A Construction of a Twisted Ate Pairing on a Family of Kawazoe-Takahashi Curves at 192-bit Security Level and Its Cost Estimate

Masahiro Ishii[1], Atsuo Inomata[2] and Kazutoshi Fujikawa[2]
[1]*Nara Institute of Science and Technology, 8916-5 Takayama, Ikoma, NARA, 630-0192, Japan*
[2]*Information Initiative Center, Nara Institute of Science and Technology, 8916-5 Takayama, Ikoma, NARA, 630-0192, Japan*

Keywords: Twisted Ate Pairings, Optimal Pairings, Hyperelliptic Curves, Final Exponentiation.

Abstract: Recently, there were major breakthroughs in computing DL in finite fields of small characteristics, as a result the symmetric pairings which is defined by using such finite fields became unsuitable for cryptography. This research aims to reveal a more efficient construction of pairings on hyperelliptic curves of genus 2, in the beginning, we focus on the ordinary genus 2 curves and the optimal pairing algorithms at high (192-bit) security level on such curves. In this paper, we show the method to construct optimal pairings over the family of pairing-friendly curves of genus 2 by Kawazoe and Takahashi and offered a twisted version of Ate pairing. We then provide the cost estimates to compare with the result of the pairings on elliptic curve at same security level.

1 INTRODUCTION

Pairings on hyperelliptic curves (including elliptic curves) have been applied to many cryptographic schemes (functional encryption and its varieties), and the various optimization methods that increase the speed of the algorithm of pairings and their arithmetic of curves have been exploited.

Recently, major theoretical and practical breakthrough in computing discrete logarithms in finite fields of small characteristic and also other fields have been made (Barbulescu et al., 2014; Barbulescu et al., 2015). As a result, the type 1 (symmetric) pairings have been almost dead since these pairings are defined on the supersingular curves of high embedding degree over finite fields of small characteristic to use their distortion maps. We should also improve the security level of pairings for the complexity of the discrete logarithm algorithm in other finite fields. Since type 1 pairings are still useful for constructing some cryptographic protocols, some authors offered the type 1 pairing on the curves not defined over finite fields of small characteristic in elliptic case (Teruya et al., 2014; Zhang and Wang, 2014) and in genus 2 case (Galbraith et al., 2008). Their pairings, however, are not suitable for the situation required high security level because of their small embedding degree.

Aranha et al. (Aranha et al., 2013) showed optimal asymmetric pairings on Kachisa-Schaefer-Scott (KSS), Barreto-Naehrig (BN), and Barreto-Lynn-Scott (BLS) elliptic curves at the 192-bit security level and their cost estimates and implementation result. They constructed the optimal (ate) pairings and Weil type ones (Hess, 2008; Vercauteren, 2010) on each elliptic curve family. The BLS pairings is the most efficient and the result of serial implementation of BLS pairings is more than 3 times faster than the result of (Scott, 2011).

In this paper, we focus on the ordinary hyperelliptic curves of genus 2 at high, i.e. 192-bit security level. We show the method to construct the optimal pairing and its twisted version over the family of pairing-friendly curves of genus 2 by Kawazoe and Takahashi (Kawazoe and Takahashi, 2008) We offered that a twisted Ate pairing is most efficient and described cost estimates in detail. Especially, we clarify the cost of the final exponentiation where embedding degree $k = 16$.

The aim of this research is that eventually reveal an efficient construction of pairings on hyperelliptic curves of genus 2. This research for exploiting more efficient pairings on genus 2 curves is in progress and our pairing showed in this paper does not faster one than the state-of-the-art elliptic pairing.

The remainder of this paper is organized as follows. We recall background on several pairings on hy-

Ishii, M., Inomata, A. and Fujikawa, K.
A Construction of a Twisted Ate Pairing on a Family of Kawazoe-Takahashi Curves at 192-bit Security Level and Its Cost Estimate.
DOI: 10.5220/0005742304320439
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 432-439
ISBN: 978-989-758-167-0

perelliptic curves in section 2. Section 3 describes the method of constructing Kawazoe-Takahashi curves and the curve parameter we used to evaluate the pairing in practice. We show how to construct optimal pairings derived from Hess (Hess, 2008) and Vercauteren (Vercauteren, 2010) on the curve and its twisted version in section 4, after that the cost estimates and its comparison are described in section 5. Finally, we present conclusions and suggestions for future work in section 6.

2 PRELIMINARY

In this section, we describe the pairings on hyperelliptic curves, especially, *Hess-Vercauteren (HV) pairings* (Balakrishnan et al., 2009) given by Hess (Hess, 2008) and Vercauteren (Vercauteren, 2010) as general framework for pairings on Frobenius eigenspaces.

Let C be a hyperelliptic curve defined over $\mathbb{F}_q$ and let $\mathrm{Jac}_C(\simeq \mathrm{Pic}^0_C)$ denote Jacobian of C. Let r be a positive integer and suppose that $\mathbb{F}_{q^k}$ is an extension field of $\mathbb{F}_q$ such that $r|(q^k-1)$ and $\mathrm{Jac}_C(\mathbb{F}_{q^k})$ contains no elements of order r^2. The smallest integer k which holds the avobe condition is called embedding degree of Jac_C with respect to r. For a divisor class $D \in \mathrm{Jac}_C(\mathbb{F}_{q^k})[r]$, $f_{r,D}$ denotes a rational function associated the principal divisor rD. Let $E = \sum n_P P$ be a divisor class disjoint from D. Then we call T_r the modified Tate-Lichtenbaum pairing as follows

$$T_r \colon \mathrm{Jac}_C(\mathbb{F}_{q^k})[r] \times \mathrm{Jac}_C(\mathbb{F}_{q^k})[r] \to \mu_r \subset F_{q^k}$$
$$(D,E) \mapsto f_{r,D}(E) = \left(\prod_P f_{r,D}(P)^{n_P} \right)^{(q^k-1)/r}.$$

The map T_r is bilinear, non-degenerate and the value of T_r is independent of representation of the divisor classes.

By limiting the domains of pairings to eigenspaces of the Frobenius map, more efficient pairings which have shorter Miller loop were exploited, called Ate pairings (Granger et al., 2007) and twisted Ate pairings (Zhang, 2010). These pairings are special case of HV pairings.

Let π be the q-th Frobenius map, we take $\mathbb{G}_1$ and $\mathbb{G}_2$ which are subgroups of $\mathrm{Jac}_C(\mathbb{F}_{q^k})$ as follows,

$$\mathbb{G}_1 := \mathrm{Jac}_C(\mathbb{F}_q^k)[r] \cap \ker(\pi - [1])$$
$$\mathbb{G}_2 := \mathrm{Jac}_C(\mathbb{F}_q^k)[r] \cap \ker(\pi - [q]).$$

We consider $h(x) = \sum_{i=0}^{n} h_i x^i \in \mathbb{Z}[x]$ such that $h(x) \equiv 0 \pmod r$ and *generalized Miller function* $f_{s,h,D}$ ($D \in \mathrm{Jac}_C(\mathbb{F}_{q^k})[r]$) which is any function with

$$\sum_{i=0}^{n} h_i \rho(s^i D),$$

where $\rho(D)$ is the reduced divisor which is equivalent to D. Let $s \equiv q^j \pmod r$ for some $j \in \mathbb{Z}$. We then obtain the bilinear pairing (HV pairing) (Balakrishnan et al., 2009, Theorem 4.1)

$$a_{s,h} \colon \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$$
$$(D_2, D_1) \mapsto f_{s,h,D_2}(D_1)^{(q^k-1)/r},$$

satisfying

$$a_{s,h}(D_2, D_1) = T_r(D_2, D_1)^{h(s)/r}.$$

$a_{s,h}$ is non-degenerate if and only if $h(s) \not\equiv 0 \pmod{r^2}$.

If C has the twist C_t of degree d, i.e., d is the minimal integer satisfying that there exists an isomorphism $\phi \colon C_t \to C$ over $\mathbb{F}_{q^d}$, a twisted version of the HV pairing exists (Balakrishnan et al., 2009, Remark 4.4). We suppose that $\gcd(k, \sharp\mathrm{Aut}(C)) \neq 1$, then

$$a^{\mathrm{twist}}_{s,h} \colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r$$

is also a bilinear and non-degenerate (under same condition of HV pairings) pairing (Hess, 2008, Theorem 1).

In twisted case, we remark that the automorphism $[\xi]\pi^{k/m}$ plays an important role where $m = \gcd(k,d)$ and $[\xi] \in \mathrm{Aut}(C)$ defined by the twist (see (Zhang, 2010)). This map acts on $\mathbb{G}_1$ as $[q^m]$ and acts on $\mathbb{G}_2$ as $[1]$, therefore we can reverse the roles of $\mathbb{G}_1$ and $\mathbb{G}_2$ in HV pairings.

3 KAWAZOE-TAKAHASHI CURVES AND SECURITY LEVEL

Many researcher has exploited the pairing-friendly curves of genus 2 (Kawazoe and Takahashi, 2008; Kachisa, 2010; Freeman and Satoh, 2011; Guillevic and Vergnaud, 2013). In this paper, we focus on Kawazoe-Takahashi curve (Kawazoe and Takahashi, 2008) of embedding degree 16 for efficient field size at 192-bit security level. By using the method to construct the cyclotomic family of type I (Kawazoe and Takahashi, 2008, Section 6.1), we can obtain a family of curves

$$C \colon y^2 = x^5 + ax$$

defined over $\mathbb{F}_p$ such that the parameter p and r (prime factor of the order of $\mathrm{Jac}_C(\mathbb{F}_p)$) are parametrized by $t \in \mathbb{Z}$ as follows:

$$r(t) = \Phi_{16}(t)/2 = (t^8+1)/2,$$

$$p(t) = (1+2t+t^2+2t^4+4t^5+2t^6+t^8 + 2t^9+t^{10}+2t^{12}-4t^{13}+2t^{14})/8.$$

Therefore, rho value $\rho = g\log q/\log r \approx 3.5$ (q is the size of finite field which the curve is defined, so now $q = p$) since $p \approx r^{14/8}$.

For 192-bit security level, we should choose r over 2^{384} and p^k over 2^{7936} (BlueKrypt, 2012, NIST and ECRYPT II Recommendations). Note that we chose the embedding degree $k = 16$ and the family of curves in the Table 1 in (Guillevic and Vergnaud, 2013) on condition that k is in the form 2^i3^j (pairing-friendly field) and the size of r is as close as possible to the appropriate key length 2^{384}.

To reduce the cost of the pairing we should take a low hamming weight t. We can find the following curve by using (Kawazoe and Takahashi, 2008, Theorem 2):

$$C\colon y^2 = x^5 + 11x,$$

$$\begin{aligned}
r &= 504407248238447657378299392789\backslash \\
&= 772896446543658624525445331163\backslash \\
&= 126537154974303129047300811340\backslash \\
&= 92152680111432970440685 61 \text{ (392 bits)}, \\
p &= 802804519546036640185560881085\backslash \\
&= 108752035653601051669471902400\backslash \\
&= 520017061910329540428131487703\backslash \\
&= 069175633541070581107341333451\backslash \\
&= 195166854084612357701976368675\backslash \\
&= 108135154063712777695376353054\backslash \\
&= 24502257207565576569 \text{ (685 bits)}, \\
t &= 562958543356163 \\
&= 2^{49}+2^{33}+2^8+2+1 \text{ (50 bits)},
\end{aligned}$$

where $\rho \approx 3.497$.

4 CONSTRUCTION OF THE PAIRING

Here we construct the optimal HV pairing and its twisted version on the Kawazoe-Takahashi curve of embedding degree 16 as described previous section. First we consider optimal pairings over genus 2 curves as offered in elliptic case by (Aranha et al., 2013), then we focus twisted version of the pairing in order to reduce the cost of computing the pairing since the cost of arithmetic on Jacobian over extension field become extremely high.

4.1 Optimal HV Pairing

According to the optimal conjecture by Vercauteren (Vercauteren, 2010), we can take the total loop length of the Miller function as $(\log_2 r)/\varphi(k)$ where φ is the Euler's totient function and this length is optimal. In order to construct optimal HV pairings, we need to choose $h(x) = \sum_{i=0}^{n} h_i x^i \in \mathbb{Z}[x]$ so that the total loop length $h(x) = \sum_{i=0}^{n} \log_2 h_i$ is optimal. Vercauteren showed the several optimal HV pairings on elliptic curve families by finding the shortest vectors in a lattice (Vercauteren, 2010). Specifically, for a $\varphi(k)$-dimensional lattice (spanned by the rows)

$$L = \begin{pmatrix} r & 0 & 0 & \cdots & 0 \\ -s \pmod r & 1 & 0 & \cdots & 0 \\ -s^2 \pmod r & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \ddots & \\ -s^{\varphi(k)-1} \pmod r & 0 & 1 & \cdots & 0 \end{pmatrix},$$

he used the function `ShortestVectors()` or `ShortVectors()` in Magma (Bosma et al., 1997) for specific input integers, and he found parametrized the shortest vectors by interpolating for parametrized r and s.

We can obtain the shortest vectors for HV pairing $a_{p,h}$ on the Kawazoe-Takahashi curve defined in previous section in the same manner. The prameters p, r should be represented as polynomials over integer ring, we substitute $t = 2x+1$ to p, r and obtain

$$\begin{aligned}
r(x) &= 128x^8+512x^7+896x^6 \\
&+ 896x^5+560x^4+224x^3 \\
&+ 56x^2+8x+1,
\end{aligned}$$

$$\begin{aligned}
p(x) &= 4096x^{14}+24576x^{13}+67584x^{12} \\
&+ 112640x^{11}+126848x^{10}+102144x^9 \\
&+ 61184x^8+28544x^7+11184x^6 \\
&+ 4064x^5+1432x^4+456x^3 \\
&+ 115x^2+20x+2.
\end{aligned}$$

Now we can calculate shortest vectors for the lattice L ($s = p$) using Magma, we obtain the vector

$$\begin{aligned}
V(x) &= [2x+1,0,0,0,0,1,0,0] \\
&= [t,0,0,0,0,1,0,0],
\end{aligned}$$

therefore it holds $2x+1+p(x)^5 \equiv 0 \pmod{r(x)}$. We then compute the Miller function except for final exponentiation of HV pairing $a_{p,h}$ as

$$f_{t+p^5,D_2} = f_{t,D_2} f_{p^5,D_2} \frac{c(x,y)}{d(x,y)}$$

where

$$\mathrm{div}\left(\frac{c(x,y)}{d(x,y)}\right) = [t]D_2 + [p^5]D_2 - [t+p^5]D_2$$

is a rational function. Now we consider Frobenius eigenspace $\mathbb{G}_1, G_2$ as the domain of the pairing, it holds $f_{p^5,D_2} = f_{1,D_2}^{p^5}$ and f_1 is constant, therefore we can write

$$a_{p,h}(D_2,D_1) = f_{t,D_2} \cdot \frac{c(x,y)}{d(x,y)}(D_1)^{(q^k-1)/r}.$$

4.2 Twisted Optimal HV Pairing

As described in the beginning of this section, arithmetic on Jacobian over the extension field ($\mathbb{F}_{p^{16}}$) costs very high, we consider twisted version of the HV pairings

Since $p \equiv 1 \pmod 8$, C has a twist of degree $d = 8$. Here we consider the twist over $\mathbb{F}_{p^2}$ as follows:

$$C_t : y^2 = x^5 + 11\lambda x,$$
$$\varphi : C_t \to C$$
$$(x,y) \mapsto (\lambda^{\frac{1}{4}} x, \lambda^{\frac{5}{8}} y)$$

where $\lambda \in \mathbb{F}_{p^2}$ is not l-th power residue in $\mathbb{F}_{p^2}$ for $l \in \{1,2,4,8\}$. So it holds $C(\mathbb{F}_{p^{16}}) \simeq C_t(\mathbb{F}_{p^{16}})$.

In our case, since $m = \gcd(k,d) = 8$ and $e = k/m = 2$ we can represent $\mathbb{G}_2$ as

$$\mathbb{G}_2 = \mathrm{Jac}_C(\mathbb{F}_q^k)[r] \cap \ker([\xi_m]\pi^2 - 1).$$

Therefore, we should search short vectors for $h(x)$ where the coefficients of p^i (i: odd) equal to 0 to reduce the Miller function in the same manner as HV pairings. For a lattice

$$L = \begin{pmatrix} r & 0 & 0 & 0 \\ -p^2 \pmod r & 1 & 0 & 0 \\ -p^4 \pmod r & 0 & 1 & 0 \\ -p^6 \pmod r & 0 & 0 & 1 \end{pmatrix},$$

we can find the vector

$$W(x) = [(2x+1)^2, 1, 0, 0] = [t^2, 1, 0, 0]$$

by using `ShortVectors()` and it holds $(2x+1)^2 + p(x)^2 \equiv 0 \pmod{r(x)}$. In this case, the Miller loop length is twice the one of optimal pairing. We couldn't find essentially shorter vectors such that the coefficients of p^i (i: odd) is 0. The twisted HV pairing can be computed as follows:

$$a_{p,h}^{\mathrm{twist}}(D_1,D_2) = f_{t^2,D_1} \cdot \frac{c(x,y)}{d(x,y)}(D_2)^{(q^k-1)/r},$$

where

$$\mathrm{div}\left(\frac{c(x,y)}{d(x,y)}\right) = [t^2]D_1 + [p^2]D_1 - [t^2+p^2]D_1.$$

4.3 Twisted Ate Pairing

Zhang (Zhang, 2010) proposed the hyperelliptic twisted Ate pairing. Here we confirm that previous twisted HV pairing corresponds to a twisted Ate pairing. Zhang showed that

$$f_{q^{ei} \pmod r, D_1}(D_2)^{(q^k-1)/r}$$

is a bilinear pairing (Zhang, 2010, Theorem 4) where e is same as the above. We want to take the smallest $ei \pmod r$, now it holds $p^{10} \pmod r = t^2$. Therefore, we can compute simply

$$a^{\mathrm{twist}}(D_1,D_2) = f_{t^2,D_1}(D_2)^{(q^k-1)/r},$$

and the most efficient pairing on this curve is the twisted Ate pairing since there is no extra rational function occurred in the twisted optimal HV pairing in 4.2.

5 COST ESTIMATES

In this section we provide the cost estimate of the pairing on the Kawazoe-Takahashi curve of embedding degree 16. As described previous section, the twisted Ate pairing seems to be the fastest one, we only focus on this pairing. We have not optimally implemented the pairing and arithmetic on the field $\mathbb{F}_p$ and $\mathbb{F}_{p^{16}}$ yet, we show here cost estimates by number of multiplications in definition field $\mathbb{F}_p$.

The extension field $\mathbb{F}_{p^{16}}$ should be constructed the tower of quadratic extension fields. In our case, we can take 11 as a quadratic nonresidue modulo p and this is the smallest one. We then construct each extension fields as follows:

$$\mathbb{F}_{p^2} \simeq \mathbb{F}_p[x]/(x^2-11),$$
$$\mathbb{F}_{p^4} \simeq \mathbb{F}_{p^2}[y]/(y^2-\alpha),\ (\alpha^2-11=0),$$
$$\mathbb{F}_{p^8} \simeq \mathbb{F}_{p^4}[z]/(z^2-\beta),\ (\beta^2-\alpha=0),$$
$$\mathbb{F}_{p^{16}} \simeq \mathbb{F}_{p^8}[s]/(s^2-\gamma),\ (\gamma^2-\beta=0).$$

We denote a multiplication and a squaring in $\mathbb{F}_{p^i}$ by M_i and S_i, respectively. We also suppose that the cost

of a squaring equal to one of a multiplication in $\mathbb{F}_p$, i.e. $M_1 = S_1$. We assume to use Karatsuba method for multiplication in each field, so $M_{16} = 81M_1$. In the first quadratic extension field $\mathbb{F}_{p^2}$, we can perform a squaring

$$(a+bx)^2 = a^2 + 11b^2 + 2abx$$

with computing

$$ab,$$
$$(a+b)(a+11b) - ab - 11ab.$$

It costs 2 multiplications in $\mathbb{F}_p$ and additional additions for computing $11c$, $(c \in \mathbb{F}_p)$ (5 additions) and accumulating. We can therefore consider S_2 as $2M_1$, and we assume that $S_4 = 6M_4$, $S_8 = 18M_8$ and $S_{16} = 54M_{16}$.

Fan, Gong, and Jao (Fan et al., 2008) proposed to use the twist of the curve and degenerate divisors (Frey and Lange, 2006) to use denominator elimination technique and reduce the cost to evaluate the second argument divisors by the rational functions. Their method can be applied the twisted Ate pairing in our case:

$$f_{t^2,D_1}(\varphi(D_2'))^{(q^k-1)/r} \ (D_2' = [x - x_t, y_t] \in \mathrm{Jac}_{C_t}(\mathbb{F}_{q^2}))$$

where $\varphi(D_2') = [x - \lambda^{\frac{1}{4}} x_t, \lambda^{\frac{5}{8}} y_t]$.

5.1 Miller Loop

For the parameter we described in section 3, the Miller loop computation of $f_{t^2,D_1}(D_2)$ requires 96 doublings and 53 addition on Jacobian. In general case, we can do arithmetic on the divisor group using affine coordinates by Lange (Lange, 2005) where the cost of a doubling is $I_1 + 5S_1 + 22M_1$ and the one of an addition is $I_1 + 3S_1 + 22M_1$. Here we use the explicit formula and the dedicated coordinate system by (Fan et al., 2009) for C. As noted by the authors (Fan et al., 2009, Section 4.6), since $f_2, f_3 = 0$ where $C\colon y^2 = f(x)$, $f(x) = x^5 + f_3x^3 + f_2x^3 + f_1x + f_0$, a doubling need $35M_1 + 5S_1$. And we can perform a mixed addition with $36M_1 + 5S_1$.

In the Cantor's algorithm and Miller loop, we need to evaluate the auxiliary rational function by substituting the points associated D_2. The rational function can be obtained as

$$\frac{y - v(x)}{u'(x)}$$

where degree of $v(x)$ is at most 3. Since the x-coordinate of $\varphi(D_2')$ is defined in $\mathbb{F}_{p^8}$, we can use denominator elimination so we need not to evaluate $u'(x)$. By using the new coordinate system from (Fan et al., 2009), we should evaluate

$$c_D(x,y) = (\tilde{r}z_{11})y - ((s_1'z_{11})x^3 + l_2x^2 + l_1x + l_0),$$
$$c_A(x,y) = (\tilde{r}z_{21})y - ((s_1'z_{21})x^3 + l_2x^2 + l_1x + l_0)$$

for a doubling and an addition, respectively, instead of $y - v(x)$. The parameters in the above functions are from (Fan et al., 2008, Table 4,5)

Let f be the intermediate pairing value, when we take degenerate divisors $\varphi(D_2')$ as second inputs for the pairing, in each doubling step we compute

$$f^2 c_D(\varphi(D_2')) = f^2 c_D(\lambda^{\frac{1}{4}} x_t, \lambda^{\frac{5}{8}} y_t)$$

and

$$f c_A(\varphi(D_2')) = f c_A(\lambda^{\frac{1}{4}} x_t, \lambda^{\frac{5}{8}} y_t)$$

in each addition step. After precomputing $(\lambda^{\frac{1}{4}} x_t)^2, (\lambda^{\frac{1}{4}} x_t)^3$ with $S_8 + M_8 = 45M_1$, we evaluate $c_D(\varphi(D_2'))$ and $c_A(\varphi(D_2'))$ with $16M_1 + 3 \cdot 8M_1 = 40M_1$. Therefore computing $f^2 c_D(\varphi(D_2'))$ and $f c_A(\varphi(D_2'))$ requires $40M_1 + S_{16} + M_{16} = 175M_1$ and $40M_1 + M_{16} = 121M_1$, respectively. Since

$$t^2 = 1 + 2^3 + 2^9 + 2^{10} + 2^{16} + 2^{34} + 2^{35} + 2^{42} + 2^{50} + 2^{51} + 2^{58} + 2^{66} + 2^{83} + 2^{98},$$

Miller loop requires totally
$\{45 + 98(40 + 175) + 13(41 + 121)\}M_1 = 23221M_1$.

5.2 Final Exponentiation

For efficient computation of the final exponentiation, we should use the method by Scott et al. (Scott et al., 2009). In their method, we should estimate the cost of computing $\Phi_8(p)/r$ where

$$(p^{16} - 1)/r = (p-1)(p+1)(p^2+1)(p^4+1)(p^8+1)/r.$$

By using the parametrization of $p(x)$ and $r(x)$, we can compute the coefficients as polynomial of the following polynomial

$$(p(x)^8 + 1)r(x) = \sum_{i=0}^{7} l_i(x)p(x)^i.$$

where

$$\begin{aligned} l_0(x) &= 256x^9 + 896x^8 + 1344x^7 + 1120x^6 \\ &+ 568x^5 + 196x^4 + 66x^3 + 27x^2 + 8x + 3 \\ l_1(x) &= -2048x^{12} - 10240x^{11} - 23040x^{10} \\ &- 30720x^9 - 26944x^8 - 16448x^7 \\ &- 7408x^6 - 2752x^5 - 980x^4 \\ &- 348x^3 - 111x^2 - 26x - 3 \end{aligned}$$

$$
\begin{aligned}
l_2(x) &= -64x^7 - 160x^6 - 160x^5 - 80x^4 \\
&- 22x^3 - 7x^2 - 4x - 1 \\
l_3(x) &= 512x^{10} + 2048x^9 + 3584x^8 + 3584x^7 \\
&+ 2256x^6 + 960x^5 + 328x^4 + 120x^3 \\
&+ 43x^2 + 14x + 3 \\
l_4(x) &= -4096x^{13} - 22528x^{12} - 56320x^{11} \\
&- 84480x^{10} - 84608x^9 - 59840x^8 \\
&- 31264x^7 - 12912x^6 - 4712x^5 \\
&- -1676x^4 - 570x^3 - 163x^2 - 32x - 3 \\
l_5(x) &= -128x^8 - 384x^7 - 480x^6 - 320x^5 - 124x^4 \\
&- 36x^3 - 15x^2 - 6x - 1 \\
l_6(x) &= 1024x^{11} + 4608x^{10} + 9216x^9 + 10752x^8 \\
&+ 8096x^7 + 4176x^6 + 1616x^5 + 568x^4 \\
&+ 206x^3 + 71x^2 + 20x + 3 \\
l_7(x) &= 32x^6 + 64x^5 + 48x^4 + 16x^3 + 3x^2 + 2x + 1
\end{aligned}
$$

First, for an element $f \in \mathbb{F}_{p^{16}}$, we need to compute $f := f^x$ at 13 times (f^{x^i}, $1 \leq i \leq 13$) and this requires $13 \cdot (48S_{16} + 3M_{16}) = 36855M_1$ since $x = 2^{48} + 2^{32} + 2^7 + 1$.

Second, we compute $(f^{x^i})^{p^j}$ with $682M_1$ for the coefficients of $l_i(x)$ as described in (Scott et al., 2009, Section 5).

Finally, we should a vectorial addition chain such as (Scott et al., 2009, Section 5) to compute the multi-exponentiation. To do this we need to compute an addition chain from coefficients set from $l_i(x)$, and we get

[1, 2, 3, 4, 6, 7, 8, 14, 15, 16, 20, 22, 26, 27, 32, 36, 43, 48, 64, 66, 68, 71, 80, 111, 112, 120, 124, 128, 160, 163, 196, 206, 256, 320, 328, 348, 384, 480, 512, 520, 568, 570, 896, 960, 980, 1024, 1120, 1344, 1348, 1360, 1616, 1676, 2048, 2256, 2272, 2752, 3072, 3584, 3592, 4096, 4608, 4656, 4712, 4716, 7408, 7528, 8096, 8352, 9216, 10240, 10752, 10864, 11776, 12912, 16448, 16704, 22528, 23040, 26944, 27968, 28352, 30720, 30752, 31264, 31872, 53760, 56320, 59840, 84480, 84608].

We then compute a vectorial addition chain from this chain and obtain a chain of length 230. This implies $230 - 71 = 159$ multiplications in $\mathbb{F}_{p^{16}}$ including 3 squarings where 71 is the number of unit vectors. Consequently the final exponentiation requires $36855M_1 + 3S_{16} + 156M_{16} = 49653M_1$.

5.3 Comparison

In (Aranha et al., 2013), the authors showed that the pairing over the BLS curves of embedding degree 12 (BLS12) is the most efficient. Here we compare our cost estimates of the twisted Ate pairing over the Kawazoe-Takahashi curve with the result of the optimal pairing over the BLS12 in Table 1.

Table 1: Comparison of the computation cost of pairing over the pairing-friendly curve of genus 1 (BLS12) and genus2 (Kawazoe-Takahashi).

Curve	Phase	Mult. in $\mathbb{F}_p$	scaled
BLS12	Miller loop	$10865M_{640}$	$10865M_{640}$
	Final exp.	$8464M_{640}$	$8464M_{640}$
	Total	$19329M_{640}$	$19329M_{640}$
Kawazoe -Takahashi	Miller loop	$23221M_{704}$	$28098M_{640}$
	Final exp.	$49653M_{704}$	$60081M_{640}$
	Total	$72874M_{704}$	$88178M_{640}$

As described in (Aranha et al., 2013, Section 8), they represent field elements $a \in \mathbb{F}_p$ as n-bit processor words ($n = \lceil 1/\ell \rceil$, $\ell = 1 + \lfloor \log_2 p \rfloor$) and estimate the cost of field arithmetic so we should use M_{704} for comparison. We simply normalize the cost of our pairing so that $M_{704} = 1.21M_{640}$ where $1.21 = (704/640)^2$ and the data in "scaled" column are given by multiplying 1.21 to each element.

In Miller loop, the cost of Kawazoe-Takahashi pairing is about three times than the one of BLS12 pairing. Now the loop length of our pairing is twice as much as optimal one, so the Miller loop cost seemed not to be high and be efficient more of less thanks to using degenerate divisor and other techniques like denominator elimination.

On the other hand, the final exponentiation cost of our pairing is very high than the one of BLS12 since the arithmetic cost in $\mathbb{F}_{p^{16}}$ is relatively high than one in $\mathbb{F}_{p^{12}}$ due to construction of their fields.In addition, strategy to compute multi-exponentiation in final exponentiation is more complicated than when $k = 12$.

6 CONCLUSION

Aranha et al. (Aranha et al., 2013) clarify appropriate pairing-friendly elliptic curves and optimal pairings over the curves at high (192-bit) security level. In this paper, we considered several pairings over Kawazoe-Takahashi curves of embedding degree 16 and propose the twisted Ate pairing as most efficient one. We showed the method to construct the optimal pairings and its twisted version. Although the Miller loop becomes twice as much as optimal one, we offered a twisted version of Ate pairing since the

degree of twist is 8 which is half of the embedding degree to avoid performing arithmetic on divisor classes defined over the extension field. We described that some techniques to reduce the computation cost as described in (Fan et al., 2008) can apply to our twisted Ate pairing.

As shown in our cost estimates, the final exponentiation cost is much larger than the stat-of-the-art elliptic pairing. We should consider other embedding degree such as $k = 12$ to reduce complicated multi-exponentiation, although we cannot take appropriate r as an order of Jacobian whose size is close to 384-bit. The other alternative, we consider to take $k = 15$ or 27 so that the embedding degrees are coprime to degree of the twist. In this case, we can construct twisted pairings whose length of Miller loop are optimal unlike the situation in 4.2. We will tackle to construct the curves which have the above embedding degrees and a twisted Ate pairing on each curve as a future work. In addition, other pairing-friendly ordinary curves of genus 2 like (Freeman and Satoh, 2011) should be explored whether these curves are appropriate for constructing pairings at high security level.

Furthermore, we should explicitly construct extension fields and optimize the arithmetic on these field to obtain detailed cost estimate. We will implement the pairing on Haswell CPU using the SIMD instructions (AVX2) and show experimental result in practice.

REFERENCES

Aranha, D., Fuentes-Castaeda, L., Knapp, E., Menezes, A., and Rodrguez-Henrquez, F. (2013). Implementing pairings at the 192-bit security level. In Abdalla, M. and Lange, T., editors, *Pairing-Based Cryptography Pairing 2012*, volume 7708 of *Lecture Notes in Computer Science*, pages 177–195. Springer Berlin Heidelberg.

Balakrishnan, J., Belding, J., Chisholm, S., Eisenträger, K., Stange, K. E., and Teske, E. (2009). Pairings on hyperelliptic curves. CoRR, abs/0908.3731, Available: http://arxiv.org/abs/0908.3731v2.

Barbulescu, R., Gaudry, P., Guillevic, A., and Morain, F. (2015). Improving NFS for the discrete logarithm problem in non-prime finite fields. In Oswald, E. and Fischlin, M., editors, *Advances in Cryptology – EUROCRYPT 2015*, volume 9056 of *Lecture Notes in Computer Science*, pages 129–155. Springer Berlin Heidelberg.

Barbulescu, R., Gaudry, P., Joux, A., and Thom, E. (2014). A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In Nguyen, P. and Oswald, E., editors, *Advances in Cryptology EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 1–16. Springer Berlin Heidelberg.

BlueKrypt (2012). - cryptographic key length recommendation, http://www.keylength.com.

Bosma, W., Cannon, J., and Playoust, C. (1997). The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265. Computational algebra and number theory (London, 1993).

Fan, X., Gong, G., and Jao, D. (2008). Speeding up pairing computations on genus 2 hyperelliptic curves with efficiently computable automorphisms. In Galbraith, S. and Paterson, K., editors, *Pairing-Based Cryptography Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 243–264. Springer Berlin Heidelberg.

Fan, X., Gong, G., and Jao, D. (2009). Efficient pairing computation on genus 2 curves in projective coordinates. In Avanzi, R., Keliher, L., and Sica, F., editors, *Selected Areas in Cryptography*, volume 5381 of *Lecture Notes in Computer Science*, pages 18–34. Springer Berlin Heidelberg.

Freeman, D. M. and Satoh, T. (2011). Constructing pairing-friendly hyperelliptic curves using weil restriction. *Journal of Number Theory*, 131(5):959 – 983. Elliptic Curve Cryptography.

Frey, G. and Lange, T. (2006). Fast bilinear maps from the tate-lichtenbaum pairing on hyperelliptic curves. In Hess, F., Pauli, S., and Pohst, M., editors, *Algorithmic Number Theory*, volume 4076 of *Lecture Notes in Computer Science*, pages 466–479. Springer Berlin Heidelberg.

Galbraith, S. D., Lin, X., and Morales, D. J. M. (2008). Pairings on hyperelliptic curves with a real model. In Galbraith, S. and Paterson, K., editors, *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 265–281. Springer-Verlag.

Granger, R., Hess, F., Oyono, R., Thriault, N., Vercauteren, F., and Berlin, T. U. (2007). Ate pairing on hyperelliptic curves. In *In Advances in Cryptology EUROCRYPT 2007*, pages 419–436. Springer-Verlag.

Guillevic, A. and Vergnaud, D. (2013). Genus 2 hyperelliptic curve families with explicit jacobian order evaluation and pairing-friendly constructions. In Abdalla, M. and Lange, T., editors, *Pairing-Based Cryptography Pairing 2012*, volume 7708 of *Lecture Notes in Computer Science*, pages 234–253. Springer Berlin Heidelberg.

Hess, F. (2008). Pairing lattices. In Galbraith, S. and Paterson, K., editors, *Pairing-Based Cryptography – Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 18–38. Springer-Verlag.

Kachisa, E. (2010). Generating more kawazoe-takahashi genus 2 pairing-friendly hyperelliptic curves. In Joye, M., Miyaji, A., and Otsuka, A., editors, *Pairing-Based Cryptography - Pairing 2010*, volume 6487 of *Lecture Notes in Computer Science*, pages 312–326. Springer Berlin Heidelberg.

Kawazoe, M. and Takahashi, T. (2008). Pairing-friendly hyperelliptic curves with ordinary jacobians of type

$y^2 = x^5 + ax$. In Galbraith, S. and Paterson, K., editors, *Pairing-Based Cryptography Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 164–177. Springer Berlin Heidelberg.

Lange, T. (2005). Formulae for arithmetic on genus 2 hyperelliptic curves. *Applicable Algebra in Engineering, Communication and Computing*, 15(5):295–328.

Scott, M. (2011). On the efficient implementation of pairing-based protocols. In Chen, L., editor, *Cryptography and Coding*, volume 7089 of *Lecture Notes in Computer Science*, pages 296–308. Springer Berlin Heidelberg.

Scott, M., Benger, N., Charlemagne, M., Dominguez Perez, L., and Kachisa, E. (2009). On the final exponentiation for calculating pairings on ordinary elliptic curves. In Shacham, H. and Waters, B., editors, *Pairing-Based Cryptography Pairing 2009*, volume 5671 of *Lecture Notes in Computer Science*, pages 78–88. Springer Berlin Heidelberg.

Teruya, T., Saito, K., Kanayama, N., Kawahara, Y., Kobayashi, T., and Okamoto, E. (2014). Constructing symmetric pairings over supersingular elliptic curves with embedding degree three. In Cao, Z. and Zhang, F., editors, *Pairing-Based Cryptography – Pairing 2013*, volume 8365 of *Lecture Notes in Computer Science*, pages 97–112. Springer-Verlag.

Vercauteren, F. (2010). Optimal pairings. *IEEE Transactions on Information Theory*, 56(1):455–461.

Zhang, F. (2010). Twisted ate pairing on hyperelliptic curves and applications. *Science China Information Sciences*, 53(8):1528–1538.

Zhang, X. and Wang, K. (2014). Fast symmetric pairing revisited. In Cao, Z. and Zhang, F., editors, *Pairing-Based Cryptography – Pairing 2013*, volume 8365 of *Lecture Notes in Computer Science*, pages 131–148. Springer-Verlag.