種数 2 の Kawazoe-Takahashi 曲線族上の optimal ペアリングの構成とそのコスト評価

石井 将大 †　　猪俣 敦夫 ‡　　藤川 和利 ‡

† 奈良先端科学技術大学院大学
〒 630-0192 奈良県生駒市高山町 8916-5
‡ 奈良先端科学技術大学院大学総合情報基盤センター
〒 630-0192 奈良県生駒市高山町 8916-5

ああ　近年，小標数の体における DLP を解くアルゴリズムの進化に大きなブレークスルーがあり，対称 (type 1) ペアリングの暗号としてのセキュリティレベルが著しく低下してしまった．本研究では種数 2 の ordinary な超楕円曲線に注目し，その上の高 (192-bit) セキュリティレベルな optimal ペアリングの構成を目的とする．本稿において，我々は川添と高橋による曲線族に対する optimal ペアリングの構成を示し，コスト評価を行い同セキュリティレベルにおける楕円曲線上のペアリングとの比較を行う．

A construction of an optimal pairing on a family of Kawazoe-Takahashi curves and its cost estimate

Masahiro ISHII†　　Atsuo INOMATA‡　　Kazutoshi FUJIKAWA‡

†Nara Institute of Science and Technology
8916-5 Takayama, Ikoma, NARA 630-0192 JAPAN
‡Information Initiative Center, Nara Institute of Science and Technology
8916-5 Takayama, Ikoma, NARA 630-0192 JAPAN

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. We focus on the ordinary hyperelliptic curves of genus 2 and the optimal (ate) 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 we 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 [5, 4]. 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 [17, 20] and in genus 2 case [8]. Their pairings, however, are not suitable for the situation required high security level because of their small embedding degree.

Aranha et al. [2] 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 [11, 18] 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 [15].

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 its twisted version over the family of pairing-friendly curves of genus 2 by Kawazoe and Takahashi [13]

The remainder of this paper is organized as follows. We recall background on several pairings on hyperelliptic 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 [11] and Vercauteren [18] 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* [3] given by Hess [11] and Vercauteren [18] 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 [9] and twisted Ate pairings [19]. 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 obtaion the bilinear pairing (HV pairing) [3, 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' of degree d, i.e. d is the minimal integer satisfying that there exists an isomorphism $\phi\colon C' \to C$ over $\mathbb{F}_{q^d}$, a twisted version of the HV pairing exists [3, Remark 4.4]. We suppose that $\gcd(k, \sharp\mathrm{Aut}(C)) \neq 1$, then

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

is also a bilinear and non-degenerate (under same condition of HV pairings) pairing [11, 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 [19]). 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 [13, 12, 7, 10]. In this paper, we focus on Kawazoe-Takahashi curve [13] 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 [13, 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} [1]. We can find the following curve by using [13, Theorem 2]:

$$C\colon y^2 = x^5 + 13x,$$

$$\begin{aligned}
r &= 970053380833451821617465434935 5\backslash \\
&= 397572264120550978492658575160 5\backslash \\
&= 813457742421583955683941992667 7\backslash \\
&= 69788763002584662060161 \text{ (386 bits)}, \\
p &= 797324042316494540513975355795 7\backslash \\
&= 192318655792488325781794245462 8\backslash \\
&= 847218329471009457950461460860 6\backslash \\
&= 786038699393867681595656366718 9\backslash \\
&= 001194210640477412481923550795 0\backslash \\
&= 387525398745502094536069222059 8\backslash \\
&= 88176854760162721 \text{ (675 bits)}, \\
t &= 343540705870559 \text{ (49 bits)},
\end{aligned}$$

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 as offered in elliptic case by [2], 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 [18], 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 [18]. 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 [6] 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

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

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

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

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

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 $d = 8$

$$C' \colon y^2 = x^5 + 13\lambda x,$$
$$\phi \colon C' \to C$$
$$(x, y) \mapsto (\lambda^{\frac{1}{4}} x, \lambda^{\frac{5}{8}} y)$$

where $\lambda \in \mathbb{F}_p$ is not l-th power residue in $\mathbb{F}_p$ for $l \in \{1, 2, 4, 8\}$.

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

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

Therefore, we should search short vectors for $h(x)$ where the coefficients of p^i (i: odd) 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 twise 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 [19] 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 [19, 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.

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 implemented the pairing and arithmetic on the field $\mathbb{F}_p$ and $\mathbb{F}_{p^{16}}$ yet. The cost we show here is somewhat rough and the cost of final exponentiation is only described its estimated upper limit.

The extension field $\mathbb{F}_p^{16}$ should be constructed the tower of quadratic extension fields

$$\mathbb{F}_{p^{16}}/\mathbb{F}_{p^8}/\mathbb{F}_{p^4}/\mathbb{F}_{p^2}/\mathbb{F}_p.$$

We denote a multiplication in $\mathbb{F}_{p^i}$ by M_i. We assume to use Karatsuba method for multiplication in each field, so $M_{16} = 81M_1$. We also suppose that the cost of a squaring equal to one of a multiplication.

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. We use the algorithm to do arithmetic on the divisor group by Lange [14] so the cost

of a doubling is $I_1 + 5S_1 + 22M_1 = 37M_1$ and the one of an addition is $I_1 + 3S_1 + 22M_1 = 35M_1$ where we assume that $I_1 = 10M_1$.

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 elements of D_2 can be represented by twist C' over $\mathbb{F}_{p^2}$ we can use denominator elimination so we need not to evaluate $u'(x)$. Let f be the intermidiate pairing value, in each doubling step we compute

$$f^2(y_1 - v(x_1))(y_2 - v(x_2))$$

requiring $2 \cdot 78M_1 + 3M_{16} = 399M_1$, and in each addition step computing

$$f(y_1 - v(x_1))(y_2 - v(x_2))$$

requires $2 \cdot 78M_1 + 2M_{16} = 318M_1$. Therefore the Miller loop requires totally $\{96(37+399)+53(35+318)\}M_1 = 60565M_1$.

5.2 Final exponentiation

For efficient computation of the final exponentiation, we should use the method by Scott et al. [16]. 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

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

The degree of each coefficient $l_i(x)$ is at most 13, and the total number of coefficients which are not zero in all $l_i(x)$ is 84. For an element $f \in \mathbb{F}_{p^{16}}$, we need to compute $f := f^x$ at 13 times and in worst case we must act 284 Frobenius map to the element of $\mathbb{F}_{p^{16}}$. In addition we estimate the size of coefficients of $l_i(x)$ to be as a larger ones, we should $84 \cdot 15$ multiplications in $\mathbb{F}_{p^{16}}$. Therefore, we suppose the cost of the final exponentiation does not exceed $2196M_{16} + 284F_r = 177876M_1 + 284F_r$.

5.3 Comparison

In [2], BLS12 pairing is the most efficient and the Miller loop requires $19329m_{640}$. In our case the Miller loop required $60565m_{704}$ (assuming implementation on 64-processor) and it costs about 3 times as high as elliptic case.

The estimated cost of final exponentiation is extremely high, we need to apply the optimization method to this in order to obtain accurate estimates.

6 Conclusion

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

参考文献

[1] Bluekrypt - cryptographic key length recommendation, `http://www.keylength.com`

[2] Aranha, D., Fuentes-Castaeda, L., Knapp, E., Menezes, A., Rodrguez-Henrquez, F.: Implementing pairings at the 192-bit security level. In: Abdalla, M., Lange, T. (eds.) Pairing-Based Cryptography Pairing 2012. Lecture

Notes in Computer Science, vol. 7708, pp. 177–195. Springer Berlin Heidelberg (2013)

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

[4] Barbulescu, R., Gaudry, P., Guillevic, A., Morain, F.: Improving NFS for the discrete logarithm problem in non-prime finite fields. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology – EUROCRYPT 2015. Lecture Notes in Computer Science, vol. 9056, pp. 129–155. Springer Berlin Heidelberg (2015)

[5] Barbulescu, R., Gaudry, P., Joux, A., Thom, E.: A heuristic quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic. In: Nguyen, P., Oswald, E. (eds.) Advances in Cryptology EUROCRYPT 2014. Lecture Notes in Computer Science, vol. 8441, pp. 1–16. Springer Berlin Heidelberg (2014)

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

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

[8] Galbraith, S.D., Lin, X., Morales, D.J.M.: Pairings on hyperelliptic curves with a real model. In: Galbraith, S., Paterson, K. (eds.) Pairing-Based Cryptography – Pairing 2008. Lecture Notes in Computer Science, vol. 5209, pp. 265–281. Springer-Verlag (2008)

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

[10] Guillevic, A., Vergnaud, D.: Genus 2 hyperelliptic curve families with explicit jacobian order evaluation and pairing-friendly constructions. In: Abdalla, M., Lange, T. (eds.) Pairing-Based Cryptography Pairing 2012. Lecture Notes in Computer Science, vol. 7708, pp. 234–253. Springer Berlin Heidelberg (2013)

[11] Hess, F.: Pairing lattices. In: Galbraith, S., Paterson, K. (eds.) Pairing-Based Cryptography – Pairing 2008. Lecture Notes in Computer Science, vol. 5209, pp. 18–38. Springer-Verlag (2008)

[12] Kachisa, E.: Generating more kawazoe-takahashi genus 2 pairing-friendly hyperelliptic curves. In: Joye, M., Miyaji, A., Otsuka, A. (eds.) Pairing-Based Cryptography - Pairing 2010. Lecture Notes in Computer Science, vol. 6487, pp. 312–326. Springer Berlin Heidelberg (2010)

[13] Kawazoe, M., Takahashi, T.: Pairing-friendly hyperelliptic curves with ordinary jacobians of type $y^2 = x^5 + ax$. In: Galbraith, S., Paterson, K. (eds.) Pairing-Based Cryptography Pairing 2008. Lecture Notes in Computer Science, vol. 5209, pp. 164–177. Springer Berlin Heidelberg (2008)

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

[15] Scott, M.: On the efficient implementation of pairing-based protocols. In: Chen,

L. (ed.) Cryptography and Coding. Lecture Notes in Computer Science, vol. 7089, pp. 296–308. Springer Berlin Heidelberg (2011)

[16] Scott, M., Benger, N., Charlemagne, M., Dominguez Perez, L., Kachisa, E.: On the final exponentiation for calculating pairings on ordinary elliptic curves. In: Shacham, H., Waters, B. (eds.) Pairing-Based Cryptography Pairing 2009. Lecture Notes in Computer Science, vol. 5671, pp. 78–88. Springer Berlin Heidelberg (2009), http://dx.doi.org/10.1007/978-3-642-03298-1_6

[17] Teruya, T., Saito, K., Kanayama, N., Kawahara, Y., Kobayashi, T., Okamoto, E.: Constructing symmetric pairings over supersingular elliptic curves with embedding degree three. In: Cao, Z., Zhang, F. (eds.) Pairing-Based Cryptography – Pairing 2013. Lecture Notes in Computer Science, vol. 8365, pp. 97–112. Springer-Verlag (2014)

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

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

[20] Zhang, X., Wang, K.: Fast symmetric pairing revisited. In: Cao, Z., Zhang, F. (eds.) Pairing-Based Cryptography – Pairing 2013. Lecture Notes in Computer Science, vol. 8365, pp. 131–148. Springer-Verlag (2014)