfying $\mathrm{div} h_{n,P} = n[P] - [nP] - (n-1)[\mathcal{O}]$.

2. Supersingular Curves

We construct some supersingular elliptic curves used in reducing certain computational Diffie-Hellman problems to pairing inversion problems. Their construction is well known or easily derived from well known results. Let p be a prime. For an integer n which is co-prime to p, we denote by μ_n the group of n-th roots of unity in $\mathbf{F}_p^a$ where $\mathbf{F}_p^a$ is an algebraic closure of $\mathbf{F}_p$. Let k be a finite extension of $\mathbf{F}_p$ and put $K := k(\mu_n)$. Let E/k be an elliptic curve. For $P \in E(K)[n]$ and $Q \in E(K)$, the n-th reduced Tate pairing is defined by

$$\langle P, Q \rangle_n := h_{n,P}(Q)^{\#(K^\times)/n}.$$

In our application, $E[n] \subset E(K)$ and it induces a bilinear pairing $E[n] \times E[n] \to \mu_n$. Let $G \subset \mathbf{F}_p^{a\times}$ be a finite subgroup of a prime order $l \geq 5$

Lemma 2.1. *Assume $p \equiv 5 \bmod 6$. Let k be the smallest positive integer satisfying $G \subset \mathbf{F}_{p^k}^\times$. Assume that k is divisible by 3. Put*

$$q' := \begin{cases} p^{k/3} & (k/3 \text{ is odd}), \\ p^{k/6} & (k/3 \text{ is even}), \end{cases}$$

and $q := q'^2$. *Then there exists a supersingular curve* $E/\mathbf{F}_q$ *satisfying the followings.*

(1) $l \mid {}^{\#}E(\mathbf{F}_q)$.

(2) $E[l] \subset E(\mathbf{F}_{q^3})$.

(3) $\mu_l \subset \mathbf{F}_{q^3}^{\times}$.

(4) $j(E) = 0$.

Proof. First we prove (1)-(3) in case that $k/3$ is odd. The assertion (3) is obvious since $q^3 = p^{2k}$. Put $t := -q'$ and $N := q - t + 1$. Since l is prime, either $l \mid q' - 1$ or $l \mid q + q' + 1 = N$. By the minimality of k, we see $l \mid N$. By Waterhouse[18, Theorem 4.1], there exists a supersingular curve $E/\mathbf{F}_q$ whose trace of the q-th power Frobenius φ_q is t. Hence ${}^{\#}E(\mathbf{F}_q) = N$, which proves (1). Suppose $l \mid q - 1$. Then, we have

$$l \mid \gcd(q-1, q+q'+1) = \gcd(q-1, q'+2) = \gcd(q-1-(q'^2-4), q'+2) = \gcd(3, q'+2) = 1,$$

a contradiction. By Balasubramanian and Koblitz[2, Theorem 1], we see (2) holds.

Next, we prove (1)-(3) in case that $k/3$ is even. Again, the assertion (3) is obvious since $q^3 = p^k$. Put $t := q$ and $N := q - t + 1$. We see l divides one of $q' - 1$, $q' + 1$, $q + t + 1$, N. However $l \mid q + t + 1$ implies $G \subset \mathbf{F}_{p^{k/2}}^{\times}$ which contradicts the minimality of k. Similarly, we see $l \nmid q' \pm 1$. Thus $l \mid N$. The existence of E and the assertion (1) follow from the same argument as above. The assertion (2) holds because

$$\gcd(q-1, q-q'+1) = \gcd(q-1, -q'+2) = \gcd(q-1-(q'^2-4), q'-2) \mid 3$$

implies $l \nmid q - 1$.

Finally, we prove (4). Let t and N be as above. Since $[q']$ is purely inseparable, there exists $\omega \in \mathrm{Aut}(E)$ satisfying $[q'] = \omega\varphi_q$. Then $\varphi_q^2 - t\varphi_q + q = 0$ in $\mathrm{End}(E)$ implies that

$$\omega^2 - \mathrm{sgn}(t)\omega + 1 = 0. \tag{2.1}$$

This shows that $\mathrm{sgn}(t)\mathrm{lc}(\omega)$ $(\in \mathbf{F}_q^{\times})$ is a primitive 6th root of unity. Therefore ${}^{\#}\mathrm{Aut}(E) = 6$, which proves $j(E) = 0$ (see e.g. Silverman[15, Sect. III.10]). □

Lemma 2.2. *Assume* $p \equiv 3 \bmod 4$. *Let* k *be the smallest positive integer satisfying* $G \subset \mathbf{F}_{p^k}^{\times}$. *Assume that* k *is divisible by 2. Put* $q := p^{k/2}$. *Then there exists a supersingular curve* $E/\mathbf{F}_q$ *satisfying the followings.*

(1) $l \mid {}^{\#}E(\mathbf{F}_q)$.

(2) $E[l] \subset E(\mathbf{F}_{q^2})$.

(3) $\mu_l \subset \mathbf{F}_{q^2}^{\times}$.

(4) $j(E) = 1728$.

Proof. Assertions (1)-(3) are proved by a similar (in fact easier) method to the proof of Lemma 2.1. We prove (4). In case that $k/2$ is odd, any elliptic curve E defined over $\mathbf{F}_q$ satisfying $j(E) = 1728$ is supersingular. We *choose* such a curve as E. In case that $k/2$ is even, the unique automorphism ω satisfying $[\sqrt{q}] = \omega\varphi_q$ satisfies $\omega^2 + 1 = 0$ in $\mathrm{End}(E)$. Hence ${}^{\#}\mathrm{Aut}(E) = 4$ and $j(E) = 1728$. □

Once we have proved $j(E)=0$ or $j(E)=1728$, we can easily construct an explicit Weierstrass model for E and its distortion map from Galbraith[8, Table IX.1] with some modifications. Just for completeness, we list them. For a field K and $n\in\mathbf{N}$, we put $K^{\neg n}:=K-\{x^n:x\in K\}$.

k	p	Weierstrass model	distortion map
$3\mid k$	$5 \bmod 6$	$Y^2=X^3+c,\ c\in\mathbf{F}_q^{\neg 3}$.	$(\gamma\zeta^p, c^{-(p-1)/2}\eta^p),\ \gamma\in\mathbf{F}_{q^3}^{\times}$ s.t. $\gamma^3=c^{-(p-1)}$.
$k\equiv 2 \bmod 4$	$3 \bmod 4$	$Y^2=X^3-cX,\ c\in\mathbf{F}_q^{\times}$.	$(-\zeta, \gamma\eta),\ \gamma\in\mathbf{F}_{q^2}^{\times}$ s.t. $\gamma^2=-1$.
$4\mid k$	$3 \bmod 4$	$Y^2=X^3-cX,\ c\in\mathbf{F}_q^{\neg 2}$.	$(c^{-(p-1)/2}\zeta^p, \gamma\eta^p),\ \gamma\in\mathbf{F}_{q^2}^{\times}$ s.t. $\gamma^2=c^{-3(p-1)/2}$.

Note that $\gamma\notin\mathbf{F}_q^{\times}$ in the all cases. Note also that powering is not a q-th power but a p-th power in the first and the third case. In the first case, the followings are equivalent: $\mathrm{Tr}(\varphi_q)=q'$, $3\mid{}^{\#}E(\mathbf{F}_q)$, $E[3](\mathbf{F}_q)\neq\{\mathcal{O}\}$, c is square in $\mathbf{F}_q$ (consider the third division polynomial).

The above table and Karabina, Knapp and Menezes[12, Theorem 3] summarizes to the following statement.

Proposition 2.3. *Let p, G, k and E be as above. Assume that $2\mid k$ and $p\equiv 3 \bmod 4$ or that $3\mid k$ and $p\equiv 5 \bmod 6$. Then, the computational Diffie-Hellman problem on G is reduced to the reduced Tate pairing inversion on E in probabilistic polynomial time with respect to ${}^{\#}G$.*

3. The case of Embedding Degree Three

In this section, we consider the Miller inversion for the case that embedding degree is three. Let p be a prime satisfying $p\equiv 5 \bmod 6$ and let q be an even power of p. We put $q':=\sqrt{q}\in\mathbf{N}$. Let t be either q' or $-q'$. Let $E/\mathbf{F}_q$ be a supersingular elliptic curve of $\mathrm{Tr}(\varphi_q)=t$, given by the *short* Weierstrass form. Define $\omega\in\mathrm{Aut}(E)$ by $[q']=\omega\varphi_q$, as in Lemma 2.1. Note $j(E)=0$ and

$$\omega = (\mathrm{lc}(\omega)^{-2}\zeta, \mathrm{lc}(\omega)^{-3}\eta) \tag{3.1}$$

(see Silverman[15, Sect. III.10] for example). Put $N:=q-t+1$ and $r:=q^3$. By Schoof[14, Lemma 4.8], $E(\mathbf{F}_q)\cong\mathbf{Z}/N\mathbf{Z}$. The embedding degree for $E[N]$ is 3. However we note that in case of $t=-q'$, the minimal embedding field in the sense of Hitt[11] is not $\mathbf{F}_r$ but $\mathbf{F}_{q^3}$.

Let l be an divisor of N, which is not necessarily a prime in this section. In case of $t\equiv 2 \bmod 3$, we further assume that l is not divisible by 3. Put $G_1:=E[l]\cap E(\mathbf{F}_q)$ and $G_0:=\{P\in E[l]:\varphi_q P=qP\}$. Then $G_1\cap G_0=\{\mathcal{O}\}$ and $E[l]=G_1\oplus G_0$ since $\gcd(q-1, l)\mid\gcd(3, t-2)$ (cf. proof of Lemma 2.1). In particular, G_0 is also a cyclic group of order l. For $A\in G_0$, observe $[q']A=\omega\varphi_q A=q\omega A$, hence $\omega^{-1}A=[q']A$ and

$$\omega^{-2}A = qA = \varphi_q A. \tag{3.2}$$

Observe that $\mathrm{lc}(\omega)^{-2}$ is a primitive cubic root of the unity (cf. (2.1) and below). Then (3.1) and (3.2) imply

$$\eta\circ\omega^{-2} = \eta, \tag{3.3}$$

$$\eta(A) \in \mathbf{F}_q \text{ for } A \in G_0-\{\mathcal{O}\} \tag{3.4}$$

and

$$\xi(\omega^{-2}A) \neq \xi(A) \text{ for } A \in G_0 - \{\mathcal{O}\}. \tag{3.5}$$

(Otherwise, $(1-\mathrm{lc}(\omega)^4)\xi(A)=0$. Hence $\xi(A)=0$ and $A \in E(\mathbf{F}_q)$, which contradicts to $G_0 \cap G_1 = \{\mathcal{O}\}$). Let ζ be a primitive 3rd root of the unity. Now we state our algorithm.

Algorithm 3.1.

Input: $v \in \mathbf{F}_r$, $A \in G_0 - \{\mathcal{O}\}$. // Note that A may not be a generator.

Output: $Q \in G_1 - \{\mathcal{O}\}$ satisfying $h_{N,A}(Q)=v$ if such Q exists. Otherwise, **nil**.

Procedure:

1: $u := v^{(1+q+q^2)(2+t)/3}$;
2: if $u \notin \mathbf{F}_q$ then return **nil** ;
3: $y_i := \eta(A) - \zeta^i u$ for $i=1, 2, 3$.
4: Build a set $L_i := \{Q \in E(\mathbf{F}_q) : \eta(Q) = y_i\}$ for $i=1, 2, 3$. // Note $0 \leq {}^{\#}L_i \leq 3$.
5: for each $Q \in L_1 \cup L_2 \cup L_3$
6: if $lQ = \mathcal{O}$ and $h_{N,A}(Q)=v$ then return Q ;
7: return **nil** ;

Before we evaluate computational complexity of our algorithm, we clarify assumptions on time complexities for operations on elements of $\mathbf{F}_q$ or $\mathbf{F}_r$. We assume that $\mathbf{F}_q$ and $\mathbf{F}_r$ are so realized that one arithmetic operation in $\mathbf{F}_q$ or $\mathbf{F}_r$ amounts to $O((\log q)^2)$ bit operations. We also assume that a generator g of 3-Sylow subgroup of $\mathbf{F}_q^{\times}$ is precomputed. This is achieved by a probabilistic algorithm which needs $O((\log q)^3)$ bit operations in average. Using g, we can deterministically compute a cubic root of a cubic element of $\mathbf{F}_q^{\times}$ with $O((\log q)^3)$ bit operations.

Theorem 3.2. *Algorithm 3.1 returns a correct result with $O((\log q)^3)$ bit operations.*

Proof. First, we prove correctness. Suppose there exists $Q \in G_1 - \{\mathcal{O}\}$ satisfying $h_{N,A}(Q)=v$. By the definition of the Miller function,

$$\begin{aligned} \mathrm{div} h_{N,A} &= N([A] - [\mathcal{O}]), \\ \mathrm{div} h_{N,\omega^{-2}A} &= N([\omega^{-2}A] - [\mathcal{O}]), \\ \mathrm{div} h_{N,\omega^{-4}A} &= N([\omega^{-4}A] - [\mathcal{O}]). \end{aligned} \tag{3.6}$$

Observe that $A + \omega^{-2}A + \omega^{-4}A = \mathcal{O}$. For A, $B \in E$, let, as usual, $L_{A,B}$ be the normalized rational function on E whose divisor is $[A]+[B]+[-(A+B)]-3[\mathcal{O}]$. Summing up both sides of (3.6), we obtain

$$\mathrm{div}(h_{N,A} h_{N,\omega^{-2}A} h_{N,\omega^{-4}A}) = N([A] + [\omega^{-2}A] + [\omega^{-4}A] - 3[\mathcal{O}]) = N \,\mathrm{div} L_{A,\omega^{-2}A}.$$

Since both functions $h_{N,A} h_{N,\omega^{-2}A} h_{N,\omega^{-4}A}$ and $L_{A,\omega^{-2}A}$ are normalized,

$$h_{N,A} h_{N,\omega^{-2}A} h_{N,\omega^{-4}A} = L_{A,\omega^{-2}A}^N.$$

By (3.5),

$$L_{A,\omega^{-2}A} = -\eta + \frac{\eta(\omega^{-2}A) - \eta(A)}{\xi(\omega^{-2}A) - \xi(A)}(\xi - \xi(A)) + \eta(A).$$

The term containing $\xi(A)$ vanishes by (3.3). Therefore

$$h_{N,A} h_{N,\omega^{-2}A} h_{N,\omega^{-4}A} = (-\eta + y)^N$$

where $y := \eta(A) = \eta(\omega^{-2}A) = \eta(\omega^{-4}A)$. Since E is defined over $\mathbf{F}_q$,

$$\varphi_q(h_{N,A}(Q)) = h_{N,\varphi_q A}(\varphi_q Q) = h_{N,\omega^{-2}A}(Q)$$

while by definition $\varphi_q h_{N,A}(Q) = h_{N,A}(Q)^q$. Taking (3.4) and $\eta(Q) \in \mathbf{F}_q$ into consideration, we obtain

$$h_{N,A}(Q)^{1+q+q^2} = (\eta(A) - \eta(Q))^{q-t+1} = (\eta(A) - \eta(Q))^{2-t}$$
$$v^{(1+q+q^2)(2+t)} = (\eta(A) - \eta(Q))^{(2-t)(2+t)} = (\eta(A) - \eta(Q))^{4-q} = (\eta(A) - \eta(Q))^3.$$

Therefore $\eta(Q)$ is either y_1, y_2 or y_3. If $\eta(Q) = y_i$ then $Q \in L_i$ by the definition of L_i. Let R be any point in $L_1 \cup L_2 \cup L_3$. A priori $R \in E(\mathbf{F}_q)$. The tests in Step 6 ensures that the algorithm terminates with an output R whenever $R \in G_1 - \{\mathcal{O}\}$ and $h_{N,A}(R) = v$. (Note that R may be different from Q.) This also implies that the algorithm reaches Step 7 only if there is no element Q in G_1 satisfying $h_{q+1,A}(Q) = v$.

Next, we evaluate computational complexity of Algorithm 3.1. Since $\frac{1+q+q^2}{3} \in \mathbf{N}$, Step 1 needs $O(\log q)$ multiplications in $\mathbf{F}_r$. For each i, we obtain L_i with $O(1)$ arithmetic operations and one cubic root computation in $\mathbf{F}_q$ (not in $\mathbf{F}_r$, which is ensured by Step 2). At Step 6, we have a point $Q \in E(\mathbf{F}_q)$. Since $G_0 \cap E(\mathbf{F}_q) = \{\mathcal{O}\}$ by the condition on l, no division by zero occurs during evaluation of $h_{N,A}(Q)$ by the Miller algorithm. Hence we obtain the value of $h_{N,A}(Q)$ with $O(\log q)$ arithmetic operations over $\mathbf{F}_r$. Thus the algorithm terminates with $O(\log q)$ arithmetic operations over $\mathbf{F}_r$ or $\mathbf{F}_q$ and at most nine cubic root computations in $\mathbf{F}_q$. By our assumptions, they amount to $O((\log q)^3)$ bit operations. □

Example 3.3. We consider the case $p := 11$, $t := 11$, $q := p^2$, $N := q - t + 1 = 111$ and $l := 37$. Let θ be the class of T in $\mathbf{F}_p[T]/\langle T^6 + T + 2\rangle$ and put $i := 5\theta^5 + 9\theta^4 + 8\theta^3 + 7\theta^2 + \theta + 6$. We see $i^2 = -1$. So, we use $\mathbf{F}_p(\theta)$ and its subfield $\mathbf{F}_p(i)$ as $\mathbf{F}_{q^3}$ and $\mathbf{F}_q$, respectively. One of the primitive third roots of unity is $\zeta := 8i + 5$. Consider $E: Y^2 = X^3 + 8i + 4/\mathbf{F}_q$. We see $^{\#}E(\mathbf{F}_q) = N$. Put $A := (8\theta^5 + \theta^4 + 4\theta^3 + 8\theta^2 + 6\theta + 3, 7i) \in G_0$ and $v := \theta^5 - \theta^4 - 2\theta^2 - \theta - 1$. Then $u := v^{63973} = 6 + 6i \in \mathbf{F}_q$ and we obtain $y_1 := 6i + 7$, $y_2 := 3i - 1$, $y_3 := i + 5$. Then $L_1 = \emptyset$, $L_2 = \emptyset$, and $L_3 = \{(1+i, y_3), (2i+8, y_3), (8i+2, y_3)\}$. The Miller algorithm gives

$$h_{N,A}(1+i, y_3) = 2\theta^4 + \theta^3 + 8\theta^2 + 6\theta,$$
$$h_{N,A}(2i+8, y_3) = 10\theta^5 + 10\theta^4 + 10\theta^3 + 5\theta^2 + 6\theta + 1,$$
$$h_{N,A}(8i+2, y_3) = \theta^5 - \theta^4 - 2\theta^2 - \theta - 1.$$

Therefore we obtain the desired answer $Q := (8i+2, i+5)$.

4. The case of Embedding Degree Two

Since the Miller inversion itself does not use a distortion map, we consider any odd prime p in this section. Let q be a power of p and put $r := q^2$. Let E be a supersingular elliptic curve over $\mathbf{F}_q$ satisfying $\mathrm{Tr}(\varphi_q) = 0$ and defined by the Weierstrass model. Such a curve exits if $p \equiv 3 \bmod 4$ or $2 // [\mathbf{F}_q : \mathbf{F}_p]$ by Waterhouse[18, Theorem 4.1]. We assume that we precomputed a generator of 2-Sylow subgroup of $\mathbf{F}_q^{\times}$. Let l be an odd number dividing $q+1$. Put $G_1 := E[l] \cap E(\mathbf{F}_q)$ and $G_0 := \{P \in E[l] : \varphi_q(P) = qP\}$. By Schoof[14, Lemma 4.8], $E(\mathbf{F}_r) = E[q+1]$ and $E(\mathbf{F}_q)$ is isomorphic to either $\mathbf{Z}/(q+1)\mathbf{Z}$ or

$\mathbf{Z}/\left(\frac{q+1}{2}\right)\mathbf{Z}\oplus\mathbf{Z}/2\mathbf{Z}$. We have $G_0\cap G_1=\{\mathcal{O}\}$ since l is odd. In stead of (3.2), we have

$$\varphi_q A = -A$$

which implies $\xi(A)\in\mathbf{F}_q$ for $A\in G_0$ in the embedding degree two case. Our algorithm for embedding degree two curves is as follows:

Algorithm 4.1.
Input: $v\in\mathbf{F}_r$, $A\in G_0-\{\mathcal{O}\}$. // Note that A may not be a generator.
Output: $Q\in G_1-\{\mathcal{O}\}$ satisfying $h_{q+1,A}(Q)=v$ if such Q exists. Otherwise, **nil**.
Procedure:
1: $u:=v^{(q+1)/2}$;
2: if $u\notin\mathbf{F}_q$ then return **nil** ;
3: $x_1:=\xi(A)+u$; $x_2:=\xi(A)-u$;
4: Build a set $L_i:=\{Q\in E(\mathbf{F}_q):\xi(Q)=x_i\}$ for $i=1,2$. // Note $0\le{}^{\#}L_i\le 2$.
5: for each $Q\in L_1\cup L_2$
6: if $lQ=\mathcal{O}$ and $h_{q+1,A}(Q)=v$ then return Q ;
7: return **nil** ;

Theorem 4.2. *Algorithm 4.1 returns a correct result with $O((\log q)^3)$ bit operations.*

Proof. First, we prove correctness. Suppose there exists $Q\in G_1-\{\mathcal{O}\}$ satisfying $h_{q+1,A}(Q)=v$. Recall that E is defined by the Weierstrass model. Since $A\in G_0\subset E[q+1]$, we have

$$h_{q+1,A} = (\xi-\xi(A))h_{q,A}. \tag{4.1}$$

Now key observation of our algorithm is $h_{q,A}(Q)\in\mu_l\subset\mu_{q+1}$ by Granger et al.[10, Theorem 2]. Thus evaluation of (4.1) at Q followed by $q+1$ powering yields

$$v^{q+1} = (\xi(Q)-\xi(A))^{q+1}. \tag{4.2}$$

That is, we do not need the value $h_{q,A}(Q)$ at all. Since $Q\in E(\mathbf{F}_q)-\{\mathcal{O}\}$, we have $\xi(Q)\in\mathbf{F}_q$. On the other hand $A\in G_0-\{\mathcal{O}\}$ implies $\xi(A)=\varphi_q(\xi(A))$. Thus $\xi(A)\in\mathbf{F}_q$. Therefore $\xi(Q)-\xi(A)\in\mathbf{F}_q$ and $(\xi(Q)-\xi(A))^{q+1}=(\xi(Q)-\xi(A))^2$. Substituting the right side of (4.2), we obtain

$$v^{q+1} = (\xi(Q)-\xi(A))^2. \tag{4.3}$$

Recall that q is odd. Hence

$$\xi(Q)-\xi(A) = \pm v^{(q+1)/2}.$$

Therefore $\xi(Q)$ is either x_1 or x_2. Since l is odd, $G_0\cap E(\mathbf{F}_q)=\{\mathcal{O}\}$. The rest of proof of correctness and a proof for computational complexity are similar to the proof of Theorem 3.2. □

Remark 4.3. In case that q is a power of 2, the algorithm and its implementation are in fact easier because (4.3) yields a unique candidate of Q. However in cryptographic point of view, this case is irrelevant.

Example 4.4. Consider $E: Y^2=X^3-13X-7$ over $\mathbf{F}_{139}$ and take $l:=35$. Let θ be the class of T in $\mathbf{F}_{139}[T]/\langle T^2+4\rangle$. Then $\mathbf{F}_{139^2}=\mathbf{F}_{139}(\theta)$. Put $A:=(67,38\theta)$ and $v:=25\theta+109$. Note that $\langle A\rangle=G_0$ and that v^{138} is a primitive 35-th root of unity. Then $u:=v^{70}=131$

and we obtain $x_1 := 59$ and $x_2 := 75$. Thus $L_1 := \{(59, \pm 54)\}$ and $L_2 := \{(75, \pm 1)\}$. The Miller algorithm gives $h_{140,A}((59, 54)) = 114\theta + 109$, $h_{140,A}((59, -54)) = 25\theta + 109$, $h_{140,A}((75, 1)) = 112\theta + 22$ and $h_{140,A}((75, -1)) = 27\theta + 22$. Therefore we obtain the desired answer $Q := (59, -54)$.

We observe an example for a non-generator. Put $B := 5A$ and $v := 56\theta + 55$ whose orders are both 7. There are five points $Q_n := (83, 55) + n(69, 11) \in G_1$, where $0 \le n < 5$, satisfying $e_{140}(B, Q_n) = v$. Although the paring values are equal, the algorithm requires correct input from FEI, which are different for each n. For example, the algorithm returns unique point Q_0 for input $(4\theta + 135, B)$, whereas it returns unique point Q_1 for input $(98\theta + 41, B)$. It is a role of FEI to provide a correct value to Algorithm 4.1.

Acknowledgments. The author would like to thank Frederik Vercauteren and Steven Galbraith for their comments.

References

1. Akagi, S. and Nogami, Y.: Exponentiation inversion problem reduced from fixed argument pairing inversion on twistable Ate pairing and its difficulty, Advances in Information and Computer Security. IWSEC 2014, Lect. Notes in Comput. Sci., **8639**, 240-249, ed. Yoshida, M. and Mouri, K., Springer, 2014. doi: 10.1007/978-3-319-09843-2_18
2. Balasubramanian, R. and Koblitz, N.: The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. J. Cryptology, **11**, 141-145 (1998).
3. Barreto, P.S.L.M. and Naehrig, M.: Pairing-friendly elliptic curves of prime order, SAC 2005, Lect. Notes in Comput. Sci., **3897**, 319-331, Berlin, Heidelbert: Springer, 2006.
4. Bateman, P.T. and Horn, R.A.: A heuristic asymptotic formula concerning the distribution of prime numbers. Math. Comp., **16**, 363-367 (1962).
5. Brezing, F. and Weng, A.: Elliptic curves suitable for pairing based cryptography. Des. Codes Crypt., **37**, 133-141 (2005). doi: 10.1007/s10623-004-3808-4
6. Duc, A. and Jetchev, D.: Hardness of computing individual bits for one-way functions on elliptic curves, Crypto 2012, Lect. Notes in Comput. Sci., **7417**, 832-849, ed. Safavi-Naini, R. and Canetti, R., Berlin, Heidelberg: Springer, 2012. doi: 10.1007/978-3-642-32009-5_48
7. Freeman, D.: Constructing pairing-friendly elliptic curves with embedding degree 10, Algorithmic Number Theory, Proc. 7th Internat. Sympo, ANTS-VII, Berlin, Germany, July 23-28, 2006, Lect. Notes in Comput. Sci., **4076**, 452-465, 2006. doi: 10.1007/11792086_32
8. Galbraith, S.: Pairings, Advances in elliptic curve cryptography, Chap. 9, London math. soc. lect. note series, **317**, ed. Blake, I.F., Seroussi, G. and Smart, N.P., Cambridge: Cambride University Press, 2005.
9. Galbraith, S., Hess, F. and Vercauteren, F.: Aspects of Pairing inversion. IEEE Trans. Info. Theory, **54**, 5719-5728 (2008). doi: 10.1109/TIT.2008.2006431
10. Granger, R., Hess, F., Oyono, R., Thériault, N. and Vercauteren, F.: Ate pairing on hyperelliptic curves, Advances in Cryptology - EUROCRYPT 2007, Lect. Notes in Comput. Sci., **4515**, 430-447, ed. Naor, M., Springer, 2007. doi: 10.1007/978-3-540-72540-4_25
11. Hitt, L.: On the minimal embedding field, Pairing-based cryptography – Pairing 2007, Lect. Notes in Comput. Sci., **4575**, 294-301, Berlin, Heidelberg: Springer, 2007. doi: 10.1007/978-3-540-73489-5_16
12. Karabina, K., Knapp, E. and Menezes, A.: Generalizations of Verheul's theorem to asymmetric pairings. Adv. Math. Comm., **7**, 103-111 (2013). doi: 10.3934/amc.2013.7.103
13. Lashermes, R., Fournier, J. and Goubin, L.: Inverting the final exponentiation of Tate pairings on ordinary elliptic curves using faults., CHES 2013, Lect. Notes in Comput. Sci., **8086**, 365-382, ed. Bertoni, G. and Coron, J.-S., Springer, 2013. doi: 10.1007/978-3-642-40349-1_21
14. Schoof, R.: Nonsingular plane cubic curves over finite fields. J. Combinatorial theory, Ser. A, **46**, 183-211 (1987). doi: 10.1016/0097-3165(87)90003-3
15. Silverman, J. H.: The arithmetic of elliptic curves. GTM, 106. Berlin-Heidelberg-New York: Springer 1986.

16. Vercauteren, F.: The hidden root problem, Paring-based cryptography 2008, Lect. Notes in Comput. Sci., **5209**, 89-99, Berlin, Heidelberg: Springer, 2008. doi: 10.1007/978-3-540-85538-5
17. Verheul, E.R.: Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. J. Cryptology, **17**, 277-296 (2004). doi: 10.1007/s00145-004-0313-x
18. Waterhouse, W.C.: Abelian varieties over finite fields. Ann. Scient. Éc. Norm. Sup., **2**, 521-560 (1969).