International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 13, Number 2, pages 242–257, July 2023

Improvement of Miller Loop for a Pairing on FK12 Curve and Evaluation with other STNFS Curves

Kazuma Ikesaka[†], Yuki Nanjo[††], Yuta Kodera[†], Takuya Kusaka[†] and Yasuyuki Nogami[†]

[†] *Okayama University* 3-1-1, Tsushima-naka, Kita, Okayama 700-8530, Japan

[††] *Toshiba Corporation* 1-1, Shibaura 1-chome, Minato-ku, Tokyo 105-8001, Japan.

Received: February 15, 2023
Revised: May 5, 2023
Accepted: June 1, 2023
Communicated by Toru Nakanishi

Abstract

Pairing is carried out by two steps, Miller loop and final exponentiation. In this manuscript, the authors propose an efficient Miller loop for a pairing on the FK12 curve. A Hamming weight and bit-length of loop parameter have a great effect on the computational cost of the Miller loop. Optimal-ate pairing is used as the most efficient pairing on the FK12 curve currently. The loop parameter of optimal-ate pairing is $6z + 2$ where z is the integer to make the FK12 curve parameter. Our method uses z which has a shorter bit-length than the previous optimal-ate pairing as the loop parameter. Usually, z has a low Hamming weight to make final exponentiation efficient. Therefore, the loop parameter in our method has a lower Hamming weight than the loop parameter of the previous one in many cases. The authors evaluate our method by the number of multiplications and execution time. As a result, the proposed algorithm leads to a 3.71% reduction in the number of multiplications and a 3.03% reduction in the execution time. In addition, the authors implement other STNFS secure curves and evaluate these curves from viewpoint of execution time.

Keywords: pairing based cryptography, STNFS, Miller loop

1 Introduction

A pairing on the elliptic curve is a special map which has two properties, bilinear and non-degenerate. The pairing is used for innovative protocols such as ID-based cryptography and Attribute-Based Encryption, however, the pairing computation is the bottleneck of implementation. Therefore, an efficient pairing implementation is essential to use these innovative protocols practically. The safety of pairing is based on the difficulties to solve a finite field discrete logarithm problem (FFDLP) and an elliptic curve discrete logarithm problem (ECDLP). However, the Tower of Number Field Sieve (TNFS) [1, 2] and special TNFS (STNFS) [3, 4] are improved in these years. These methods solve the FFDLP which is one of the safeties of the pairing. Especially, STNFS is an attacking method for the extension field that is used for pairing implementation. To against these attacking methods, new parameters and new curves are proposed. In [5], STNFS secure curves are listed. The Fotiadis-Konstantinou curve with embedding degree 12 (FK12) is one of the STNFS secure curves and according to [6], it has high efficiency as well as the BLS12 curve which is known as one of the best STNFS secure curves at the 128-bit security level. For the final exponentiation of pairing on

the FK12 curve, Ikesaka et al. improved the algorithm to compute it in [7]. In this manuscript, we improve the efficiency of pairing on the FK12 curve.

The pairing on an elliptic curve is carried out by two steps which are called the Miller loop and the final exponentiation and there are many optimization methods corresponding to curves on which pairings are defined. In this manuscript, the authors focus on the Miller loop. The efficiency of the Miller loop depends on a loop parameter. In other words, a loop parameter is desired to have a low Hamming weight and short bit-length for an efficient Miller loop. For pairing on various curves, ate pairing and optimal-ate pairing are known as methods to make an efficient Miller loop. In [6], an optimal-ate pairing on the FK12 curve is proposed. A loop parameter of the optimal-ate pairing on the FK12 curve is $6z+2$, where z is an integer to parameterize the elliptic curve. If we make a loop parameter smaller, the Miller loop becomes more efficient. Therefore, in this manuscript, we aim to make a more efficient pairing by using z as a loop parameter for the Miller loop.

In the case of pairing on the BN12 curve, a loop parameter of the optimal-ate pairing is $6z+2$ by applying [8]. To reduce the computational cost of the Miller loop for pairing on the BN12 curve Nogami et al. proposed Xate pairing in [9]. This work proved that z which has a shorter bit-length than $6z+2$ can be a loop parameter for pairing on the BN12 curves. Xate pairing is based on relation with p, r, t where p, r, t are parameters of BN12 curve. Nogami et al. made Xate pairing from ate pairing by using the relation with p, r, and t. There is the possibility to make smaller loop parameters for pairing on the FK12 curve by applying the Xate pairing method.

For pairing on the FK12 curve, we find the relationship with p, r, t and construct a pairing on FK12 that has the shortest Miller loop parameter z, which is called the Xate pairing on FK12 for convenience. To ensure the validity of the obtained pairings, the authors prove the bilinearity of Xate pairing on the FK12 curve. The authors also estimate the calculation cost of optimal-ate pairing and Xate pairing on FK12 based on the number of $\mathbb{F}_p$-multiplication to compare the efficiency of them. Finally, the authors implement them with C programming language and compare their execution times. As a result, the proposed algorithm leads to a 3.71% reduction in the number of multiplications and a 3.03% reduction in the execution time.

This paper is an extended version of the authors' previous work [10] in CANDAR'22. The previous version provided Xate pairing on the FK12 curve and evaluate their efficiency of them. In [5], several curves are listed as STNFS secure curves such as the BLS12 curve and Cocks-Pinch curve with embedding degree $k = 6, 8$. These curves are listed with parameters for the 128-bit security level. Therefore, the authors implement these curves and measure the execution times of pairing on these curves. In this manuscript, the authors show the computational evaluation of the STNFS secures curve which includes the FK12 curve.

The rest of this manuscript is organized as follows. Sect. 2 provides a brief background on this research. Sect. 3 provides related works, optimal-ate pairing on FK12 and ate-like pairing on BN12. In Sect. 4, the authors propose Xate pairing on the FK12 curve and verify the effect of the proposed method. Sect. 5 provides the evaluation for execution times of the STNFS secure curve which includes the FK12 curve. Finally, Sect. 6 is the conclusion of this research.

2 Background

In this section, the authors describe the background of this research. In this manuscript, let p be a prime number that is larger than 3 and $\mathbb{F}_p$ be a prime field with characteristic p. Let $\mathbb{F}_q$ be an extension field of degree m over $\mathbb{F}_p$ where m is a positive integer and $q = p^m$.

2.1 Elliptic Curves on Finite Fields

An elliptic curve over $\mathbb{F}_p$ is defined as follows:

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b.$$

Note that a and b are elements over $\mathbb{F}_p$ and they satisfy $4a^3 + 27b^2 \neq 0$. Let $E(\mathbb{F}_p)$ be a set of rational points on the curve, including the infinity point $\mathcal{O}$. In this set, the elliptic curve addition

between P and Q is defined where P and Q are arbitrary rational points on the curve. Then, $E(\mathbb{F}_p)$ performs an elliptic curve additive group, and the infinity point $\mathcal{O}$ is the unity of the group. For a positive integer s, a point multiplication endomorphism, scalar multiplication, is defined by $[s] : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q), P \mapsto P + P + \cdots + P$ which involves $(s-1)$-times additions. In this paper, the order of the $E(\mathbb{F}_p)$ is denoted by $\#E(\mathbb{F}_p)$. The order of the $E(\mathbb{F}_p)$ is given with Frobenius trace t as follows:

$$\#E(\mathbb{F}_p) = p + 1 - t.$$

Let r be a prime that is not equal to p and $r \mid \#E(\mathbb{F}_p)$. The set of curves which parameterized $p(x), r(x), t(x)$ is called a family of curves, if the three parameters p, r, t are given by polynomials $p(x), r(x), t(x)$. The smallest positive integer k that satisfies $r \mid (p^k - 1)$ is called the embedding degree. Let π_p be the Frobenius endomorphism defined as follows:

$$\pi_p : E \to E : (x, y) \mapsto (x^p, y^p),$$

where x and y are x-coordinate and y-coordinate of rational points on elliptic curve, respectively. The Frobenius endomorphism can be computed with low computational costs, therefore using the Frobenius endomorphism efficiently is one of the important points in reducing the pairing computational costs.

2.2 FK12 Curves

In this section, the authors explain FK12. The FK family is one of the STNFS-secure pairing-friendly curves[11]. Moreover, the FK12 curve is one of the efficient curves for STNFS-secure pairing at the 128-bit security level.

The FK12 curve is parameterized by the following parameters.

$$\begin{cases} p(x) &= 1728x^6 + 2160x^5 + 1548x^4 \\ & \qquad +756x^3 + 240x^2 + 54x + 7, \\ r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1, \\ t(x) &= -6x^2 + 1. \end{cases}$$

To identify the curve, an integer z is needed that $p(z)$ and $r(z)$ are prime numbers respectively. In this manuscript, the authors use $z = -2^{72} - 2^{46} - 2^8 - 2$ as a parameter for the pairing at the 128-bit security level. We define base-field and a trace-zero subgroup of $E[r]$ defined as follows:

$$\begin{cases} \mathbb{G}_1 &= E[r] \cap \ker(\pi_p - [1]) \\ \mathbb{G}_2 &= E[r] \cap \ker(\pi_p - [p]). \end{cases}$$

2.3 Divisor

Let f be a rational function on E defined over $\mathbb{F}_q$. Let $\mathrm{ord}_P(f)$ count the multiplicity of f at a point P, which is positive if f has a zero at P, and negative if f has a pole at P. Then, a *divisor of a rational function* f is defined as follows:

$$\mathrm{div}(f) = \sum_{P \in E(\mathbb{F}_q)} \mathrm{ord}_P(f)(P).$$

The divisor $\mathrm{div}(f)$ denotes a multi-set of intersection points and their multiplicities of f and E. For two rational functions f and g, there are properties such that $\mathrm{div}(f \cdot g) = \mathrm{div}(f) + \mathrm{div}(g)$, $\mathrm{div}(f/g) = \mathrm{div}(f) - \mathrm{div}(g)$, and only if $f = c \cdot g$ with $c \in \mathbb{F}_q^*$, $\mathrm{div}(f) = \mathrm{div}(g)$.

For example, let $l_{P,Q}$ be a line function on E defined over $\mathbb{F}_q$, which intersects points $P, Q \in E(\mathbb{F}_q)$. Indeed, $l_{P,Q}$ intersects E in three points, which are denoted as P, Q, and $-(P+Q)$, all with multiplicity 1. Note that $l_{P,Q}$ also intersects E with multiplicity -3 at $\mathcal{O}$, i.e., l has a pole of order 3 at $\mathcal{O}$. Thus, a divisor of $l_{P,Q}$ is denoted as $\mathrm{div}(l_{P,Q}) = (P) + (Q) + (-(P+Q)) - 3(\mathcal{O})$. If $P = -Q$, i.e., $l_{P,Q}$ is a vertical line and is especially denoted as v_P, a divisor of v_P is denoted as

$\mathrm{div}(v_P) = (P) + (-P) + (\mathcal{O}) - 3(\mathcal{O}) = (P) + (-P) - 2(\mathcal{O})$. Then, a divisor of function $l_{P,Q} \cdot v_P$ is given by $\mathrm{div}(l_{P,Q} \cdot v_P) = \mathrm{div}(l_{P,Q}) + \mathrm{div}(v_P) = 2(P) + (-P) + (Q) + (-(P+Q)) - 5(\mathcal{O})$. Any divisor of a rational function on E can be expressed by using a combination of divisors of line functions, i.e., any rational function can be built by line functions.

For an integer s, there is a rational function $f_{s,P}$ on E defined over $\mathbb{F}_q$ with divisor $\mathrm{div}(f_{s,P}) = s(P) - ([s]P) - (s-1)(\mathcal{O})$, which plays an important role in the pairing. In [12], Miller gave an iterative algorithm for constructing $f_{s,P}$ with loop length $\log_2 s$, which is called Miller's algorithm. The following lemmas show the properties associated with this function.

Lemma 1 *For integers a, b and $d > 0$, the followings are true.*

(a) $f_{ab,P} = f_{a,P}^b \cdot f_{b,[a]P}$,
(b) $f_{a+b,P} = f_{a,P} \cdot f_{b,P} \cdot \frac{l_{a[P],[b]P}}{v_{[a+b]P}}$.

For $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, the following is true.

(c) $f_{a,\pi_p^d(Q)}(P) = f_{a,Q}^{p^d}(P)$.

Proof. (a) and (b) can be proved easily by writing down the divisors for the functions involved. It is enough to show the left and right sides have the same divisors.

(a)

$$\begin{aligned}
\mathrm{div}(f_{ab,P}) &= ab(P) - ([ab]P) - (ab-1)(\mathcal{O}) \\
&= ab(P) - b([a]P) - (ab-b)\mathcal{O} + b([a]P) - ([ab]P) - (b-1)\mathcal{O} \\
&= b(a(P) - ([a]P) - (a-1)\mathcal{O}) + (b([a]P) - ([ab]P) - (b-1)\mathcal{O}) \\
&= b \cdot \mathrm{div}(f_{a,P}) + \mathrm{div}(f_{b,[a]P}) \\
&= \mathrm{div}(f_{a,P}^b) + \mathrm{div}(f_{b,[a]P}) \\
&= \mathrm{div}(f_{a,P}^b \cdot f_{b,[a]P}).
\end{aligned}$$

(b)

$$\begin{aligned}
\mathrm{div}(f_{a+b,P}) &= (a+b)(P) - ([a+b]P) - (a+b-1)(\mathcal{O}) \\
&= a(P) - ([a]P) - (a-1)(\mathcal{O}) + b(P) - ([b]P) \\
&\qquad - (b-1)(\mathcal{O}) + ([a]P) + ([b]P) - ([a+b]P) - (\mathcal{O}) \\
&= (a(P) - ([a]P) - (a-1)(\mathcal{O})) + (b(P) - ([b]P) - (b-1)(\mathcal{O})) \\
&\quad + (([a]P) + ([b]P) + (-[a+b]P) - 3(\mathcal{O})) - (([a+b]P) + (-[a+b]P) - 2(\mathcal{O})) \\
&= \mathrm{div}(f_{a,P}) + \mathrm{div}(f_{b,P}) + \mathrm{div}(l_{[a]P,[b]P}) - \mathrm{div}(v_{[a+b]P}) \\
&= \mathrm{div}\left(f_{a,P} \cdot f_{b,P} \cdot \frac{l_{[a]P,[b]P}}{v_{[a+b]P}} \right).
\end{aligned}$$

(c) Let $P \in \forall\mathbb{G}_1$ and $Q_1, Q_2, Q_3 \in \forall\mathbb{G}_2$. $f_{a,Q}^{p^d}(P)$ is constructed with $l_{Q_1,Q_2}(P)$ and $v_{Q_3}(P)$. Since the following relations hold, $f_{a,\pi_p^d(Q)}(P) = f_{a,Q}^{p^d}(P)$ is true.

(i) $l_{Q_1,Q_2}^{p^d}(P) = l_{\pi_p^d(Q_1),\pi_p^d(Q_2)}(P)$,
(ii) $v_{Q_3}^{p^d}(P) = v_{\pi_p^d(Q_3)}(P)$.

Proof of (i)
We note that $x_{Q_1}, y_{Q_1}, x_{Q_2}, y_{Q_2}, x_P, y_P$ are x and y coordinates of Q_1, Q_2, P respectively. Then, the line function $l_{Q_1,Q_2}(P)$ is given as follows:

$$l_{Q_1,Q_2}(P) = \lambda(x_P - x_{Q_1}) - (y_P - y_{Q_1}),$$

where λ is as follows:

$$\lambda = \begin{pmatrix} \dfrac{y_{Q_2} - y_{Q_1}}{x_{Q_2} - x_{Q_1}} & Q_1 \neq Q_2, x_{Q_1} \neq x_{Q_2} \\ \dfrac{3x_{Q_1}^2}{2y_{Q_1}} & Q_1 = Q_2, y_{Q_1} \neq 0 \end{pmatrix}.$$

Then, we obtain the following relation:

$$\begin{aligned} l_{Q_1,Q_2}(P)^{p^d} &= \sum_{k=0}^{p^d} \binom{n}{k} \{\lambda(x_P - x_{Q_1})\}^k (-1)^{n-k} (y_P - y_{Q_1})^{n-k} \\ &= \{\lambda(x_P - x_{Q_1})\}^{p^d} + \sum_{k=1}^{p^d-1} \binom{n}{k} \lambda(x_P - x_{Q_1})^k (-1)^{n-k} (y_P - y_{Q_1})^{n-k} + (-1)^{p^d} (y_P - y_{Q_1})^{p^d} \\ &= \{\lambda(x_P - x_{Q_1})\}^{p^d} + \sum_{k=1}^{p^d-1} \binom{n}{k} \lambda(x_P - x_{Q_1})^k (-1)^{n-k} (y_P - y_{Q_1})^{n-k} - (y_P - y_{Q_1})^{p^d} \\ & \qquad \because p^d \text{ is odd} \end{aligned}$$

The second term of the above equation can be ignored because it is a multiple of p. Similarly to the above, we obtain the following relation:

$$\begin{aligned} l_{Q_1,Q_2}(P)^{p^d} &= \lambda^{p^d}(x_P^{p^d} + (-1)^{p^d} \cdot x_{Q_1}^{p^d}) - (y_P^{p^d} + (-1)^{p^d} \cdot y_{Q_1}^{p^d}) \\ &= \lambda^{p^d}(x_P - x_{Q_1}^{p^d}) - (y_P - y_{Q_1}^{p^d}). \qquad \because x_P, y_P \in \mathbb{F}_p \end{aligned}$$

Furthermore, λ^{p^d} is similarly given as follows:

$$\begin{aligned} \lambda^{p^d} &= \begin{pmatrix} \left(\dfrac{y_{Q_2} - y_{Q_1}}{x_{Q_2} - x_{Q_1}}\right)^{p^d} & Q_1 \neq Q_2, x_{Q_1} \neq x_{Q_2} \\ \left(\dfrac{3x_{Q_1}^2}{2y_{Q_1}}\right)^{p^d} & Q_1 = Q_2, y_{Q_1} \neq 0 \end{pmatrix} \\ &= \begin{pmatrix} \dfrac{y_{Q_2}^{p^d} - y_{Q_1}^{p^d}}{x_{Q_2}^{p^d} - x_{Q_1}^{p^d}} & Q_1 \neq Q_2, x_{Q_1} \neq x_{Q_2} \\ \dfrac{3(x_{Q_1}^{p^d})^2}{2y_{Q_1}^{p^d}} & Q_1 = Q_2, y_{Q_1} \neq 0 \end{pmatrix}. \end{aligned}$$

Therefore, we obtain the following relation:

$$l_{Q_1,Q_2}^{p^d}(P) = l_{\pi_p^d(Q_1),\pi_p^d(Q_2)}(P)$$

Proof of (ii)
We note that x_{Q_3}, y_{Q_3} are x and y coordinates of Q_3 respectively. Then, the vertical function $v_{Q_3}(P)$ is given as follows:

$$v_{Q_3}(P) = x_P - x_{Q_3}.$$

Then, we obtain the following relation similarly as proof of (i):

$$\begin{aligned} v_{Q_3}^{p^d}(P) &= (x_P - x_{Q_3})^{p^d} \\ &= x_P^{p^d} - x_{Q_3}^{p^d}. \\ &= x_P - x_{Q_3}^{p^d}. \qquad \because x_P \in \mathbb{F}_p \end{aligned}$$

Therefore, we obtain the following relation:

$$v_{Q_3}^{p^d}(P) = v_{\pi_p^d(Q_3)}(P).$$

□

Lemma 2 *For an integer $d > 0$ and rational point $Q \in \mathbb{G}_2$, $f_{p^d,Q} = f_{p,Q}^{d \cdot p^{d-1}}$.*

Proof. We have following relation $\pi_p(Q) = [p]Q$, where $Q \in \mathbb{G}_2$ from definition of $\mathbb{G}_2$. Therefore, the following relation is obtained:

$$\begin{aligned} f_{p^k,Q}^p &= f_{p^k,Q}^p \\ &= (f_{p,Q}^{p^{k-1}} \cdot f_{p^{k-1},[p](Q)})^p && \text{(applying Lemma 1 (a))} \\ &= (f_{p,Q}^{p^{k-1}} \cdot f_{p^{k-1},\pi_p(Q)})^p && \text{(from definition of } \mathbb{G}_2) \\ &= f_{p,Q}^{p^k} \cdot f_{p^{k-1},\pi_p(Q)}^p. && (1) \end{aligned}$$

Additionally case (a) in Lemma 1 with $a = p$ leads to

$$\begin{aligned} f_{bp,Q} &= f_{p,Q}^b \cdot f_{b,[p]Q} && \text{(Lemma 1 (a) with } a = p) \\ &= f_{p,Q}^b \cdot f_{b,\pi_p(Q)} && \text{(from definition of } \mathbb{G}_2) \\ &= f_{p,Q}^b \cdot f_{b,Q}^p. && \text{(from Lemma 1 (c))} \quad (2) \end{aligned}$$

Then, applying $b = p^{d-1}$ to the above relation, we have the following result.

$$\begin{aligned} f_{p^d,Q} &= f_{p^{d-1} \cdot p,Q} \\ &= f_{p,Q}^{p^{d-1}} \cdot f_{p^{d-1},Q}^p && \text{(applying } b = p^{d-1} \text{ to Eq (2))} \\ &= f_{p,Q}^{p^{d-1}} \cdot f_{p,Q}^{p^{d-1}} \cdot f_{p^{d-2},Q}^p && \text{(from Eq (1))} \\ &= f_{p,Q}^{p^{d-1}} \cdot f_{p,Q}^{p^{d-1}} \cdot f_{p,Q}^{p^{d-1}} \cdot f_{p^{d-3},Q}^p && \text{(from Eq (1))} \\ &\quad \vdots \\ &= f_{p,Q}^{p^{d-1}} \cdot f_{p,Q}^{p^{d-1}} \cdots f_{p,Q}^{p^{d-1}} \cdot f_{p,Q}^p && \text{(from Eq (1))} \\ &= f_{p,Q}^{p^{d-1}} \cdot f_{p,Q}^{p^{d-1}} \cdots f_{p,Q}^{p^{d-1}} \cdot f_{1,Q}^p && \text{(from Eq (1))} \\ &= \underbrace{f_{p,Q}^{p^{d-1}} \cdot f_{p,Q}^{p^{d-1}} \cdots f_{p,Q}^{p^{d-1}}}_{d-1 \text{ times multiplications}} \\ &= f_{p,Q}^{d \cdot p^{d-1}}. \end{aligned}$$

□

2.4 Pairings on Elliptic Curves

The pairing on elliptic curves is the map that has two inputs and one output as follows:

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T.$$

One of the inputs is an element over $\mathbb{G}_1$ and the other one is an element over $\mathbb{G}_2$. $\mathbb{G}_1$ and $\mathbb{G}_2$ are base-field and trace-zero subgroup of $E[r]$ defined as follows:

$$\begin{cases} \mathbb{G}_1 &= E[r] \cap \ker(\pi_p - [1]) \\ \mathbb{G}_2 &= E[r] \cap \ker(\pi_p - [p]), \end{cases}$$

The output is an element over $\mathbb{G}_T$ where $\mathbb{G}_T$ is a multiplicative subgroup in $\mathbb{F}_{p^k}$ of order r. When restricting the subgroup to $\mathbb{G}_1$ and $\mathbb{G}_2$, a pairing can be constructed by using Theorem 1.

Theorem 1 *Let $\lambda \equiv p \pmod{r}$. Then, the following map defines a bilinear pairing on $\mathbb{G}_2 \times \mathbb{G}_1$.*

$$(Q, P) \mapsto f_{\lambda,Q}(P)^{\frac{p^k-1}{r}},$$

where $f_{\lambda,Q}$ is a rational function on E with divisor $div(f_{\lambda,Q}) = \lambda(Q) - ([\lambda]Q) - (\lambda - 1)(\mathcal{O})$.

Proof. Please refer to [13]. □

Since $r \mid \#E(\mathbb{F}_p)$, it is obvious that $t - 1 \equiv p \pmod{r}$. This leads to a pairing, which is called an ate pairing, defined by

$$\alpha_{t-1} : (Q, P) \mapsto f_{t-1,Q}(P)^{\frac{p^k-1}{r}}.$$

The above equation shows that this ate pairing requires Miller's algorithm with loop length $\log_2(t-1)$. Miller's algorithm is shown in Alg. 1. In Alg. 1, an input s is called a loop parameter because the number of iterations depends on the bit length of s. Therefore, the bit length of s is an important factor to consider in the calculation cost of Miller's loop. Additionally, the Hamming weight of s is also an important factor because the count of ADD step and SUB step depends on Hamming weight. To make Miller's algorithm efficient, selecting a loop parameter that has a short bit-length and low Hamming weight is necessary.

Algorithm 1 Miller's algorithm

Require: $s, P \in \mathbb{G}_1, Q \in \mathbb{G}_2$;

Ensure: $f_{s,Q}(P)$;

$f \leftarrow 1, T \leftarrow Q$;

for $i = \lfloor \log_2(s) \rfloor - 1$ **downto** 1; **do**

$f \leftarrow f^2 \cdot \dfrac{l_{T,T}(P)}{v_{[2]T}(P)}$;

$T \leftarrow [2]T$; ▷ DBL

if $s[i] = 1$; **then**

$f \leftarrow f \cdot \dfrac{l_{T,Q}(P)}{v_{T+Q}(P)}$;

$T \leftarrow T + Q$; ▷ ADD

else if $s[i] = -1$; **then**

$f \leftarrow f \cdot \dfrac{l_{T,-Q}(P)}{v_{T-Q}(P)}$;

$T \leftarrow T - Q$; ▷ SUB

end if

end for

return f;

More generally, the ate pairing corresponding to $\lambda \equiv p \pmod{r}$ is one of the special cases of pairings given by Theorem 2.

Theorem 2 *Let $k' = \phi(k)$ and $\sum_{i=0}^{k'} c_i p^i \equiv 0 \pmod{r}$ where function ϕ is Euler's phi function. Then, the following map defines a bilinear pairing on $\mathbb{G}_2 \times \mathbb{G}_1$.*

$$(P, Q) \mapsto \left(\prod_{i=0}^{k'-1} f_{c_i,Q}(P)^{p^i} \cdot \prod_{i=0}^{k'-2} \frac{l_{s_{i+1}Q,c_i p^i Q}(P)}{v_{s_i Q}(P)} \right)^{\frac{p^k-1}{r}},$$

where $s_i = \sum_{j=i}^{k'-1} c_j p^j$, $l_{s_{i+1}Q,c_i p^i Q}$ and $v_{s_i Q}(P)$ are line functions in $\mathbb{F}_q(E)$ with the divisors $div(l_{s_{i+1}Q,c_i p^i Q}) = (s_{i+1}Q) + (c_i p^i Q) + (-(s_{i+1} + c_i p^i)Q) - 3(\mathcal{O})$ and $div(v_{s_i Q}(P)) = (s_i Q) + (-s_i Q) - 2(\mathcal{O})$, respectively.

Proof. Please refer to [8]. □

A pairing constructed by Theorem 2 is called an ate-like pairing. One can find $\sum_{i=0}^{k'} c_i p^i \equiv 0 \pmod{r}$ which leads to a pairing with a short length of Miller's algorithm. We say that a pairing with one of the shortest lengths $\log_2 r/\phi(k)$ is an *optimal ate pairing*.

3 Related Works

In this section, the authors explain previous works related to our proposed method. The first subsection shows an optimal-ate pairing on the FK12 curve by the previous work in [6]. The authors explain the Xate pairing on the BN12 curve in the following subsection.

3.1 Optimal-Ate Pairing on FK12 Curve.

The loop parameter of the Miller loop for ate pairing on FK12 is $t-1=-6z^2$. Therefore, an ate pairing on the FK12 curve is defined as follows:

$$e_{ate}:\mathbb{G}_2\times\mathbb{G}_1\to\mathbb{G}_T,(Q,P)\mapsto f_{-6z^2,Q}(P)^{\frac{p^{12}-1}{r}}.$$

There is a relation $6z+2\equiv p+p^2+p^3 \pmod{r}$ and this gives rise to an ate-like pairing by Theorem 2 given as follows [6]:

$$\begin{aligned}&e_{opt}:\mathbb{G}_2\times\mathbb{G}_1\to\mathbb{G}_T,\\&(Q,P)\mapsto (f_{(6z+2),Q}(P)\cdot l_{(6z+2)Q,-\pi_p(Q)}(P)\cdot\\&\qquad\qquad l_{(6z+2)Q-\pi_p(Q),-\pi_p^2(Q)}(P))^{\frac{p^{12}-1}{r}}.\end{aligned}$$

For the efficient optimal ate pairing, a parameter should be low Hamming weight with z and $6z+2$.

3.2 Ate-like Pairing on BN12 Curve

In this subsection, the authors explain ate-like pairings on the BN12 curve i.e., an optimal ate pairing and Xate pairing.
The BN12 curve is parameterized by the following parameters.

$$\begin{cases} p(x) &= 36x^4+36x^3+24x^2+6x+1,\\ r(x) &= 36x^4+36x^3+18x^2+6x+1,\\ t(x) &= -6x^2+1. \end{cases} \tag{3}$$

In the case of the BN curve, same as the FK curve, z is used as the parameter to identify only one curve.

The loop parameter of the Miller loop for ate pairing on BN12 is $t-1=-6z^2$. Therefore, an ate pairing on the FK12 curve is defined as follows:

$$e_{ate}:\mathbb{G}_2\times\mathbb{G}_1\to\mathbb{G}_T,(Q,P)\mapsto f_{-6z^2,Q}(P)^{\frac{p^{12}-1}{r}}.$$

3.2.1 Optimal-Ate Pairing on BN12 Curve

According to [8], applying Theorem 2 with a relation $p^3-p^2+p\equiv -6z-2 \pmod{r}$,

$$\begin{aligned}&e_{opt}:\mathbb{G}_2\times\mathbb{G}_1\to\mathbb{G}_T,\\&(Q,P)\mapsto (f_{(6z+2),Q}(P)\cdot l_{(6z+2)Q,\pi_p(Q)}(P)\cdot\\&\qquad\qquad l_{(6z+2)Q+\pi_p(Q),\pi_p^2(Q)}(P))^{\frac{p^{12}-1}{r}}.\end{aligned}$$

For the efficient optimal ate pairing, a parameter should be low Hamming weight with z and $6z+2$.

3.2.2 Xate Pairing on BN12 Curve

In [9], Nogami et al proposed another ate-like pairing, which is called Xate pairing as follows:

$$e_{xate} : \mathbb{G}_2 \times \mathbb{G}_1 \to \mathbb{G}_T,$$
$$(Q, P) \mapsto (f_{z,Q}^{1+p+p^3+p^{10}}(P) \cdot l_{zQ,z\pi_p(Q)}(P) \cdot$$
$$l_{z\pi_p^3(Q),z\pi_p^{10}(Q)}(P) \cdot l_{zQ+z\pi_p(Q),z\pi_p^3(Q)+z\pi_p^{10}(Q)}(P))^{\frac{p^{12}-1}{r}}.$$

The loop parameter of the Miller loop for Xate pairing on BN12 is z and it is shorter than the optimal ate's one. The Xate pairing is based on the relation $6z = 1 + p + p^3 + p^{10} \pmod r$. The Xate pairing doesn't need Theorem 2 but applying Theorem 1 and transform.

4 Proposal

In this section, the authors propose a pairing on the FK12 curve with a shorter loop length $\log z$ of Miller's algorithm than the previous optimal ate pairing. We say the pairing as the Xate pairing on FK12 since the basic approach is based on the Xate pairing on BN12 curve given in [9].

4.1 Xate Pairing on FK12 Curve

The concrete equation is described in Theorem 3 with the following proof.

Theorem 3 *The following map defines a bilinear pairing on* $\mathbb{G}_2 \times \mathbb{G}_1$.

$$e_z : (Q, P) \mapsto$$
$$\Big(f_{z,Q}^{1+p^7+p^9+p^{10}} \cdot l_{\pi_p^9([z]Q),\pi_p^{10}([z]Q)} \cdot l_{\pi_p^7([z]Q),\pi_p^9([z]Q)+\pi_p^{10}([z]Q)} \cdot$$
$$l_{[z]Q,\pi_p^7([z]Q)+\pi_p^9([z]Q)+\pi_p^{10}([z]Q)}\Big)^{\frac{p^k-1}{r}}.$$

For proof of Theorem 3, we need Lemmas 3 and 4.

Lemma 3 *The following maps define bilinear pairings on* $\mathbb{G}_2 \times \mathbb{G}_1$.

(a) $(P, Q) \mapsto f_{p,Q}(P)^{\frac{p^k-1}{r}}$,
(b) For an integer $a \neq 0$ *such that* $a \nmid r$, $(P, Q) \mapsto f_{p,[a]Q}(P)^{\frac{p^k-1}{r}}$.

Proof of Lemma 3. (a) This is one of the cases of Theorem 1. (b) Since (a) is true, we can write $f_{p,[a]Q}(P)^{\frac{p^k-1}{r}} = f_{p,Q}(P)^{a\frac{p^k-1}{r}}$. This clearly leads to the map being a bilinear pairing. □

Lemma 4 *Let* f *and* g *be certain rational functions on* E *such that* $(Q, P) \mapsto f(Q, P)^{\frac{p^k-1}{r}}$ *and* $(Q, P) \mapsto g(Q, P)^{\frac{p^k-1}{r}}$ *being bilinear maps on* $\mathbb{G}_2 \times \mathbb{G}_1$. *Then, for any integers* $m, n \neq 0$, $e : (P, Q) \mapsto (f(Q, P)^m \cdot g(Q, P)^n)^{\frac{p^k-1}{r}}$ *is a bilinear map on* $\mathbb{G}_2 \times \mathbb{G}_1$.

Proof of Lemma 4. It is enough to show that $e([a]Q, [b]P) = e(Q, P)^{ab}$ for any integers $a, b \neq 0$. We can easily see that

$$\begin{aligned} e([a]Q, [b]P) &= (f([a]Q, [b]P)^m \cdot g([a]Q, [b]P)^n)^{\frac{p^k-1}{r}} \\ &= f([a]Q, [b]P)^{m\frac{p^k-1}{r}} \cdot g([a]Q, [b]P)^{n\frac{p^k-1}{r}} \\ &= f(Q, P)^{abm\frac{p^k-1}{r}} \cdot g(Q, P)^{abn\frac{p^k-1}{r}} \\ &= (f(Q, P)^m \cdot g(Q, P)^n)^{ab\frac{p^k-1}{r}} \\ &= e(Q, P)^{ab}. \end{aligned}$$

□

Proof of Theorem 3. The parameters $p = p(z)$ and $r = r(z)$ for FK12 satisfy $-6z \equiv 1 + p^7 + p^9 + p^{10} \pmod{r}$. Thus, it is obtained that $-6z^2 \equiv z \cdot (1 + p^7 + p^9 + p^{10}) \equiv p \pmod{r}$. According to Theorem 1, this allows us to have the following definition of a bilinear pairing.

$$(Q, P) \mapsto f_{z\cdot(1+p^7+p^9+p^{10}),Q}(P)^{\frac{p^k-1}{r}}.$$

When applying Lemma 1 and Lemma 2,

$$\begin{aligned}
&f_{z\cdot(1+p^7+p^9+p^{10}),Q} \\
&\quad = f_{z,Q}^{1+p^7+p^9+p^{10}} \cdot f_{1+p^7+p^9+p^{10},[z]Q}, \\
&f_{1+p^7+p^9+p^{10},[z]Q} \\
&\quad = f_{1,[z]Q} \cdot f_{p^7+p^9+p^{10},[z]Q} \cdot \frac{l_{[z]Q,[z\cdot(p^7+p^9+p^{10})]Q}}{v_{[z\cdot(1+p^7+p^9+p^{10})]Q}}, \\
&f_{p^7+p^9+p^{10},[z]Q} \\
&\quad = f_{p,[z]Q}^{7\cdot p^6} \cdot f_{p^9+p^{10},[z]Q} \cdot \frac{l_{[z\cdot p^7]Q,[z\cdot(p^9+p^{10})]Q}}{v_{[z\cdot(p^7+p^9+p^{10})]Q}}, \\
&f_{p^9+p^{10},[z]Q} \\
&\quad = f_{p,[z]Q}^{9\cdot p^8} \cdot f_{p,[z]Q}^{10\cdot p^9} \cdot \frac{l_{[z\cdot p^9]Q,[z\cdot p^{10}]P}}{v_{[z\cdot(p^9+p^{10})]P}}.
\end{aligned}$$

The above shows that

$$\begin{aligned}
&f_{z\cdot(1+p^7+p^9+p^{10}),Q} \\
&= f_{z,Q}^{1+p^7+p^9+p^{10}} \cdot f_{1,[z]Q} \cdot f_{p,[z]Q}^{7\cdot p^6} \cdot f_{p,[z]Q}^{9\cdot p^8} \cdot f_{p,[z]Q}^{10\cdot p^9} \\
&\quad \cdot \frac{l_{[z\cdot p^9]Q,[z\cdot p^{10}]P}}{v_{[z\cdot(p^9+p^{10})]P}} \cdot \frac{l_{[z\cdot p^7]Q,[z\cdot(p^9+p^{10})]Q}}{v_{[z\cdot(p^7+p^9+p^{10})]Q}} \cdot \frac{l_{[z]Q,[z\cdot(p^7+p^9+p^{10})]Q}}{v_{[z\cdot(1+p^7+p^9+p^{10})]Q}}
\end{aligned}$$

According to Lemma 3, $(P, Q) \mapsto f_{p,[z]Q}$ is a bilinear pairing. Since here we have two bilinear pairings that can be applied to Lemma 4, the following equation defines a bilinear pairing.

$$\begin{aligned}
(Q, P) &\mapsto (f_{z\cdot(1+p^7+p^9+p^{10}),Q}(P) \cdot f_{p,[z]Q}^{-7\cdot p^6}(P) \cdot \\
&\qquad f_{p,[z]Q}(P)^{-9\cdot p^8} \cdot f_{p,[z]Q}(P)^{-10\cdot p^9})^{\frac{p^k-1}{r}} \\
&= \left(f_{z,Q}^{1+p^7+p^9+p^{10}} \cdot f_{1,[z]Q} \cdot \frac{l_{[z\cdot p^9]Q,[z\cdot p^{10}]P}}{v_{[z\cdot(p^9+p^{10})]P}} \right. \\
&\quad \left. \cdot \frac{l_{[z\cdot p^7]Q,[z\cdot(p^9+p^{10})]Q}}{v_{[z\cdot(p^7+p^9+p^{10})]Q}} \cdot \frac{l_{[z]Q,[z\cdot(p^7+p^9+p^{10})]Q}}{v_{[z\cdot(1+p^7+p^9+p^{10})]Q}} \right)^{\frac{p^k-1}{r}}.
\end{aligned}$$

When eliminating the terms that the final exponentiation brings to $1 \in \mathbb{F}_{p^k}$,

$$\begin{aligned}
(Q, P) \mapsto &\left(f_{z,Q}^{1+p^7+p^9+p^{10}} \cdot l_{[z\cdot p^9]Q,[z\cdot p^{10}]P} \cdot \right. \\
&\left. l_{[z\cdot p^7]Q,[z\cdot(p^9+p^{10})]Q} \cdot l_{[z]Q,[z\cdot(p^7+p^9+p^{10})]Q} \right)^{\frac{p^k-1}{r}}.
\end{aligned}$$

Applying the Frobenius mapping π_p on E, we finally have the equation given in Theorem 3. □

4.2 Cost Estimation and Implementation

The authors construct the following tower of extension field for pairing on the FK12 curve.

$$\begin{aligned}\mathbb{F}_{p^2} &= \mathbb{F}_p[\alpha]/(\alpha^2+1),\\ \mathbb{F}_{p^4} &= \mathbb{F}_{p^2}[\beta]/(\beta^2-(\alpha+1)),\\ \mathbb{F}_{p^{12}} &= \mathbb{F}_{p^4}[\gamma]/(\gamma^3-\beta).\end{aligned}$$

The authors estimate the computational cost based on multiplication m_1 in $\mathbb{F}_p$. Since $6z+2$ has 75 as bit-length and 8 as Hamming weight where the parameter $z=-2^{72}-2^{46}-2^8-2$, ADD step and DBL step in Miller loop take $80m_1$ and $99m_1$ respectively where m_1 is $\mathbb{F}_p$-multiplication and SUB step in the Miller loop is presumed to be the same cost as ADD step. For optimal ate pairing on the FK12 curve, 7 ADD or SUB steps and 75 DBL steps are required to compute $f_{(6z+2),Q}(P)$. Additionally, we have to compute $\pi_p(Q)$,$\pi_p^2(Q)$, and 2 SUB steps. These 2 SUB steps are required to compute $l_{(6z+2)Q,-\pi_p(Q)}(P)$ and $l_{(6z+2)Q-\pi_p(Q),-\pi_p^2(Q)}(P)$. Please note that the last SUB step can reduce operations practically and as a result, it takes only $55m_1$. $\pi_p(Q)$,$\pi_p^2(Q)$ take $6m_1$ respectively. Then, the total cost of the Miller loop for optimal ate pairing on the FK12 curve is obtained as follows:

$$\begin{aligned}(cost_{opt}) &= 7\times(80m_1)+75\times(99m_1)+80m_1+55m_1+6m_1+6m_1\\ &= 8132m_1\end{aligned}$$

In the case of Xate pairing, 3 SUB steps and 72 DBL steps are required to compute $f_{z,Q}(P)$ because z has 72 as bit-length and 4 as Hamming weight. Additionally, we have to compute $f_{z,Q}^{1+p^7+p^9+p^{10}}$, $[z\cdot p^7]Q$, $[z\cdot p^9]Q$, $[z\cdot p^{10}]Q$, and 3 ADD steps. Three Frobenius endomorphism and three $\mathbb{F}_{p^{12}}$-multiplications are required to compute $f_{z,Q}^{1+p^7+p^9+p^{10}}$ from $f_{z,Q}(P)$ and total cost of them is $207m_1$. Addtionally, it takes $51m_1$ to compute $[z\cdot p^7]Q$, $[z\cdot p^9]Q$, and $[z\cdot p^{10}]Q$. Additional 3 ADD steps are required to compute $l_{[z\cdot p^9]Q,[z\cdot p^{10}]P}$, $l_{[z\cdot p^7]Q,[z\cdot(p^9+p^{10})]Q}$ and $l_{[z]Q,[z\cdot(p^7+p^9+p^{10})]Q}$. Note that the last ADD step can reduce operations as we mentioned in the case of optimal ate pairing. Then, the total cost of the Miller loop for optimal ate pairing on the FK12 curve is obtained as follows:

$$\begin{aligned}(cost_{xate}) &= 3\times(80m_1)+72\times(99m_1)+207m_1+51m_1+2\times(80m_1)+55m_1\\ &= 7841m_1\end{aligned}$$

In Table 1, it is shown that the proposed algorithm leads to 3.71% reduction of the calculation of the Miller loop from the view of the number of multiplications in $\mathbb{F}_p$.

Table 1: The calculation costs of the Miller loopfor the pairing at the 128-bit security level.

	Calculation costs
Previous [6]	$8132m_1$
This work	$7841m_1$

The authors implemented the Xate pairing and optimal-ate pairing and compared the execution time of the Miller loop. Table 2 shows the experimental environment and Table 3 shows the results of the execution time. Note that these results are remeasured for this paper from [10]. In the experiment, the authors measured 1000000 trials of the execution time of the Miller loop and obtained the average execution time. From the viewpoint of execution time, this work leads to a 3.03% reduction in the calculation of the Miller loop.

Table 2: Experimental environment

	PC
CPU	11th Gen Intel(R) Core(TM) i9-11900K @ 3.50GHz
OS	Ubuntu 20.04
gcc ver	9.4.0
Optimize option	O2
Memory	64GB

Table 3: Experimental results

	Execution time [ms]
Previous [6]	0.887
This work	0.861

5 Evaluation for Execution Times of the STNFS Secure Curves

In this section, the authors show the evaluation of pairings on the STNFS secure curve. The authors implement pairing on BLS12 curve , BN12 curve, Cocks-Pinch curve with $k = 6, 8$, FK12 curve, KSS16 and the cyclotomic family of curves with $k = 10, 11, 13, 14$. The following subsections show the parameters of these curves.

5.1 BLS12 Curve

The BLS12 curve[14] is parameterized by the following parameters.

$$\begin{cases} p(x) &= (x-1)^2(x^4-x^2+1)/3+x \\ r(x) &= \Phi_{12}(x) = x^4-x^2+1, \\ t(x) &= x+1, \end{cases}$$

where $\Phi_N(\cdot)$ is the N-th cyclotomic polynomial. To specify the curve, the authors use

$$x = -2^{74} - 2^{73} - 2^{63} - 2^{57} - 2^{50} - 2^{17} - 2^0 \tag{4}$$

as a parameter for a 128-bit security level in this experiment.

5.2 BN12 Curve

The BN12 curve is parameterized Eq. 3. To specify the curve, the authors use

$$x = 2^{110} + 2^{36} + 2^0 \tag{5}$$

as a parameter for a 128-bit security level in this experiment.

5.3 Cocks-Pinch Curve

Guillevic et al. constructed pairing-friendly curves with embedding degree $k = 5, 6, 7, 8$ by using Cocks-Pinch method in [15] and they are called Cocks-Pinch curves. In this paper, the authors implemented Cocks-Pinch curves with embedding degree $k = 6, 8$. To parameterize Cocks-Pinch curve, we define E^t and $\tilde{E}$ such that $E(\mathbb{F}_{p^k})[r] \simeq \tilde{E}(\mathbb{F}_{p^{k/d}})[r]$. E^t is the quadratic twist of an elliptic curve E and $\tilde{E}$ is the d-th twist of E. Cocks-Pinch curve with embedding degree $k = 6$ is

parameterized with the following parameters. The elliptic curve E is defined as $y^2 = x^3 - 1$ defined over $\mathbb{F}_p$ where

$$\begin{aligned} p =& \text{0x9401ff90f28bffb0c610fb10bf9e0fefd59211629a7991563c5e468} \\ & \text{d43ec9cfe1549fd59c20ab5b9a7cda7f27a0067b8303eeb4b31555cf4} \\ & \text{f24050ed155555cd7fa7a5f8aaaaaaad47ede1a6aaaaaaaab69e6dcb} \end{aligned}$$

and

$$r = \text{0xe0ffffffffffc400000000000003ff1000000000000020000000000000001}$$

In addition, the following relation holds. Note that p_N is a prime of N bits.

$$\begin{aligned} \#E(\mathbb{F}_p) &= 2^2 \cdot p_{414} \cdot r, \\ \#\tilde{E}(\mathbb{F}_p) &= 3 \cdot p_{414} \cdot r, \\ \#E^t(\mathbb{F}_p) &= 2^2 \cdot 3 \cdot 7 \cdot p_{665}, \\ \#E^t(\mathbb{F}_p) &= 13 \cdot 19 \cdot p_{664}. \end{aligned}$$

These parameters can be expressed with h_y and x as follows:

$$\begin{cases} p(x) &= \{(9h_y^2 + 6h_y + 4)x^4 + (-18h_y^2 - 6h_y - 12)x^3 + \\ & \qquad (27h_y^2 + 18h_y + 16)x^2 + (-18h_y^2 - 12h_y)x + (9h_y^2 + 12h_y + 4)\}/12 \\ r(x) &= \Phi_6(x) = x^2 - x + 1, \\ t(x) &= -x^2 + 2x. \end{cases}$$

To fix the curve, the authors use the following integers x and h_y.

$$\begin{aligned} h_y &= 2^{80} - 2^{70} - 2^{66} - 2^{14} + 2^5 \\ x &= 2^{128} - 2^{124} - 2^{69} \end{aligned}$$

Cocks-Pinch curve with embedding degree $k = 8$ is parameterized similarly.

$$\begin{aligned} p =& \text{0xbb9dfd549299f1c803ddd5d7c05e7cc0373d9b1ac15b} \\ & \text{47aa5aa84626f33e58fe66943943049031ae4ca1d2719b} \\ & \text{3a84fa363bcd2539a5cd02c6f4b6b645a58c1085e14411} \end{aligned}$$

and

$$r = \text{0xff0060739e18d7594a978b0ab6ae4ce3dbfd52a9d00197603fffdf0000000101}$$

In addition, the following relation holds.

$$\begin{aligned} \#E(\mathbb{F}_p) &= 2^2 \cdot 3^2 \cdot 5 \cdot 41 \cdot p_{275} \cdot r, \\ \#\tilde{E}(\mathbb{F}_{p^2}) &= 2 \cdot 89 \cdot p_{824} \cdot r, \\ \#E^t(\mathbb{F}_p) &= 2^4 \cdot p_{540}. \end{aligned}$$

5.4 KSS16 Curve

The KSS family is one of the families of curves proposed by Kachisa, Schaefer, and Scott in [16]. There are five embedding degrees for KSS curves, {16, 18, 32, 26, 40}. In this paper, the authors refer to KSS curves defined over $\mathbb{F}_q$ with embedding degree $k = 16$ (KSS16 curve). The KSS16 curve is parameterized as follows:

$$\begin{cases} p(x) &= (x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + \\ & \qquad 240x^4 + 625x^2 + 2398x + 3125)/980, \\ r(x) &= (x^8 + 48x^4x + 625)/61250, \\ t(x) &= (2x^5 + 41x + 35)/35. \end{cases}$$

Let z be an integer such that $p(z)$ and $r(z)$ are prime. The necessary condition for z is $z = 25$ or $45 \pmod{75}$ and $\rho = (\log_2 p(z))/\log_2 \mathrm{r(z)} \simeq 1.25$.

5.5 Cyclotomic Family of Curves

In [5], Guillevic et al. proposed the cyclotomic family of pairing-friendly curves with embedding degree $k = 10, 11, 13, 14$ with the Brezing-Weng method. The curve with $k = 10, D = 15$ and $\rho = 1.75$ is parameterized as follows.

$$\begin{cases} p(x) &= (4x^{14} + 4x^{13} + x^{12} - 12x^{11} - 12x^{10} - 7x^9 \\ & \quad +11x^8 + 17x^7 + 15x^6 - 3x^5 - 11x^4 + x^3 - 2x^2 + 3x + 6)/15, \\ r(x) &= \Phi_{30}(x) \\ &= x^8 + x^7 - x^5 - x^4 - x^3 + x + 1, \\ t(x) &= x^3 + 1. \end{cases}$$

The authors used $x = 2^{32} - 2^{26} - 2^{17} + 2^{10} - 1$ for this curve.

The curve with $k = 11, D = 11$ and $\rho = 1.60$ is parameterized as follows.

$$\begin{cases} p(x) &= (x^{16} + 2x^{15} + x^{14} - 12x - 3x^{11} - x^5 + 9x^4 - x^3 + x + 3)/11, \\ r(x) &= \Phi_{11}(x) \\ &= x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\ t(x) &= x^4 + 1. \end{cases}$$

The authors used $x = -2^{26} + 2^{21} + 2^{19} - 2^{11} - 2^9 - 2^0$ as a parameter to specify the curve.

The curve with $k = 13, D = 3$ and $\rho = 1.17$ is parameterized as follows.

$$\begin{cases} p(x) &= (x^{28} + x^{27} + x^{26} + x^{15} - 2x^{14} + x^{13} + x^2 - 2x + 1)/3, \\ r(x) &= \Phi_{39}(x) \\ &= x^{24} - x^{23} + x^{21} - x^{20} + x^{18} - x^{17} + x^{15} - x^{14} \\ & \quad +x^{12} - x^{10} + x^9 - x^7 + x^6 - x^4 + x^3 - x + 1, \\ t(x) &= x^3 + 1. \end{cases}$$

The authors used $x = 2^{11} + 2^8 - 2^6 - 2^4$ to fix the curve.

The curve with $k = 14, D = 3$ and $\rho = 1.33$ is parameterized as follows.

$$\begin{cases} p(x) &= (x^{16} + 4x^{15} + x^{14} - x^9 + 2x^8 - x^7 + x^2 - 2x + 1)/3, \\ r(x) &= \Phi_{42}(x) \\ &= x^{12} + x^{11} - x^9 - x^8 + x^6 - x^4 - x^3 + x + 1, \\ t(x) &= x^8 - x + 1. \end{cases}$$

To fix the curve, the authors used $x = 2^{21} + 2^{19} + 2^{10} - 2^6$.

5.6 Experimental

The authors implement the STNFS secure curves with the parameters mentioned before and measured execution times of the Miller loop and final exponentiation. For pairing on the FK12 curves, we implement two pairings. The first one is based on [6]. The second one's Miller loop is used Xate pairing which I mentioned in this paper and [7] is used for final exponentiation. The experimental environment is the same in Table 2. Table. 4 shows the execution time of pairings on the STNFS secure curve.

Table 4: Execution time of pairings on STNFS secure curve

Curves,(k, D, ρ)	Miller's alg [ms]	Final exp [ms]	Total [ms]
BLS12 (12, 3, 1.50)	0.872	0.979	1.851
BN12 (12, 3, 1.00)	1.359	0.777	2.135
Cocks-Pinch (6, 3, 2.63)	0.910	0.844	1.755
Cocks-Pinch (8, 4, 2.13)	0.717	1.133	1.850
Curve-10 Cyclo (10, 15, 1.75)	1.135	0.973	2.109
Curve-11 Cyclo (11, 11, 1.60)	2.126	2.049	4.176
Curve-13 Cyclo (13, 3, 1.17)	2.700	3.264	5.964
Curve-14 Cyclo (14, 3, 1.33)	1.414	1.469	2.883
FK12 [6] (12, 3, 1.50)	0.887	1.095	1.982
FK12 (Ours) (12, 3, 1.50)	0.861	0.942	1.803
KSS16 (16, 1, 1.25)	0.774	1.946	2.719

Pairing on the Cocks-Pinch curve with embedding degree 6 has the fastest execution time and pairing on the FK12 curve with the proposed method has the second fastest execution time. However, we have to note that the efficiency of pairing depends on parameters which make p, r and t in other words depends on x. In this experiment, the BLS12 curve is made by a parameter x whose Hamming weight is 7 and if we use the parameter whose Hamming weight is lighter, the execution time of the BLS12 curve can be faster.

6 Conclusion

The authors proposed and evaluated the Xate pairing on the FK12 curve which is known as the STNFS secure curve. By using this method, a loop parameter of the Miller loop has a shorter bit-length and lighter hamming weight than the optimal-ate's one. Moreover, the authors get a 3.03% reduction of the execution time to compute the Miller loop for pairing on the FK12 curve. In addition, to evaluate the pairing on the FK12 curve, the authors implement and compare other efficient STNFS curves such as the BLS12 curve and Cocks-Pinch curves with $k = 6$ and 8. The FK12 curve is not the fastest one however, the execution is the second fastest in this experiment. In future works, the authors would like to compare more curves which are made by other parameters x. And the authors would like to keep considering Xate pairing on the FK12 curve since the Xate pairing on the FK12 curves possibly depends on a parameter x.

7 Acknowledgement

This research was supported by JSPS KAKENHI Grant Number 19H05579.

References

[1] Taechan Kim and Razvan Barbulescu. "Extended tower number field sieve: A new complexity for the medium prime case". In: *Annual international cryptology conference*. Springer. 2016, pp. 543–571.

[2] Taechan Kim and Jinhyuck Jeong. "Extended tower number field sieve with application to finite fields of arbitrary composite extension degree". In: *IACR International Workshop on Public Key Cryptography*. Springer. 2017, pp. 388–408.

[3] Razvan Barbulescu and Sylvain Duquesne. "Updating key size estimations for pairings". In: *Journal of cryptology* 32.4 (2019), pp. 1298–1336.

[4] Aurore Guillevic and Shashank Singh. "On the alpha value of polynomials in the tower number field sieve algorithm". In: *Mathematical Cryptology* 1.1 (2021), p. 39.

[5] Aurore Guillevic. "A short-list of pairing-friendly curves resistant to special TNFS at the 128-bit security level". In: *IACR international conference on public-key cryptography*. Springer. 2020, pp. 535–564.

[6] Georgios Fotiadis and Chloe Martindale. "Optimal TNFS-secure pairings on elliptic curves with composite embedding degree". In: *IACR Cryptol. ePrint Arch.* 2019 (2019). (Retrieved on May 21, 2022), p. 555.

[7] Kazuma Ikesaka et al. "Improvement of Final Exponentiation for a Pairing on FK12 Curve and its Implementation". In: *2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)*. IEEE. 2022, pp. 205–208.

[8] Frederik Vercauteren. "Optimal pairings". In: *IEEE transactions on information theory* 56.1 (2010), pp. 455–461.

[9] Yasuyuki Nogami et al. "Integer variable χ–based ate pairing". In: *International Conference on Pairing-Based Cryptography*. Springer. 2008, pp. 178–191.

[10] Kazuma Ikesaka et al. "Improvement of Miller Loop for a Pairing on FK12 Curve and its Implementation". In: *2022 Tenth International Symposium on Computing and Networking (CANDAR)*. IEEE. 2022, pp. 104–109.

[11] Georgios Fotiadis and Elisavet Konstantinou. "TNFS resistant families of pairing-friendly elliptic curves". In: *Theoretical Computer Science* 800 (2019), pp. 73–89.

[12] Victor S Miller. "The Weil pairing, and its efficient calculation". In: *Journal of cryptology* 17.4 (2004), pp. 235–261.

[13] Florian Hess, Nigel P Smart, and Frederik Vercauteren. "The eta pairing revisited". In: *IEEE transactions on information theory* 52.10 (2006), pp. 4595–4602.

[14] Paulo SLM Barreto, Ben Lynn, and Michael Scott. "Constructing elliptic curves with prescribed embedding degrees". In: *Security in Communication Networks: Third International Conference, SCN 2002 Amalfi, Italy, September 11–13, 2002 Revised Papers 3*. Springer. 2003, pp. 257–267.

[15] Aurore Guillevic, Simon Masson, and Emmanuel Thomé. "Cocks–Pinch curves of embedding degrees five to eight and optimal ate pairing computation". In: *Designs, Codes and Cryptography* 88.6 (2020), pp. 1047–1081.

[16] Ezekiel J Kachisa, Edward F Schaefer, and Michael Scott. "Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field". In: *International conference on pairing-based cryptography*. Springer. 2008, pp. 126–135.