On a Relation between the Ate Pairing and the Weil Pairing for Supersingular Elliptic Curves

Takakazu Satoh

e-mail: satoh.df603@gmail.com

Abstract

The hyperelliptic curve Ate pairing provides an efficient way to compute a bilinear pairing on the Jacobian variety of a hyperelliptic curve. We prove that, for supersingular elliptic curves with embedding degree two, square of the Ate pairing is nothing but the Weil pairing. Using the formula, we develop an X-coordinate only pairing inversion method. However, the algorithm is still infeasible for cryptographic size problems.

1. Introduction

In [3, Theorem 2], Granger et al. introduced the Ate pairing for hyperelliptic curves. For a supersingular elliptic curve $E/\mathbf{F}_q$ with $^{\#}E(\mathbf{F}_q)=q+1$, the pairing in the form [3, Lemma 6] is stated as follows: Let σ_q be the q-th power Frobenius endomorphism and let r be the maximal odd divisor of $q+1$. Put $G_1 := E(\mathbf{F}_q)[r]$ and $G_0 := \{A \in E[r] : \sigma_q(A) = -A\}$. Note that the embedding degree for r is two. Let $h_{q,A}$ be the q-th Miller function for A. Then the hyperelliptic ate pairing a under this setting is defined as

$$a(Q,A) := h_{q,A}(Q)$$

where $Q \in G_1 - \{\mathcal{O}\}$, $A \in G_0$. Note this is different from the elliptic curve Ate pairing defined in Hess, Smart and Vercauteren [5, Theorem 1]. The Ate pairing a_q defined in Hess [4, Sect. 2.2] is a^2 (it is intended for ordinary elliptic curves but the definition makes sense for supersingular elliptic curves).

Let e_{q+1} be the $(q+1)$-st Weil pairing. The main result of this paper is

$$e_{q+1}(Q,A) = h_{q,A}(Q)^2. \tag{1.1}$$

Therefore

$$e_{q+1}(Q,A) = a(A,Q)^2 = a_q(A,Q). \tag{1.2}$$

Of course, a bilinear pairing on two cyclic groups is unique up to constant power. Hess[4] and Vercauteren[12] give systematic constructions of such a simplified formula for pairings. What (1.2) asserts is that we determined the constant. We further show

$$e_{q+1}\left(Q, \frac{r+1}{2}A\right) = h_{q,A}(Q). \tag{1.3}$$

The proof of (1.1) is divided into two steps. The first step is to explicitly describe the Weil pairing in terms of group extensions, which is valid for any elliptic curve.[1] Let m be an integer prime to q. Let $A \in E[m]$ and take a (random point) $S \in E$. Let f be a symmetric rational factor system on E with values in $\mathbf{G}_{\mathrm{m}}$ associated to the divisor $\Pi := [A+S]-[S]$ in the sense of Serre[10, VII.16, Remark]. We normalize f so that $f(\mathcal{O}, \mathcal{O}) = 1$. The factor system f introduces a (rational) binomial operation $\underset{f}{+}$ on the product $E \times \mathbf{G}_{\mathrm{m}}$ by

$$(P, x) \underset{f}{+} (Q, y) \;:=\; (P+Q, xyf(P,Q)). \tag{1.4}$$

We denote this "rational" group by $E \underset{f}{*} \mathbf{G}_{\mathrm{m}}$. (It is birationally equivalent to an algebraic group (see Serre[10, VII.4, Prop. 4]) but we work on the rational group in view of implementation efficiency.) Since $m\Pi$ is principal, $E \underset{f^m}{*} \mathbf{G}_{\mathrm{m}}$ is a trivial extension. More explicitly, it holds that

$$f^m(P, Q) \;=\; \frac{h_{m,\Pi}(P)h_{m,\Pi}(Q)}{h_{m,\,\Pi}(P+Q)}$$

where $h_{m,\Pi} := h_{m,A+S}/h_S$. Thus

$$\begin{tikzcd}
0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, equal] & E \times \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, "C_1"] & E \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, equal] & E \underset{f^m}{*} \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, "C_2"] & E \arrow[r] \arrow[d, "m_E"] & 0 \\
0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] & E \underset{f}{*} \mathbf{G}_{\mathrm{m}} \arrow[r] & E \arrow[r] & 0
\end{tikzcd} \tag{1.5}$$

commutes where

$$\begin{aligned} C_1(P, x) \;&:=\; (P, x/h_{m,\Pi}(P)), \\ C_2(P, x) \;&:=\; m_f(P, 1) \underset{f}{+} (\mathcal{O}, x). \end{aligned}$$

Here, m_f is the m-times map with respect to $\underset{f}{+}$. If $Q \in E[m]$, then $C_2(C_1(Q, 1))$ is also an m torsion element of $E \underset{f}{*} \mathbf{G}_{\mathrm{m}}$ because C_1 and C_2 are group homomorphisms. By (1.4), the fist component of $C_2(C_1(Q, 1))$ is $\mathcal{O}$. Note that $x \to (\mathcal{O}, x)$ is an injective group homomorphism from $\mathbf{G}_{\mathrm{m}}$ to $E \underset{f}{*} \mathbf{G}_{\mathrm{m}}$. Thus we obtained a group homomorphism $E[m] \to \mu_m$. We will show this give rise to the Weil pairing (Remark 3.5).

---

[1] Probably, the first step is already known to the experts. However, the author could not find a proof in open literatures. Eventually, our proof of the first step is to write the well known isomorphism $\mathrm{Pic}^0(E) \to \mathrm{Ext}(E, \mathbf{G}_{\mathrm{m}})$ and an inclusion $\mathrm{Hom}(E[m], \mathbf{G}_{\mathrm{m}}) \to \mathrm{Ext}(E, \mathbf{G}_{\mathrm{m}})$ (cf. Milne[8, Prop. 11.3]) so explicitly that we can construct a pairing computation algorithm.

In the second step, we simplify the formula obtained in the first step. Note that a group operation is associative. One can evaluate m_f with $O(\log_2 m)$ evaluations of $\underset{f}{+}$. This eventually results in a usual Weil pairing computation algorithm. However, we decompose $(q+1)_f$ as $q_f \underset{f}{+} 1_f$. In computing q times map, we take advantage of supsersingularity and the embedding degree being 2 (i.e. $r \mid q+1$).

Using (1.3), we make a slight improvement to the pairing inversion algorithm due to Galbraith, Ó hÉigartaigh and Sheedy[2]. They gave an algorithm to compute the eta pairing on supersingular hyperelliptic curve with the final exponentiation raising to the power -2. Using the algorithm, the proposed a multivariate attack on the pairing inversion problems. Our method is only applicable to supersingular elliptic curves of embedding degree two. However, we have only to find a zero of a polynomial defined over a smaller field in the following sense. Let z be a given r-th root of the unity and consider to find $Q \in G_1$ satisfying $h_{q,A}(Q) = z$. We construct $U_{A,z}(X) \in \mathbf{F}_q[X]$, rather than $\mathbf{F}_{q^2}[X]$, of degree approximately $q/2$ from $h_{q,A}$ and $\mathrm{Tr}_{\mathbf{F}_{q^2}/\mathbf{F}_q}(z)$ such that one of $\mathbf{F}_q$-solutions of $U_{A,z}(X) = 0$ gives the X-coordinate of Q. Although the computational complexity of our method is smaller than that of [2], it is still infeasible. It might be worth to mention that Kanayama and Okamoto[6], Kim and Cheon[7] and Chang, Hong, Lee and Lee[1] reduce the difficulty of pairing inversion problems to the difficulty of final exponentiation inversions.

The rest of the paper is organized as follows. In Section 2, we briefly review mathematical backgrounds on group extensions. In Section 3, we perform the first step described as above. In Section 4, we perform the second step and prove (1.1) and (1.3). In Section 5, we discuss some application of (1.3) to pairing inversion.

Acknowledgments. The author would like to thank Frederik Vercauteren, Steven Galbraith and Yuuichiro Taguchi for comments and/or discussions.

Notation: Throughout the paper, p denotes a prime and N is a positive integer. We put $q := p^N$. The q-th power Frobenius map is denoted by σ_q. Divisors mean the Weil divisors. (Since we will work only on nonsingular varieties, we identify them with the Cartier divisors.) Let k be a perfect field. An elliptic curve E/k is defined by the Weierstrass equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{1.6}$$

with $a_1, \ldots, a_6 \in k$. In Sections 4 and 5, we assume that E is defined over $\mathbf{F}_q$ and that ${}^{\#}E(\mathbf{F}_q) = q+1$ unless otherwise noted. Note that this implies that E is supersingular. 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. We say a rational function f on E is **normalized** if the leading coefficient $\mathrm{lc}(f)$ of the Laurent expansion of f with respect to τ is 1. For $\varphi \in \mathrm{End}(E)$, we define

$$\mathrm{lc}(\varphi) := \mathrm{lc}(\tau \circ \varphi). \tag{1.7}$$

For $n \in \mathbf{Z}$ and $P \in E$, we define the **Miller function** $h_{n,P}$ as the normalized function satisfying

$$\mathrm{div} h_{n,P} = n[P] - [nP] - (n-1)[\mathcal{O}]. \tag{1.8}$$

For $P \in E$, we denote the translation by P map by t_P:

$$t_P(Q) := Q+P. \tag{1.9}$$

For P, $Q \in E$, we denote by $L_{P,Q}$ the normalized function satisfying

$$\mathrm{div} L_{P,Q} = [P]+[Q]+[-P-Q]-3[\mathcal{O}]$$

and put $V_P := L_{P,-P}$. Explicitly, $V_P = \xi - \xi(P)$ for $P \neq \mathcal{O}$. For $n \in \mathbf{N}$, we define

$$\varepsilon(n) := \begin{cases} 1 & \text{if } \mathrm{char}(k) = 0, \\ p^e & \text{if } \mathrm{char}(k) = p \geq 2 \text{ and } E \text{ is ordinary}, \\ p^{2e} & \text{if } \mathrm{char}(k) = p \geq 2 \text{ and } E \text{ is supersingular}, \end{cases} \tag{1.10}$$

where $n = p^e n'$ with $\gcd(p, n') = 1$.

2. Factor Systems

We summarize some properties on group extensions which are used in the later sections. Further details can be found in Serre [10, Chap. VII]. See also Milne [8, Sect. 11 and 16]. Let k be a perfect field and let E be an elliptic curve defined over k. A symmetric rational factor system on E with values in $\mathbf{G}_{\mathrm{m}}$ is a rational function f on $E \times E$ satisfying $f(P, Q) = f(Q, P)$ and

$$\frac{f(Q, R) f(P, Q+R)}{f(P+Q, R) f(P, Q)} = 1 \tag{2.1}$$

as a rational function on $(P, Q, R) \in E^3$. The abelian group consisting of such functions are denoted by $Z^2(E, \mathbf{G}_{\mathrm{m}})$. For $n \geq 1$, let $C^n(E, \mathbf{G}_{\mathrm{m}})$ be the abelian group of rational functions on E^n. We define $\delta \in \mathrm{Hom}(C^1(E, \mathbf{G}_{\mathrm{m}}), C^2(E, \mathbf{G}_{\mathrm{m}}))$ by

$$(\delta g)(P, Q) := g(P) g(Q) / g(P+Q) \tag{2.2}$$

and put $B^2(E, \mathbf{G}_{\mathrm{m}}) := \delta(C^1(E, \mathbf{G}_{\mathrm{m}}))$. It is easy to see that $B^2(E, \mathbf{G}_{\mathrm{m}})$ is a subgroup of $Z^2(E, \mathbf{G}_{\mathrm{m}})$.

In case that f is regular at $(\mathcal{O}, \mathcal{O})$ and $(\mathcal{O}, P)$ for $P \in E$,

$$f(\mathcal{O}, P) = f(P, \mathcal{O}) = f(\mathcal{O}, \mathcal{O}) \tag{2.3}$$

by (2.1). We say a factor system f is normalized if f is regular at $(\mathcal{O}, \mathcal{O})$ and $f(\mathcal{O}, \mathcal{O}) = 1$. Let $f \in Z^2(E, \mathbf{G}_{\mathrm{m}})$ be a normalized factor system. Then, we obtain the following exact sequence:

$$0 \to \mathbf{G}_{\mathrm{m}} \xrightarrow{x \to (\mathcal{O}, x)} E \underset{f}{*} \mathbf{G}_{\mathrm{m}} \xrightarrow{(P, x) \to P} E \to 0$$

where $E \underset{f}{*} \mathbf{G}_{\mathrm{m}}$ is a rational group whose underlying set is $E \times \mathbf{G}_{\mathrm{m}}$ and whose group operation $\underset{f}{+}$ is defined by

$$(P, x) \underset{f}{+} (Q, y) := (P + Q, xyf(P, Q)).$$

Let f, g and h be normalized symmetric rational factor systems. Assume that we have commutative diagrams

$$\begin{tikzcd} 0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, equal] & E \underset{f}{*} \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, "\Phi"] & E \arrow[r] \arrow[d, "\varphi"] & 0 \\ 0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] & E \underset{h}{*} \mathbf{G}_{\mathrm{m}} \arrow[r] & E \arrow[r] & 0 \end{tikzcd}$$

and

$$\begin{tikzcd} 0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, equal] & E \underset{g}{*} \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, "\Psi"] & E \arrow[r] \arrow[d, "\psi"] & 0 \\ 0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] & E \underset{h}{*} \mathbf{G}_{\mathrm{m}} \arrow[r] & E \arrow[r] & 0. \end{tikzcd}$$

Then we see

$$\begin{tikzcd} 0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, equal] & E \underset{fg}{*} \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, "\Gamma"] & E \arrow[r] \arrow[d, "\varphi + \psi"] & 0 \\ 0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] & E \underset{h}{*} \mathbf{G}_{\mathrm{m}} \arrow[r] & E \arrow[r] & 0 \end{tikzcd} \tag{2.4}$$

where $\Gamma(P, x) := \Phi(P, 1) \underset{h}{+} \Psi(P, 1) \underset{h}{+} (\mathcal{O}, x)$ commutes. For $m \in \mathbf{N}$, let m_f be the m-times map on $E \underset{f}{*} \mathbf{G}_{\mathrm{m}}$. Put $\Lambda_m(P, x) = m_f(P, 1) \underset{f}{+} (\mathcal{O}, x)$. Using induction on $m \in \mathbf{N}$ to (2.4), we see that the following diagram commutes:

$$\begin{tikzcd} 0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, equal] & E \underset{f^m}{*} \mathbf{G}_{\mathrm{m}} \arrow[r] \arrow[d, "\Lambda_m"] & E \arrow[r] \arrow[d, "m_E"] & 0 \\ 0 \arrow[r] & \mathbf{G}_{\mathrm{m}} \arrow[r] & E \underset{f}{*} \mathbf{G}_{\mathrm{m}} \arrow[r] & E \arrow[r] & 0. \end{tikzcd}$$

Explicitly,

$$\Lambda_m(P, x) = \left(mP, x \prod_{n=1}^{m-1} f(P, nP) \right). \tag{2.5}$$

Let π_1, $\pi_2 : E\times E \to E$ be the projection to the first and the second component, respectively and let $s : E\times E \to E$ be the sum on E. By definition (see Milne [8, Sect. 9]),

$$\mathrm{Pic}^0(E) \;=\; \{\, d \in \mathrm{Pic}(E) \;:\; (\pi_1^* + \pi_2^* - s^*)(d) \;=\; 0\,\}.$$

For $P \in E$, the divisor class $\overline{[P]-[\mathcal{O}]} \in \mathrm{Pic}(E)$ in fact belongs to $\mathrm{Pic}^0(E)$. Indeed, we construct a rational function f_P on $E\times E$ satisfying

$$\mathrm{div}(f_P) \;=\; (\pi_1^* + \pi_2^* - s^*)([P] - [\mathcal{O}]). \tag{2.6}$$

Note that (2.6) determines f_P uniquely up to constant multiple and that, if such a f_P exists, f_P is a rational symmetric factor system. See Serre [10, VII.§3.16]. However, f_P is not normalized.

Theorem 2.1. *Let $P \in E - E[2]$. Define a rational function f_P on $E\times E$ by*

$$f_P(Q, R) \;:=\; L_{P,-Q}(R)/V_{P-Q}(R). \tag{2.7}$$

(i) *The function f_P satisfies (2.6).*

(ii) *Let z and w be the local parameter at $\mathcal{O}$ for Q and R, respectively. Let $\mathscr{E}$ be the formal group law associated to E. Then, expansion of f_P at $(\mathcal{O}, \mathcal{O})$ is*

$$f_P(Q,R) \;=\; \frac{\mathscr{E}(w, z)}{wz}(1 + O(z^2, zw, w^2)). \tag{2.8}$$

(iii) *Let $T \in E - \{\mathcal{O}, \pm P\}$. Put $z_{-T} := z\circ t_T$ and $w_T := w\circ t_{-T}$. (See (1.9) for the definition of t. Note that z_{-T} and w_T are local parameters of Q at T and R at $-T$.) Then, around $(-T, T)$, it holds that*

$$f_P(Q, R) \;=\; \mathscr{E}(z_{-T}, w_T)(\xi(P) - \xi(T) + O(z_{-T}, w_T)). \tag{2.9}$$

Proof. All claims follow from checking whether the Laurent series expansion of f_P has a correct leading term for the (Cartier divisor corresponding to the Weil) divisor $(\pi_1^*+\pi_2^*-s^*)([P]-[\mathcal{O}])$ at all (closed) points of $E\times E$. The computation is standard (but quite lengthy), hence omitted. □

Remark 2.2. For $Q \neq \mathcal{O}$, P, we can easily check

$$\begin{aligned}
\mathrm{div} f_P(Q, \cdot) \;&=\; ((\pi_1^* + \pi_2^* - s^*)([P] - [\mathcal{O}]))\,|_{\{Q\}\times E} \\
&=\; [P] + [\mathcal{O}] - ([P-Q] - [-Q]) \\
&=\; \mathrm{div}(L_{P,-Q}/V_{P-Q}).
\end{aligned}$$

This does *not* imply (2.6). For a counter example, let $P \in E$ be of finite order of $m > 1$. If (2.6) holds, then a function $\widetilde{f}_P(Q, R) := f_P(Q, R)h_{m,P}(Q)$ also satisfies

$$\mathrm{div}(\widetilde{f}_P(Q, \cdot)) \;=\; \mathrm{div}(L_{P,-Q}/V_{P-Q})$$

for all $Q \neq \mathcal{O}, P$. Apparently, $\widetilde{f}_P$ does not satisfy (2.6).

Remark 2.3. In case of $k = \mathbf{F}_q$, we briefly observe how certain factor systems give rise to a group homomorphism from $E(\mathbf{F}_q)$ to $\mathbf{G}_{\mathrm{m}}$. Put $\Gamma := E(\mathbf{F}_q)$ for simplicity. Let $r \in \mathbf{N}$. Take A, $B \in E$ of order r satisfying $\sigma_q(A) = qA$ and $\sigma_q(B) = qB$. Put $\Phi := (f_A/f_B)^r$ and $\varphi := h_{r,A}/h_{r,B}$. Then Φ is a normalized symmetric rational factor system by (2.8) and we see $\Phi = \delta\varphi$. For any Q, $R \in \Gamma - \{\mathcal{O}\}$, we have $f_A^q(Q, R) = \sigma_q(f_A(Q, R)) = f_{qA}(Q, R)$ and $f_B^q(Q, R) = f_{qB}(Q, R)$. Now write $r = \sum_{i=0}^{n} a_i q^i$ with some $n \in \mathbf{N}$ and $a_i \in \mathbf{Z}$. Put $\Psi := \prod_{i=0}^{n} (f_{q^iA}/f_{q^iB})^{a_i}$. Using (2.3) for the case $Q = \mathcal{O}$ or $R = \mathcal{O}$, we obtain

$$\Phi|_{\Gamma\times\Gamma} = \Psi|_{\Gamma\times\Gamma}. \tag{2.10}$$

Note $D := \sum_{i=0}^{n} a_i([q^iA] - [q^iB])$ is principal. Construct a normalized rational function ψ satisfying $\operatorname{div}\psi = D$. Then $\Psi = \delta\psi$. Therefore (2.10) implies $\delta(\varphi/\psi)|_{\Gamma\times\Gamma} = 1$, hence $\varphi/\psi \in \mathrm{Hom}(E(\mathbf{F}_q), \mathbf{G}_{\mathrm{m}})$. Of course determination of $\mathrm{Ker}(\varphi/\psi)$ is another story and needs more fine arguments.

3. The Weil Pairing

In this section, we study connection between the Weil pairing and the diagram (1.5). As was in the previous section, E denotes an elliptic curve defined over a perfect field k. Let $P \in E - \{\mathcal{O}\}$ and let f_P be a factor system defined by (2.7). Define $i_n : E \to E \times E$ by $i_n(Q) = (Q, nQ)$.

Definition 3.1. (Silverman[11, Sect. 3.8]) Let $m \geq 1$ be an integer. In case of $\mathrm{char}(k) \geq 2$, we assume that m is prime to $\mathrm{char}(k)$. For $P \in E[m]$, define a normalized function $g_{m,P}$ by $\operatorname{div} g_{m,P} = m_E^*([P] - [\mathcal{O}])$. For a given $Q \in E[m]$, take any $S \in E$ such that $g_{m,P}$ is regular and non-zero at both $Q{+}S$ and S. The m-th Weil pairing e_m is defined by

$$e_m(Q, P) = g_{m,P}(Q + S)/g_{m,P}(S).$$

Now we study (2.5) for $f = f_P$ more closely.

Lemma 3.2. *For $m \geq 1$ and $P \in E$, it holds that* $\mathrm{lc}\left(\prod_{n=1}^{m-1} (f_P \circ i_n)\right) = \mathrm{lc}(m_E)$. *(See (1.7) for the definition of* lc *for an endomorphism).*

Proof. Recall that we use $\tau := -\xi/\eta$ for a local parameter on E at $\mathcal{O}$. By (2.8), $f_P \circ i_n = \dfrac{\tau \circ (n+1)_E}{\tau \cdot \tau \circ n_E}(1 + O(\tau))$. Thus, $\prod_{n=1}^{m-1} (f_P \circ i_n) = \dfrac{\tau \circ m_E}{\tau^m}(1 + O(\tau))$. The assertion is now obvious. □

Lemma 3.3. *For $m \in \mathbf{N}$ and $P \in E$, we define*

$$F_{m,P} := \mathrm{lc}(m_E)^{-1} \prod_{n=1}^{m-1} (f_P \circ i_n).$$

Let $g_{m,P}$ *be the normalized rational function on* E *satisfying*

$$\operatorname{div}(g_{m,P}) = -[mP]+[\mathcal{O}]+m_E^*([P]-[\mathcal{O}]).$$

(Note this is compatible to Definition 3.1.) Then,

$$F_{m,P} = h_{m,P}/g_{m,P}, \tag{3.1}$$

where $h_{m,P}$ *is the Miller function (1.8).*

Proof. Note that $h_{m,P}$ and $g_{m,P}$ are normalized by definition. So is $F_{m,P}$ by Lemma 3.2. Thus we have only to show $\operatorname{div} F_{m,P} = \operatorname{div} h_{m,P} - \operatorname{div} g_{m,P}$. By (2.6),

$$\begin{aligned}\operatorname{div}(f_P \circ i_n) &= i_n^*(\operatorname{div} f_P) = i_n^*\pi_1^*([P]-[\mathcal{O}]) + i_n^*\pi_2^*([P]-[\mathcal{O}]) - i_n^* s^*([P]-[\mathcal{O}]) \\ &= \mathrm{id}^*([P]-[\mathcal{O}]) + n_E^*([P]-[\mathcal{O}]) - (n+1)_E^*([P]-[\mathcal{O}]).\end{aligned}$$

Hence for $m \geq 2$,

$$\begin{aligned}\operatorname{div}(F_{m,P}) &= \sum_{n=1}^{m-1} \operatorname{div}(f_P \circ i_n) = m([P]-[\mathcal{O}]) - m_E^*([P]-[\mathcal{O}]) \\ &= m[P]-[mP]-(m-1)[\mathcal{O}]+[mP]-[\mathcal{O}]-m_E^*([P]-[\mathcal{O}]) \\ &= \operatorname{div} h_{m,P} - \operatorname{div} g_{m,P}.\end{aligned}$$

□

Theorem 3.4. *Let* $\operatorname{char}(k) \nmid m$. *Let* $P \in E[m]$. *Take* $S \in E - E[2]$ *satisfying* $P+S \notin E[2]$. *Put* $\Pi := [P+S]-[S] \in \operatorname{Div}(E)$ *and put*

$$F_{m,\Pi} := F_{m,P+S}/F_{m,S}, \qquad h_{m,\Pi} := h_{m,P+S}/h_{m,S}.$$

Then,

$$F_{m,\Pi}(Q)/h_{m,\Pi}(Q) = e_m(P,Q)$$

for all $Q \in E[m]$ *at which* $F_{m,\Pi}$ *and* $h_{m,\Pi}$ *are regular and non-zero.*

Proof. We also define

$$f_\Pi := f_{P+S}/f_S, \; h_{m,\Pi} := h_{m,P+S}/h_{m,S}.$$

Note f_Π is a symmetric rational factor system associated to Π. By (2.8), f_Π is normalized. It is easy to verify

$$F_{m,\Pi} = \prod_{n=1}^{m-1} (f_\Pi \circ i_n) \tag{3.2}$$

and

$$F_{m,\Pi} = h_{m,\Pi}/g_{m,\Pi}. \tag{3.3}$$

We choose and fix P_m and $S_m \in E$ satisfying $mP_m = P$ and $mS_m = S$. Since $mP = \mathcal{O}$ and $\mathrm{char}(k) \nmid m$,

$$\begin{aligned}\operatorname{div} g_{m,P} &= \sum_{T \in E[m]} ([P_m + T] - [T]),\\ \operatorname{div} g_{m,\Pi} &= \sum_{T \in E[m]} ([P_m + S_m + T] - [S_m + T]) = \operatorname{div}(g_{m,P} \circ t_{-S_m}).\end{aligned}$$

(Recall that t_{-S_m} is the translation by $-S_m$ map, cf. (1.9).) Since $S \neq \mathcal{O}$ and $S \neq -P$, the rational function $g_{m,P}$ is regular and non-zero at $-S_m$. On the other hand, $g_{m,\Pi}$ is normalized. Therefore

$$g_{m,\Pi} = \frac{1}{g_{m,P}(-S_m)} g_{m,P} \circ t_{-S_m}.$$

If $g_{m,\Pi}$ is regular at Q, we have

$$g_{m,\Pi}(Q) = \frac{g_{m,P}(Q - S_m)}{g_{m,P}(-S_m)} = e_m(Q, P) \tag{3.4}$$

by Definition 3.1. The assertion follows from (3.3) and the alternating property of the Weil pairing. □

Remark 3.5. Letting $f = f_\Pi$ in (1.5), we see $C_2 \circ C_1 = (m_E, F_{m,\Pi}/h_{m,\Pi})$. Theorem 3.4 gives $C_2(C_1(Q)) = (\mathcal{O}, e_m(P, Q))$ for $Q \in E[m]$.

4. The Weil Pairing on Supersingular Curves

This section is devoted to a proof of (1.1) and (1.3). Let $E/\mathbf{F}_q$ be an elliptic curve. Throughout this section except for Lemma 4.4, E is assumed to satisfy $^{\#}E(\mathbf{F}_q) = q+1$. This implies that E is supersingular. Let r be the maximal odd divisor of $q+1$. Put

$$\begin{aligned}G_0 &:= \{P \in E[r] \,:\, \sigma_q(P) = qP\},\\ G_1 &:= E(\mathbf{F}_q)[r].\end{aligned}$$

Since r is odd, the embedding degree for E and r is 2. We note $qP = -P$ for $P \in E[r]$. We also note that $E[r] = G_0 \oplus G_1$. (This is the reason why we required r to be odd.) For $P \in E$ and a power m of p, there exists the unique P_m satisfying $mP_m = P$. By the uniqueness of P_m, we write P_m as $m^{-1}P$. We keep the notation i_n, $F_{m,P}$, $F_{m,\Pi}$ introduced in the previous section. We begin with a technical lemma.

Lemma 4.1. *Let $m \in \mathbf{N}$. We fix $Q \in E - \{\mathcal{O}\}$ and consider $h_{m,S}(Q)$ as a rational function of $S \in E$. Let ϱ be the local parameter for S at $\mathcal{O}$. Then,*

$$h_{m,S}(Q) = c_{m,Q} \varrho^{\varepsilon(m)-m} + O(\varrho^{\varepsilon(m)-m+1})$$

with $c_{m,Q}^2 = \mathrm{lc}(m_E)^{-2}$. (See (1.10) and (1.7) for the definition of ε and lc, *respectively).*

Proof. Let $h_{m,S}(Q) = \sum_{n=\nu}^{\infty} \gamma_{m,n}(Q) \varrho^n$ with $\gamma_{m,\nu}(Q) \neq 0$ be the Laurent expansion with respect to ϱ. Note

$$h_{m,-S}(Q) \;=\; \sum_{n=\nu}^{\infty} \gamma_{m,n}(Q)(\varrho^{\circ}-1_E)^n \;=\; (-1)^{\nu}\gamma_{m,\nu}(Q)\varrho^{\nu} + O(\varrho^{\nu+1}).$$

On the other hand, as a rational function on Q,

$$\mathrm{div} h_{m,S}h_{m,-S} \;=\; m([S]+[-S]-2[\mathcal{O}]) - ([mS]+[-mS]-2[\mathcal{O}]) \;=\; \mathrm{div}(V_S^m/V_{mS}).$$

The both hand sides are normalized rational function on Q. Nothing that E is supersingular, we have

$$h_{m,S}(Q)h_{m,-S}(Q) \;=\; \frac{V_S(Q)^m}{V_{mS}(Q)} \;=\; \frac{(Q_x-S_x)^m}{Q_x-(mS)_x} \;=\; \frac{(-\varrho^{-2}+O(\varrho^{-1}))^m}{-\mathrm{lc}(m_E)^2\varrho^{-2\varepsilon(m)}+O(\varrho^{-2\varepsilon(m)+1})}.$$

Therefore we obtain $2\nu=-2m+2\varepsilon(m)$ and $(-1)^{\nu}\gamma_{m,\nu}(Q)^2=(-1)^{m+1}\mathrm{lc}(m_E)^{-2}$. In case of $p=2$, we are done. Otherwise, $\varepsilon(m)$ is odd and $(-1)^{\nu}=-(-1)^m$. Hence $c_{m,Q}^2=\gamma_{m,\nu}(Q)^2=\mathrm{lc}(m_E)^{-2}$. □

The next lemma explains why we can expect a simple formula for the Weil pairing on supersingular curves.

Lemma 4.2. *Let $P\in E-E[2]$. For a power m of p, it holds that $F_{m,P}=h_{m,m^{-1}P}^{-m}$.*

Proof. Since E is supersingular, m_E is purely inseparable of degree m^2. Therefore

$$\begin{aligned}\mathrm{div}(F_{m,P}) &= m([P]-[\mathcal{O}])-m^2([m^{-1}P]-[\mathcal{O}]) \;=\; -m(m[m^{-1}P]-[P]-(m-1)[\mathcal{O}])\\ &= \mathrm{div}(h_{m,m^{-1}P}^{-m}).\end{aligned}$$

Since both $F_{m,P}$ and $h_{m,m^{-1}P}$ are normalized, the assertion follows. □

Theorem 4.3. *Let $A\in G_0$ and $Q\in E(\mathbf{F}_q)-\{\mathcal{O}\}$. Then $e_{q+1}(Q,A)=h_{q,A}(Q)^2$.*

Proof. The assertion trivially holds for $A=\mathcal{O}$. In what follows, we assume $A\neq\mathcal{O}$. Note $h_{q+1,P}=h_{q,P}\dfrac{L_{qP,P}}{V_{(q+1)P}}$ for any $P\in E$. Take $S\in E$ and put $\Pi:=[A+S]-[S]$. Then $h_{q+1,\Pi}=h_{q,\Pi}\dfrac{L_{q(A+S),(A+S)}}{L_{qS,S}}$ by $(q+1)A=\mathcal{O}$. Put $\tilde{\Pi}:=[q^{-1}A+q^{-1}S]-[q^{-1}S]$. By (3.2),

$$F_{q+1,\Pi} \;=\; F_{q,\Pi}\cdot(f_{\Pi}\circ i_q) \;=\; h_{q,\tilde{\Pi}}^{-q}\cdot(f_{\Pi}\circ i_q).$$

On the other hand, (3.3) gives $F_{q+1,\Pi}=h_{q+1,\Pi}/g_{q+1,\Pi}$. Therefore,

$$g_{q+1,\Pi} \;=\; h_{q,\Pi}\frac{L_{q(A+S),A+S}}{L_{qS,S}}\cdot h_{q,\tilde{\Pi}}^{q}\circ(f_{\Pi}\circ i_q)^{-1}.$$

Since $G_0\cap E(\mathbf{F}_q)=\{\mathcal{O}\}$, as a rational function of S, we have

$$g_{q+1,\Pi}(Q) \;=\; h_{q,\Pi}(Q)h_{q,\tilde{\Pi}}(Q)^q\frac{L_{q(A+S),A+S}(Q)}{L_{qS,S}(Q)}f_{\Pi}(Q,-Q)^{-1}.$$

By (2.9) and (3.4)

$$e_{q+1}(Q,A) = \frac{h_{q,A+S}(Q)h_{q,q^{-1}A+q^{-1}S}(Q)^q}{h_{q,S}(Q)h_{q,S_q}(Q)^q}\frac{L_{-A+qS,A+S}(Q)}{L_{qS,S}(Q)}\cdot\frac{V_S(Q)}{V_{A+S}(Q)}.$$

Let ϱ and $\tilde{\varrho}$ be the local parameter at $\mathcal{O}$ for S and $q^{-1}S$, respectively. Since E is supersingular, $\varrho=\tilde{\varrho}^{q^2}+O(\tilde{\varrho}^{q^2+1})$. Now as a rational function of $q^{-1}S$, the functions $h_{q,A+S}(Q)$, $h_{q,q^{-1}A+q^{-1}S}(Q)$ and $V_{A+S}(Q)$ are defined at $q^{-1}S=\mathcal{O}$. Let σ_q be the q-th power Frobenius map. Since $\sigma_q(q^{-1}A)=A$ and $\sigma_q(Q)=Q$, we obtain

$$h_{q,q^{-1}A}(Q)^q = \sigma_q(h_{q,q^{-1}A}(Q)) = h_{q,A}(Q).$$

We note that the assumption ${}^{\#}E(\mathbf{F}_q)=q+1$ implies that $\mathrm{Tr}(\sigma_q)=0$ and thus $\mathrm{lc}(q_E)=\mathrm{lc}(-\sigma_q)=-1$. Therefore, the other functions are expanded as follows:

$$\begin{aligned}
V_S(Q) &= \xi(Q)-\xi(S) = -\varrho^{-2}(1+O(\varrho)),\\
L_{-A+qS,A+S}(Q) &= L_{-(q+1)S,A+S}(Q) = \frac{(\varrho^{-3}+O(\varrho^{-2}))-\eta(A+S)}{(\varrho^{-2}+O(\varrho^{-1}))-\xi(A+S)}(\xi(Q)-\xi(A+S))+\eta(A+S)-\eta(Q)\\
&= (\xi(Q)-\xi(A))\varrho^{-1}+O(1),\\
L_{qS,S}(Q) &= \frac{(\varrho^{-3q^2}+O(\varrho^{-2q^2}))-(-\varrho^{-3}+O(\varrho^{-2}))}{(\varrho^{-2q^2}+O(\varrho^{-q}))-(\varrho^{-2}+O(\varrho^{-1})}(\xi(Q)-\varrho^{-2}+O(\varrho^{-1}))+(-\varrho^{-3}+O(\varrho^{-2}))-\eta(Q)\\
&= -\varrho^{-q^2-2}+O(\varrho^{-q^{-2}-1})).
\end{aligned}$$

By Lemma 4.1,

$$\begin{aligned}
h_{q,S}(Q) &= c_{q,Q}\varrho^{q^2-q}+O(\varrho^{q^2-q+1}),\\
h_{q,q^{-1}S}(Q) &= c_{q,Q}\tilde{\varrho}^{q^2-q}+O(\tilde{\varrho}^{q^2-q+1}),
\end{aligned}$$

hence $h_{q,q^{-1}S}(Q)^q=c_{q,Q}^q\varrho^{q-1}+O(\tilde{\varrho}^{q^3-q^2+1})$. Therefore, as a rational function of $q^{-1}S$, the function

$$\frac{1}{h_{q,S}(Q)h_{q,S_q}(Q)^q}\frac{L_{-A+qS,A+S}(Q)}{L_{qS,S}(Q)}\cdot\frac{V_S(Q)}{V_{A+S}(Q)}$$

is regular at $\mathcal{O}$ whose value at $\mathcal{O}$ is $c_{q,Q}^{q+1}$. In case of $p=2$, we have $c_{q,Q}=\mathrm{lc}(q_E)$ by Lemma 4.1. Otherwise, $q+1$ is even and Lemma 4.1 yields $c_{q,Q}^{q+1}=(\mathrm{lc}(q_E)^2)^{(q+1)/2}$. Since $\mathrm{lc}(q_E)=-1$, we obtain $c_{q,Q}^{q+1}=1$ and $e_{q+1}(Q,A)=h_{q,A}(Q)^2$. □

The next lemma is of a special case of Granger et al.[3, Theorem 2]. Here we give a direct proof which does not depend on bilinearity of other pairings.

Lemma 4.4. *Let $E/\mathbf{F}_q$ be an elliptic curve which is not necessarily supersingular. Let A, $B\in E$ and assume that the following conditions:*

(i) *$\sigma_q(A)=qA$ and $\sigma_q(B)=qB$.*

(ii) *None of A, B, $A+B$, qA, qB and $q(A+B)$ belongs to $E(\mathbf{F}_q)-\{\mathcal{O}\}$.*

Then $h_{q,A+B}(Q)=h_{q,A}(Q)h_{q,B}(Q)$ for $Q\in E(\mathbf{F}_q)-\{\mathcal{O}\}$.

Proof. First, observe that $h_{q,A+B}(Q)$, $h_{q,A}(Q)$ and $h_{q,B}(Q)$ are all defined and non-zero under the assumption (ii). Noting the divisor of the Miller function and normalization, we have $\dfrac{h_{q,A+B}}{h_{q,A}h_{q,B}} = \dfrac{(V_{A+B}/L_{A,B})^q}{V_{q(A+B)}/L_{qA,qB}}$. Therefore, $Q \in E(\mathbf{F}_q)$ and the assumption (i) imply

$$\frac{h_{q,A+B}(Q)}{h_{q,A}(Q)h_{q,B}(Q)} = \frac{V_{\sigma_q(A+B)}(\sigma_q(Q))/L_{\sigma_q(A),\,\sigma_q(B)}(\sigma_q(Q))}{V_{q(A+B)}(Q)/L_{qA,qB}(Q)} = 1.$$

□

Proposition 4.5. *Suppose $A \in G_0$ and $Q \in E(\mathbf{F}_q) - \{\mathcal{O}\}$. Then, $h_{q,A}(Q) = e_{q+1}\left(Q, \frac{r+1}{2}A\right)$. In particular, $(A, Q) \to h_{q,A}(Q)$ for $Q \neq \mathcal{O}$ yields a bilinear pairing $G_0 \times G_1 \to \mathbf{G}_{\mathrm{m}}$.*

Proof. Since r is odd, $\frac{r+1}{2} \in \mathbf{Z}$. Then $e_{q+1}\left(Q, \frac{r+1}{2}A\right)^2 = e_{q+1}(Q, A) = h_{q,A}(Q)^2$ by Theorem 4.3. Thus $e_{q+1}\left(Q, \frac{r+1}{2}A\right) = \pm h_{q,A}(Q)$. In case of $p=2$, we are done. Assume $p \geq 3$ and suppose $e_{q+1}\left(Q, \frac{r+1}{2}A\right) = -h_{q,A}(Q)$. By Lemma 4.4, $h_{q,A}(Q) = h_{q,\frac{r+1}{2}A}(Q)^2$. Using Theorem 4.3 again, we obtain $e_{q+1}\left(Q, \frac{r+1}{2}A\right) = -e_{q+1}\left(Q, \frac{r+1}{2}A\right)$, which is a contradiction.
□

5. Application to Pairing Inversion

We keep notation and assumptions of the previous sections. For simplicity, we put $K := \mathbf{F}_{q^2}$. In this section, we show some of coefficients of the rational function $h_{q,A}$, which a priori belongs to K, belongs to $\mathbf{F}_q$. Then, we develop an X-coordinate only pairing inversion algorithm.

Let $A \in G_0 \subset E(K)$. Then there exist unique $\alpha_{q,A}$ and $\beta_{q,A} \in K(\xi)$ satisfying $h_{q,A} = \alpha_{q,A} + \beta_{q,A}\eta$. Recall that E is given by the Weierstrass form (1.6). We show that in fact either $\alpha_{q,A}$ or $\beta_{q,A} \in \mathbf{F}_q(\xi)$ under some conditions.

Proposition 5.1. *Assume $p=2$.*
(i) $\beta_{q,A} \in \mathbf{F}_q(\xi)$.
(ii) *Let $Q \in E(\mathbf{F}_q) - \{\mathcal{O}\}$ and put $z := h_{q,A}(Q)$. Then,* $\mathrm{Tr}_{K/\mathbf{F}_q} z = a_3\beta_{q,A}(\xi(Q))$.

Proof. On one hand $\sigma_q(h_{q,A}) = \sigma_q(\alpha_{q,A}) + \sigma_q(\beta_{q,A})\eta$ while on the other hand

$$\begin{aligned}\sigma_q(h_{q,A}) &= h_{q,\sigma_q(A)} = h_{q,-A} = (-1)^{q-1} h_{q,A} \circ (-1)_E \\ &= \alpha_{q,A} + \beta_{q,A}(-\eta - a_1\xi - a_3).\end{aligned}$$

Therefore, regardless of p, we obtain

$$\begin{aligned}\sigma_q(\alpha_{q,A}) &= \alpha_{q,A} - a_1\xi\beta - a_3\beta, \\ \sigma_q(\beta_{q,A}) &= -\beta_{q,A}.\end{aligned} \tag{5.1}$$

When $p=2$, the last equation is $\sigma_q\beta_{q,A} = \beta_{q,A}$. This proves (i). Since E is supersingular, $a_1 = 0$. By Proposition 4.5, $z \in \mu_{q+1}$. Therefore,

$$z = h_{q,A}(Q) = \alpha_{q,A}(\xi(Q)) + \beta_{q,A}(\xi(Q))\eta(Q),$$
$$z^q = z^{-1} = h_{q,A}(-Q) = \alpha_{q,A}(\xi(Q)) + \beta_{q,A}(\xi(Q))(\eta(Q) + a_3).$$

Adding these two formula, we obtain (ii). □

Proposition 5.2. *Suppose that p is odd and that $a_1 = a_3 = 0$.*
(i) $\alpha_{q,A} \in \mathbf{F}_q(\xi)$.
(ii) *Let c be an element of K satisfying $\sigma_q c = -c$. Then $c\beta_{q,A} \in \mathbf{F}_q(\xi)$.*
(iii) *Let $Q \in E(\mathbf{F}_q) - \{\mathcal{O}\}$ and put $z := h_{q,A}(Q)$. Then,* $\mathrm{Tr}_{K/\mathbf{F}_q} z = 2\alpha_{q,A}(\xi(Q))$.

Proof. The assertions (i) and (ii) follow from (5.1). A similar argument to the proof of the preceding proposition shows

$$\begin{aligned}\mathrm{Tr}_{K/k} z &= h_{q,A}(Q) + h_{q,A}(-Q) = \alpha_{q,A}(\xi(Q)) + \beta_{q,A}(\xi(Q))\eta(Q) + \alpha_{q,A}(\xi(Q)) + \beta_{q,A}(\xi(Q))(-\eta(Q)) \\ &= 2\alpha_{q,A}(\xi(Q)).\end{aligned}$$

□

We apply the above propositions to pairing inversion. Let $A \in G_0 - \{\mathcal{O}\}$ and let m be the order of A. (Recall that r is not necessarily a prime.) For a given $z \in \mu_m$, our task is to find $Q \in E(\mathbf{F}_q)[m]$ ($\subset G_1$) satisfying $h_{q,A}(Q) = z$. In what follows, we assume that $a_1 = 0$ and that $a_3 = 0$ when p is odd. Note that $V_A = \xi - \xi(A) \in \mathbf{F}_q[\xi]$. We put

$$U_{A,z} := \begin{cases} V_A \cdot (\beta_{q,A} - \mathrm{Tr}_{K/\mathbf{F}_q}(z)/a_3) & (p = 2), \\ V_A \cdot (\alpha_{q,A} - \mathrm{Tr}_{K/\mathbf{F}_q}(z)/2) & (p \geq 3). \end{cases}$$

Then, $U_{A,z}$ is regular outside of $\{\mathcal{O}\}$, hence $U_{A,z} \in \mathbf{F}_q[\xi]$. Since $A \neq \mathcal{O}$, we have $\mathrm{ord}_{\mathcal{O}} h_{q,A} = -q+1$ and $\mathrm{ord}_{\mathcal{O}} V_A = -2$, hence $\deg U_{A,z} \leq (q+1)/2$. We can construct $h_{q,A}$ with $\widetilde{O}(q)$ space complexity with the Miller algorithm. (In case of $N = [\mathbf{F}_q : \mathbf{F}_p] > 1$, one might utilize

$$h_{p^N,A} = \prod_{i=0}^{N-1} h_{p,\,p^{N-1-i}A}^{p^i} \tag{5.2}$$

but this does not seem to bring essential improvement.) Since $Q \in E(\mathbf{F}_q)$, we can obtain candidates of $\xi(Q)$ by finding $\mathbf{F}_q$ solution of $U_{A,z}(X) = 0$. Numerical experiments for small q (≈ 5000) suggest

$$\deg \gcd(U_{A,z}(X), X^q - X) = \frac{q+1}{m} \tag{5.3}$$

in case of $\gcd\left(\frac{q+1}{m}, m\right) = 1$. However, validity of the conjecture is completely open. In order to reduce time complexity, we first compute the gcd with the asymptotically fast algorithm due to Moenck[9] (see also von zur Gathen and Gerhard[13, Sect. 11.1]) and then factorize the gcd. For each solution X, we obtain at most two candidates of $\eta(Q)$. We can detect a correct solution by numerically checking $mQ = \mathcal{O}$ and $h_{q,A}(Q) = z$.

Compared to the method which eliminates the Y-coordinate from $h_{q,A}(Q)=z$ and the curve equation, our method has two advantages:

(i) Once $U_{A,z}$ is constructed, all the computations are performed over $\mathbf{F}_q$ instead of K.

(ii) The $\deg U_{A,z}$ is approximately the half of degree of the equation after Y-coordinate elimination.

In case of $N>1$ (and small p), we can also deploy multivariate attack due to Galbraith, Ó hÉigeartaigh and Sheedy[2, Sect. 4]. Fix an $\mathbf{F}_p$-base $\{\theta_0, \ldots, \theta_{N-1}\}$ of $\mathbf{F}_q$. We try to find a $\mathbf{F}_p$ solution $(x_0, \ldots, x_{N-1})$ of $U_{A,z}(x_0\theta_0+\cdots+x_{N-1}\theta_{N-1})=0$, which turns in to a system of N equations of N unknowns over $\mathbf{F}_p$ whose degree with respect to each unknown is less than p. The space complexity is $O(Np^N)$ as $N\to\infty$ while p is fixed. Although Galbraith et al.[2] considers a supersingular curves of embedding degree four, if we apply their method to (5.2), its space complexity would be $O(Np^{2N})$.

In either way, the algorithms are infeasible for cryptgraphic sizes. Further re-saerch on it is necessary.

References

1. Chang, S., Hong, H., Lee, E. and Lee, H.S.: Reducing pairing inversion to exponentiation inversion using non-degenerate auxiliary pairing, IACR e-print 2013/313.
2. Galbraith, S.D., Ó hÉigeartaigh, C. and Sheedy, C.: Simplified pairing computation and security implications. J. Math. Crypt., **1**, 267-281 (2007). doi: 10.1515/JMC.2007.013
3. 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
4. Hess, F.: Pairing Lattices, Pairing-Based Cryptography -- Pairing 2008, Lect. Notes in Comput. Sci., **5209**, 18-38, ed. Galbraith, S.D. and Paterson, K.G., 2008. doi: 10.1007/978-3-540-85538-5_2
5. Hess, F., Smart, N.P. and Vercauteren, F.: The eta pairing revisited. IEEE trans. on IT, **52**, 4995-4602 (2006). doi: 10.1109/TIT.2006.881709
6. Kanayama, N. and Okamoto, E.: Approach to pairing inversion without solving Miller inversion. IEEE Trans. IT, **58**, 1248-1253 (2012). doi: 10.1109/TIT.2011.2173714
7. Kim, S. and Cheon, J.H.: Fixed argument pairing inversion on elliptic curves, IACR e-print 2012/657.
8. Milne, J.S.: Abelian varieties, Arithmetic Geometry, 103-150, ed. Cornell, G. and Silverman, J.H., New York: Springer, 1986.
9. Moenck, R.T.: Fast computation of GCDs, Fifth annual ACM symposium on theory of computing (Austin, Tex., 1973), 142-151, New York: ACM, 1973. doi: 10.1145/800125.804045

10. Serre, J.-P.: Algebraic groups and class fields, Graduate texts in mathematics, **117**, Springer, 1988. doi: 10.1007/978-1-4612-1035-1
11. Silverman, J. H.: The arithmetic of elliptic curves. GTM, 106. Berlin-Heidelberg-New York: Springer 1986.
12. Vercauteren, F.: Optimal pairings. IEEE Trans. IT, **56**, 455-461 (2010). doi: 10.1109/TIT.2009.2034881
13. von zur Gathen, J. and Gerhard, J.: Modern computer algebra (2nd ed.). Cambridge: Cambridge UP 2003.