Accelerating pairings on BW10 and BW14 Curves

Senegue Gomez Nyamsi[1,2*], Laurian Guimagang Azebaze[2,3†] and Emmanuel Fouotsa[1,2†]

[1*]Department of Mathematics and Computer Science, University of Dschang, P.O.Box 67, Dschang, Cameroon.
[2]Department of Mathematics, University of Yaounde, P.O.Box 812,Yaounde, Cameroon.
[3] Centre for Cybersecurity and Mathematical Cryptology, University of Bamenda, P.O.Box 39, Bambili, Cameroon.

*Corresponding author(s). E-mail(s): nyamsigomez@gmail.com;
Contributing authors: azebazelaurian@yahoo.fr;
emmanuelfouotsa@yahoo.fr;
†These authors contributed equally to this work.

Abstract

Since the advent of pairing based cryptography, many researchers have developed several techniques and variants of pairings to optimise the speed of pairing computations. The selection of the elliptic curve for a given pairing based protocol is crucial for operations in the first and second pairing groups of points of the elliptic curve and for many cryptographic schemes. A new variant of superoptimal pairing was proposed in 2023, namely x-superoptimal pairing on curves with odd prime embedding degrees BW13-310 and BW19-286. This paper extends the definition of the x-superoptimal pairing on elliptic curves with even embedding degrees BW10-511 and BW14-351 at 128 bits security level. We provide a suitable formula of the x-superoptimal pairing on BW10-511 and BW14-351 where the Miller loop is about **13.5%** and **21.6%** faster than the optimal ate pairing on BW10-511 and BW14-351 respectively. The correctness of the x-superoptimal pairing on BW10-511 and BW14-351 and bilinearity has been verified by a Magma code.

Keywords: Optimal ate pairing; x-Superoptimal pairing; Miller function.

[0]Part of this work was done when the second author visited the Centre of Cybersecurity and Mathematical Cryptology, funded by ARES-Belgium of the University of Bamenda.

1 Introduction

A pairing is a non-degenerate bilinear map, $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_3$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are subgroups of an elliptic curve and $\mathbb{G}_3$ is a multiplicative sub-group of a finite field. In 1948, pairings were introduced in mathematics by Weil [1] and to cryptography in 1993 by Menezes et *al.* [2] as an instrument to attack instances of the Discrete Logarithm Problem (DLP) on elliptic curves. Pairing later became prominent as a strong tool to design many cryptographic protocols with novel properties such as faster public key compression for isogeny-based cryptosystems (key exchange) [3], verifable delay functions from supersingular isogenies [4], enhanced Privacy ID (EPID) scheme [5], identity-based encryption [6] and the tripartite Diffie-Hellman key exchange [7]. Many authors have worked on efficient implementation of pairings on elliptic curves with even embedding degrees such as Guillevic et *al.* [8], Aranha et *al.* [9], Ghammam et *al.* [10] and many others [11–17] whereas, few implementations of superoptimal pairing have been done. In [18], Yanfeng et *al.* defined a superoptimal pairing with Miller loop length less than $\frac{\log_2(r)}{\varphi(k)}$ having the advantage that its Miller loop length is half of that of the optimal ate pairing defined by Vercauteren [19], though their pairings formulas involve more exponentiations that may affect the efficiency.

In 2023, the authors Yu Dai et *al.* [20] have revisited two pairings-friendly curves with even embedding degrees 10 and 14 over fields of size 511 and 351 respectively ensuring a security level of 128 bits called BW10-511 and BW14-351. Where for BW14-351 they provided high-speed software implementations of pairing computation, hashing to $\mathbb{G}_1$ and $\mathbb{G}_2$, group exponentiations, and subgroup membership testings on a 64-bit platform. Their results reveal that the performance of single pairing computation on BW14-351 is slightly faster than BN-446 and BW13-310, while about 18.4% slower than BLS12-446. In terms of group exponentiation in $\mathbb{G}_1$ and $\mathbb{G}_T$, BW14-351 is about 49.2% and 15.1% faster than BLS12-446, 119.6% and 73.8% faster than BN-446, while 34.4% and 5.5% slower than BW13-310. Moreover, compared to BW13-310, BW14-351 benefits from a greater performance penalty for hashing to $\mathbb{G}_2$ and group exponentiation in $\mathbb{G}_2$ that are 55.7% and 51.04% respectively, though it is still slower than BN-446 and BLS12-446. Therefore BW14-351 is an appropriate choice for protocols that aims to pursue fast group exponentiations in $\mathbb{G}_1$ and $\mathbb{G}_T$, while minimizing the performance penalty for group exponentiations in $\mathbb{G}_2$. Furthermore, BW10-511 and BW14-351 curves admit a quadratic twist which enable computations to be done in the subfields $\mathbb{F}_{q^5}$ and $\mathbb{F}_{q^7}$ respectively where El Mrabet et *al.* [21] have proposed a method to improve the arithmetic cost and also led to the denominator elimination technique. The bilinearity of the new x-superoptimal pairings has been verified by a Magma script available at https://github.com/Azebazelaurian/Azebazelaurian.git.

Our contribution. The contributions of this paper are as follows:

- We proposed two new formulas of x-superoptimal pairings on BW10-511 and BW14-351 respectively and provided a Magma script for the correctness of the bilinearity of the new x-superoptimal pairings.
- We compare the efficiency of our proposed x-superoptimal pairings computations on BW10-511 and BW14-351 with the optimal ate pairings computations done by Yu Dai et *al.* [20]

Roadmap. Section 2 gives a brief overview of the optimal ate pairing and superoptimal pairing on elliptic curves. In section 3, we provide a variant of the superoptimal pairing on BW10-511 and BW14-351 curves called x-superoptimal. In section 4, we evaluate the Miller loop of the x-superoptimal pairing on BW10-511 and BW14-351 curves. Section 5 summarizes operation costs of the previous sections and we end in section 6 with the conclusion.

2 Preliminaries.

In this section, we define a pairing-friendly elliptic curve [22], the optimal ate pairing [19] and the superoptimal pairing [18] on elliptic curves.

2.1 Pairing-friendly elliptic curve

Let $q(x), t(x), r(x) \in \mathbb{Q}[x]$ be non-zero polynomials. We say that a polynomial triple $(q(x), t(x), r(x))$ parametrizes a family of pairing-friendly ordinary elliptic curves with embedding degree k and CM discriminant D, if the following are satisfied :

(i) q(x) represents primes. That is, it is non-constant, irreductible, with positive leading coefficient. Additionally, $q(x) \in \mathbb{Z}$, for some (or infinitely many) $x \in \mathbb{Z}$ and $gcd(\{q(x) : x, q(x) \in \mathbb{Z}\}) = 1$.

(ii) r(x) is non-constant, irreducible, integer-valued, with positive leading coefficient.

(iii) r(x) divides both q(x)+1-t(x) and $\Phi_k(t(x) - 1)$, $\Phi_k(x)$ is the k^{th} cyclotomic polynomial.

(iv) there are infinitely many integer solutions (x, Y) for the parametrized CM equation $DY^2 = 4q(x) - t(x)^2$.

The ρ-value of a polynomial family $(q(x), t(x), r(x))$ is defined as $\rho(q, t, r) = \frac{degq}{degr}$. Let $f(x) = 4q(x) - t(x)^2 \in \mathbb{Q}[x]$ be the CM polynomial of the form $f(x) = g(x)y(x)^2$ with $y(x), g(x) \in \mathbb{Q}[x]$ and deg g ≤ 2. If deg g $= 0$, the family (q(x), t(x), r(x)) is complete and thus $f(x) = Dy(x)^2$, for some square-free $D > 0$. If deg g $= 1$, the family is complete with variable discriminant and finally, if deg g $= 2$, with g(x) not a perfect square and $lc(g) > 0$, the family is sparse.

2.2 Optimal ate Pairing

Let E be an elliptic curve defined over $\mathbb{F}_p$, where p is a large prime number and let r be the largest prime number such that r divides $\#E(\mathbb{F}_p)$. Let k be the smallest positive integer such that r divides $p^k - 1$. The integer k is called the embedding degree of E (with respect to r). We set

$$\mathbb{G}_1 = E(\mathbb{F}_{p^k})[r] \cap ker(\pi_p - [1]) \quad \text{and} \quad \mathbb{G}_2 = E(\mathbb{F}_{p^k})[r] \cap ker(\pi_p - [p]),$$

Where π_p denotes the p-power Frobenius endomorphism on E. Note that $\mathbb{G}_1 = E(\mathbb{F}_p)[r]$ and $\mathbb{G}_2 \subset E(\mathbb{F}_{p^k})[r]$.

Consider the $\varphi(k)-$dimensional lattice (spanned by the rows)

$$L = \begin{bmatrix} r & 0 & 0 & ... & 0 \\ -p & 1 & 0 & ... & 0 \\ -p^2 & 0 & 1 & ... & 0 \\ ... & ... & ... & ... & ... \\ -p^{\varphi(k)-1} & 0 & 0 & ... & 1 \end{bmatrix}.$$

Where $\varphi(k)$ is the Euler Totient function. The volume of L is easily seen to be r, so by Minkowski's theorem [23], there exists a short vector $V = (c_0, ..., c_{\varphi(k)-1})$ with $|c_i| \leq r^{1/\varphi(k)}$. The LLL algorithm applied to the rows of L gives such c_i's.

The optimal ate pairing [19] is defined as the non-degenerated bilinear map $\hat{a}_k : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mu_r \subset \mathbb{F}_{p^k}^*$ given by

$$\hat{a}_k(Q, P) = \left(\prod_{i=0}^{\varphi(k)-1} f_{c_i,Q}^{p^i}(P) \cdot \prod_{i=0}^{\varphi(k)-2} h_{[s_{i+1}]Q,[c_i p^i]Q}(P) \right)^{\frac{p^k-1}{r}} \tag{1}$$

Where $h_{[s_{i+1}]Q,[c_i p^i]Q}(P) = \frac{l_{[s_{i+1}]Q,[c_i p^i]Q}(P)}{v_{[s_i]Q}(P)}$, with $l_{[s_{i+1}]Q,[c_i p^i]Q}$ which represents the line passing through the two points $[s_{i+1}]Q$ and $[c_i p^i]Q$, and $v_{[s_i]Q}$ the vertical line passing through the point $[s_i]Q$. The values s_i are obtained by the relation:

$$s_i = \sum_{j=i}^{\varphi(k)-1} c_j p^j$$

For two points R, S on the curve E, $h_{R,S}$ is the rational function with divisor $(R) + (S) - (S + R) - (P_\infty)$.

We compute $f_{s,Q}(P)$ with the Miller Algorithm [19] presented in Algorithm 1:

Algorithm 1 MILLERLOOP(s, P, Q)- Compute $m = f_{s,Q}(P)$

```
$m \leftarrow 1$; $S \leftarrow Q$
for b from the second most significant bit of s to the least do
    $m \leftarrow m^2 \cdot l_{S,S}(P)/v_{[2]S}(P)$; $S \leftarrow [2]S$        ▷ DOUBLING STEP
    if $b = 1$ then
        $m \leftarrow m \cdot l_{S,Q}(P)/v_{S+Q}(P)$; $S \leftarrow S + Q$        ▷ ADDITION STEP
    end if
end for
    return $m$
```

2.3 Superoptimal pairing on $E/\mathbb{F}_p : y^2 = x^3 + b$

Let E be an elliptic curve defined over $\mathbb{F}_p$ with the form $E : y^2 = x^3 + b$ where $p \equiv 1 \mod 3$. Then there exists an automorphism of E defined by $\phi : (x, y) \mapsto (\xi x, y)$ where ξ is the primitive cube root of unity in $\mathbb{F}_p^{\star}$. Yanfeng et *al.* [18] used ϕ to construct variants of the ate pairing, twisted ate pairing and Weil pairing on pairing-friendly elliptic curves with general embedding degree k.

Let λ and μ be eigenvalues of ϕ corresponding to $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively. Let $\psi = \pi_p \circ \phi$, then eigenvalues of ψ are λ and $\omega = p\mu$ corresponding to $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively. Assume that $gcd(3, k) = 1$, then ω is a primitive $3k$-th root of unity in $\mathbb{F}_r$ and $r/(\omega^{3k} - 1)$.

Theorem 1. *[18] Let $cr = \sum_{i=0}^{n} a_i\omega^i = h(\omega), a_{n+1} = 0$ and $r^2 \nmid (\omega^{3k} - 1)$, then there exists a bilinear pairing*

$$a_{sup} : \mathbb{G}_2 \times \mathbb{G}_1 \rightarrow \mu_r$$

$$(Q, P) \mapsto \left(\prod_{j=0}^{n} \prod_{i=0}^{2} \left[f^{\omega^j}_{a_j,Q}(\phi^{2i}(P)) \cdot \frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} \right]^{\lambda^i} \right)^{\frac{p^k-1}{r}} \quad (2)$$

Where $h^{(j)} = \sum_{i=0}^{j} a_i\omega^i$. Let $h'(\omega) = \sum_{j=1}^{n} j a_j \omega^{j-1}$. Moreover, $a_{[a_0,\cdots,a_n]}(.,.)$ is non-degenerate if and only if $r \nmid [3kh(\omega) - (\omega^{3k} - 1)\omega h'(\omega)]$.

Since r divides $(\omega^{3k}-1)$, then the $3k$-th cyclotomic polynomial in ω yields $\Phi_{3k}(\omega) = 0 \mod r$ and therefore there exists a_i's such that $a_0 r = \sum_{i=1}^{\Phi(3k)-1} a_i\omega^i$. The a_i's is obtained by finding short vectors in the following $\varphi(3k)$-dimensionnal lattice

$$M = \begin{bmatrix} r & 0 & 0 & \ldots & 0 \\ -\omega & 1 & 0 & \ldots & 0 \\ -\omega^2 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -\omega^{\varphi(3k)-1} & 0 & 0 & \ldots & 1 \end{bmatrix}.$$

By the theorem of Minkowski [23] $|a_i| \leq r^{\frac{1}{\varphi(3k)}}$. The superoptimal pairings can be computed by $\log_2(r)/\varphi(3k)$ Miller iterations. Since $\log_2(r)/\varphi(3k) = \log_2(r)/(2\varphi(k))$ this Miller loop length is the half of that of optimal pairings.

Some authors have worked on the superoptimal pairing on elliptic curves such as Yanfeng et *al.* [18] and Fouotsa et *al.* [24]. In the next section, we define a superoptimal pairing formula on BW10-511 and BW14-351 curves using theorem 1.

3 Superoptimal pairing formula on BW10-511 and BW14-351 curves

In this section, we present the parameters $(t(x), q(x), r(x))$ obtained by Freeman et *al.* [22] of BW10 and BW14, techniques to optimise the superoptimal pairing on BW10 and BW14 and define the x-superoptimal pairing on BW10 and BW14.

The parameters of the pairing-friendly elliptic curve BW10 are:

$$\begin{aligned} t(x) &= x^3 + 1 \\ r(x) &= x^8 + x^7 - x^5 - x^4 - x^3 + x + 1 \\ p(x) &= 1/3(x^3 - 1)^2(x^{10} - x^5 + 1) + x^3 \end{aligned}$$

For $x = 2^7 + 2^{13} + 2^{26} - 2^{32}$, Yu Dai et *al.* [20] found $p(x)$ and $r(x)$ primes of sizes 511 bits and 256 bits respectively corresponding to 128-bit security level with $p \equiv 1$ mod 3 and they proposed an optimal ate pairing on BW10-511 curve.

similarly, the parameters of the pairing-friendly elliptic curve BW14 are:

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

For $x = 2^6 - 2^{12} - 2^{14} - 2^{22}$, Yu Dai et *al.* [20] found $p(x)$ and $r(x)$ primes of sizes 351 bits and 265 bits respectively corresponding to 128-bit security level with $p \equiv 1$ mod 3 and they proposed an optimal ate pairing on BW14-351 curve.

From Theorem 1, we defined the superoptimal pairing on BW10-511 and BW14-351 by :

$$\left(\prod_{j=0}^{n} \prod_{i=0}^{2} \left[f^{\omega^j}_{a_j,Q}(\phi^{2i}(P)) \cdot \frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} \right]^{\lambda^i} \right)^{\frac{p^k-1}{r}} . \tag{3}$$

In the case of BW10-511, the eigenvalues are $\lambda = x^{10}$ (see [20] page 6) and $\mu = \lambda^2 = x^{20}$. By using the function LLL in SageMath 8.4 calculator, we obtain a short vector of lattice M as,

$$V = (a_0, a_1, a_2, a_3, ..., a_7) = (x, 0, 1, 0, 0, 0, 0, 0)$$

So $h(\omega) = x + \omega^2$ since $a_0 = x, a_2 = 1$ and $a_i = 0$ otherwise, and

For the curve $BW10 - 511$, since, $f_{1,Q} \equiv 1$,

$$\prod_{j=0}^{n} \prod_{i=0}^{2} \left[f^{\omega^j}_{a_j,Q}(\phi^{2i}(P)) \right]^{\lambda^i} = \prod_{i=0}^{2} \left[f^{\omega^0}_{x,Q}(\phi^{2i}(P)) \cdot f^{\omega^8}_{1,Q}(\phi^{2i}(P)) \right]^{\lambda^i} = \prod_{i=0}^{2} \left[f_{x,Q}(\phi^{2i}(P)) \right]^{\lambda^i} .$$

For every i and $j = 0$

$$\frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} = \frac{l_{[x]Q,[0]Q}(\phi^{2i}(P))}{v_{[x]Q}(\phi^{2i}(P))} = \frac{v_{[x]Q}(\phi^{2i}(P))}{v_{[x]Q}(\phi^{2i}(P))} = 1.$$

For every i and $j = 1$, since $h(\omega) = 0 \mod r$ then $[x + \omega^2]Q = \mathcal{O}$ and $[\omega^2]Q = -[x]Q$,

$$\frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} = \frac{l_{[x]Q,[\omega^2]Q}(\phi^{2i}(P))}{v_{[x+\omega^2]Q}(\phi^{2i}(P))} = \frac{l_{[x]Q,-[x]Q}(\phi^{2i}(P))}{v_{[x+\omega^2]Q}(\phi^{2i}(P))} \equiv v_{[x]Q}(\phi^{2i}(P)),$$

this is because $v_{[x+\omega^2]Q}(\phi^{2i}(P))$ will be sent to 1 during the final exponentiation.

For every i and $2 \leq j \leq 6$,

$$\frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} = \frac{l_{[x+\omega^2]Q,[0]Q}(\phi^{2i}(P))}{v_{[x+\omega^2]Q}(\phi^{2i}(P))} = \frac{v_{[x+\omega^2]Q}(\phi^{2i}(P))}{v_{[x+\omega^2]Q}(\phi^{2i}(P))} = 1$$

Thus,

$$\begin{aligned} a_{sup}(Q,P) &= \left(\prod_{j=0}^{n}\prod_{i=0}^{2}\left[f^{\omega^j}_{a_j,Q}(\phi^{2i}(P)) \cdot \frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}\right]^{\lambda^i}\right)^{\frac{p^k-1}{r}} \qquad (4) \\ &= \left(\prod_{i=0}^{2}\left[f_{x,Q}(\phi^{2i}(P)) \cdot v_{[x]Q}(\phi^{2i}(P))\right]^{\lambda^i}\right)^{\frac{p^k-1}{r}} \qquad (5) \end{aligned}$$

Since $x < 0$, $x = -|x|$ and $f_{x,Q} = f^{-1}_{|x|,Q} \cdot f_{-1,[|x|]Q} = f^{-1}_{|x|,Q} \cdot v^{-1}_{[x]Q}$. Therefore Equation 5 yields :

$$a_{sup}(Q,P) = \left(\prod_{i=0}^{2}\left[f^{-1}_{|x|,Q}(\phi^{2i}(P))\right]^{\lambda^i}\right)^{\frac{p^k-1}{r}}.$$

Also, since $\lambda^2 = \mu$ and $\phi^4(P) = \phi(P)$ then,

$$a_{sup}(Q,P) = \left(f_{|x|,Q}(P) \cdot f^{\lambda}_{|x|,Q}(\phi^2(P)) \cdot f^{\mu}_{|x|,Q}(\phi(P))\right)^{-\frac{p^k-1}{r}}. \qquad (6)$$

For the curve BW14-351, the eigenvalues are $\lambda = -x^7$ (see [20] page 6) and $\mu = \lambda^2 = x^7 - 1$. By using the function LLL in SageMath 8.4 calculator, we obtain a short vector of lattice M as,

$$V = (a_0, a_1, a_2, a_3, ..., a_{11}) = (x, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0)$$

So $h(\omega) = x + \omega^8$ since $a_0 = x, a_8 = 1$ and $a_i = 0$. In the similar manner as on the curve BW10-511, we have the Eq. 6

The following Lemma 1 and Lemma 2 help to lower the cost of the inner exponents of the superoptimal pairing defined in Eq. 6 for the curves BW10-511 and BW14-351.

Lemma 1. *For any $f \in \mathbb{F}_{p^k}^*$, from the eigenvalues $\lambda = x^5 - 1 \mod r$ and $\mu = -x^5 \mod r$ of the BW10-511 curve, we have*

i) $f^{-x\mu\frac{p^k-1}{r}} = f^{(p^2)\frac{p^k-1}{r}}$.

ii) $f^{x\lambda\frac{p^k-1}{r}} = f^{(p^2-x)\frac{p^k-1}{r}}$.

Proof. The order of the elliptic curve $BW10-511$ is given by $|E(\mathbb{F}_p)| = p+1-t = p+1-(x^3+1) = p-x^3 = 0 \mod r$ i.e $p = x^3 \mod r$, this implies that $p^2 = x^6 \mod r$ so we have, $p^2 = -x\mu \mod r$ because $\mu = -x^5 \mod r$ and since $r/|E(\mathbb{F}_p)|$ then, there exists α such that $p^2+x\mu = \alpha r$ and for $f \in \mathbb{F}_{p^k}^*$, $f^{p^2+x\mu} = f^{\alpha r}$ when raising it to the power $\frac{p^k-1}{r}$ we then have that $f^{(p^2+x\mu)\frac{p^k-1}{r}} = 1$. So, $f^{(-x\mu)\frac{p^k-1}{r}} = f^{(p^2)\frac{p^k-1}{r}}$.

Similarly we have, $|E(\mathbb{F}_p)| = p+1-t = p+1-(x^3+1) = p-x^3 = 0 \mod r$ i.e $p = x^3 \mod r$, this implies that $p^2 - x = x^6 - x \mod r$ so we have, $p^2 - x = x\lambda \mod r$ because $\lambda = x^5 - 1 \mod r$ and since $r/|E(\mathbb{F}_p)|$ then, there exists β such that $p^2 - x - x\lambda = \beta r$ and for $f \in \mathbb{F}_{p^k}^*$, $f^{p^2-x-x\lambda} = f^{\beta r}$ when raising it to the power $\frac{p^k-1}{r}$ we then have that $f^{(p^2-x-x\lambda)\frac{p^k-1}{r}} = 1$. So, $f^{(x\lambda)\frac{p^k-1}{r}} = f^{(p^2-x)\frac{p^k-1}{r}}$. □

Lemma 2. *For any $f \in \mathbb{F}_{p^k}^*$, from the eigenvalues $\lambda = -x^7 \mod r$ and $\mu = x^7 - 1 \mod r$ of the BW14-351 curve, we have*

i) $f^{x\mu\frac{p^k-1}{r}} = f^{(p)\frac{p^k-1}{r}}$.

ii) $f^{-x\lambda\frac{p^k-1}{r}} = f^{(p+x)\frac{p^k-1}{r}}$.

Proof. The order of the elliptic curve $BW14-351$ is given by $|E(\mathbb{F}_p)| = p+1-t = p+1-(x^8-x+1) = p-x(x^7-1) = p-x\mu$ and since $r/|E(\mathbb{F}_p)|$ then, there exists α such that $p - x\mu = \alpha r$ and for $f \in \mathbb{F}_{p^k}^*$, $f^{p-x\mu} = f^{\alpha r}$ when raising it to the power $\frac{p^k-1}{r}$ we then have that $f^{(p-x\mu)\frac{p^k-1}{r}} = 1$. So, $f^{(x\mu)\frac{p^k-1}{r}} = f^{(p)\frac{p^k-1}{r}}$.

Similarly we have, $|E(\mathbb{F}_p)| = p+1-t = p+1-(x^8-x+1) = p+x+x(-x^7) = p+x+x\lambda$ and since $r/|E(\mathbb{F}_p)|$ then, there exists β such that $p+x+x\lambda = \beta r$ and for $f \in \mathbb{F}_{p^k}^*$, $f^{p+x+x\lambda} = f^{\beta r}$ when raising it to the power $\frac{p^k-1}{r}$ we then have that $f^{(p+x+x\lambda)\frac{p^k-1}{r}} = 1$. So, $f^{(-x\lambda)\frac{p^k-1}{r}} = f^{(p+x)\frac{p^k-1}{r}}$. □

We then define a x-superoptimal pairing on BW10-511 and BW14-351, since a fixed non-degenerate power of a pairing is still a pairing.

Theorem 2. *Since $gcd(x, r) = 1$, we derive two new pairings called x-superoptimal pairing defined as*

$$a^{x}_{sup_1}(Q, P) = \left(\left(f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))\right)^{-x} \cdot \left(f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))\right)^{p^2}\right)^{\frac{p^k-1}{r}} \tag{7}$$

For $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. It is a non-degenerate bilinear pairing on $BW10 - 511$.

and

$$a^{x}_{sup_2}(Q, P) = \left(\left(f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))\right)^{-x} \cdot \left(f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))\right)^{-p}\right)^{\frac{p^k-1}{r}} \tag{8}$$

For $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. It is a non-degenerate bilinear pairing on $BW14 - 351$

Proof. Let $f_1 = f_{|x|,Q}(P)$, $f_2 = f_{|x|,Q}(\phi^2(P))$ and $f_3 = f_{|x|,Q}(\phi(P))$ then, $a_{sup_1}(Q, P) = \left(f_1 \cdot f_2^{\lambda} \cdot f_3^{\mu}\right)^{-\frac{p^k-1}{r}}$. By raising to the power x and using Lemma 1, we have :

$$\begin{aligned} a^{x}_{sup_1}(Q, P) &= \left(f_1^{x} \cdot f_2^{x\lambda} \cdot f_3^{x\mu}\right)^{-\frac{p^k-1}{r}} \\ &= \left(f_1^{-x} \cdot f_2^{x-p^2} \cdot f_3^{p^2}\right)^{\frac{p^k-1}{r}} \\ &= \left((f_1 \cdot f_2^{-1})^{-x} \cdot (f_2^{-1} \cdot f_3)^{p^2}\right)^{\frac{p^k-1}{r}}. \end{aligned}$$

Similarly, we have $a_{sup_2}(Q, P) = \left(f_1 \cdot f_2^{\lambda} \cdot f_3^{\mu}\right)^{-\frac{p^k-1}{r}}$. By raising to the power x and using Lemma 2, we have :

$$\begin{aligned} a^{x}_{sup_2}(Q, P) &= \left(f_1^{x} \cdot f_2^{x\lambda} \cdot f_3^{x\mu}\right)^{-\frac{p^k-1}{r}} \\ &= \left(f_1^{-x} \cdot f_2^{p+x} \cdot f_3^{-p}\right)^{\frac{p^k-1}{r}} \\ &= \left((f_1 \cdot f_2^{-1})^{-x} \cdot (f_2^{-1} \cdot f_3)^{-p}\right)^{\frac{p^k-1}{r}}. \end{aligned}$$

□

Remark 1. *The superoptimal pairing formula obtained in Eq 6 for BW10 and BW14 curves is exactly the same as the one obtained for BW13 and BW19 curves in [24]. Moreover the only difference between the x-superoptimal formulas found in this work and the previous work done by Fouotsa et al. [24] is on the power of $f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$.*

In the following section, we present some algorithms and evaluate the cost of the Miller loop of the x-superoptimal pairing defined in Theorem 2 for the curves BW10-511 and BW14-351.

4 Faster Evaluation of the Miller loop for the x-superoptimal pairings

This section evaluates the cost of the miller loop of the x-superoptimal pairing on BW10-511 and BW14-351 defined in Thereom 2 by using the algorithms presented by Guillevic et *al.* [8] and by Fouotsa et *al.* [24].

4.1 Miller loop algorithm and his sub-algorithms on BW10-511 and BW14-351 curves

Under this subsection, we use the quadratic twist on $BW10-511$ and $BW14-351$ curves, which enable computations to be done in the subfields $\mathbb{F}_{p^5}$ and $\mathbb{F}_{p^7}$ and some algorithms [24] in order to improve x-superoptimal pairing cost.

For this fact, we consider the equation of the BW10-511 curve given by $E : y^2 = x^3 - 2$ and his quadratic twist with equation defined by $E^{'} : y^2 = x^3 - 2\tau^{-3}$ over $\mathbb{F}_{p^5}$ where $\tau \in \mathbb{F}_{p^5}$ with the isomorphism $\varphi_1 : (x, y) \longmapsto (x\tau, y\tau v)$, where the tower extension of $\mathbb{F}_{p^{10}}$ is given by $\mathbb{F}_p \xrightarrow{\tau^5+4} \mathbb{F}_{q^5} \xrightarrow{v^2-\tau} \mathbb{F}_{q^{10}}$ (see Yu Dai et *al.* [20] for more evidence).

Similarly, we consider the equation of the BW14-351 curve given by $E : y^2 = x^3+3$ and his quadratic twist with equation defined by $E^{'} : y^2 = x^3 + 3\tau^{-3}$ over $\mathbb{F}_{p^7}$ where $\tau \in \mathbb{F}_{p^7}$ with the isomorphism $\varphi_2 : (x, y) \longmapsto (x\tau, y\tau v)$, where the tower extension of $\mathbb{F}_{p^{14}}$ is given by $\mathbb{F}_p \xrightarrow{\tau^7-2} \mathbb{F}_{q^7} \xrightarrow{v^2-\tau} \mathbb{F}_{q^{14}}$.

Moreover, for $P = (x, y) \in E$, we have $\phi(P) = (\xi x, y)$ and $\phi^2(P) = (\xi^2 x, y)$ since ϕ is an automorphism on E and ξ is the primitive cube root of unity, then the functions $f_{|x|,Q}(P)$, $f_{|x|,Q}(\phi(P))$ and $f_{|x|,Q}(\phi^2(P))$ have different $x-$coordinate of P. From the algorithms ([8], Algorithms 3,4,5 from page 15) of Guillevic et *al.*, we observe that λ_d and μ_d are identical for all Miller's functions $f_{|x|,Q}(P)$, $f_{|x|,Q}(\phi(P))$ and $f_{|x|,Q}(\phi^2(P))$ since they do not depend on the point P but only on the point Q. In addition, $(\frac{\mu_d}{\lambda_d})'s$ are factors of each Miller's functions, thus $(\frac{\mu_d}{\lambda_d})'s$ cancel themselves in the products $f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))$ and $f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$.

Algorithm 2 [24] takes as input the Jacobian coordinates $S = (X, Y, Z, Z_2), Q = (x_Q, y_Q) \in \mathbb{G}_2 = E^{'}(\mathbb{F}_{p^{k/2}})[r] \cap ker(\pi_P - [P])$, computes the point addition $S + Q$ as $\mathbf{S} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z}, \mathbf{Z^2})$ and evaluate the line (SQ) at P, $\phi(P)$, $\phi^2(P) \in \mathbb{G}_1 = E(\mathbb{F}_{p^k})[r] \cap ker(\pi_p - [1])$ as $(\lambda_n, \lambda_{n1}, \lambda_{n2})$ where λ_n and λ_{n2} represents the numerator and the denominator respectively for the function $f = f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))$, also λ_{n1} and λ_{n2} represents the numerator and the denominator respectively for the function $g = f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$.

Algorithm 2 ADDING LINE Given $S, Q \in \mathbb{G}_2$, compute $S + Q$ and the evaluation of the lines (SQ) at $P, \phi(P)$ and $\phi^2(P)$ in $\mathbb{G}_1$

```
$(X, Y, Z, Z_2) \leftarrow S$; $(x_Q, y_Q) \leftarrow Q$; $(x_P, y_P) \leftarrow P$; $t_1 \leftarrow x_Q \cdot Z_2 - X$; $t_2 \leftarrow y_Q \cdot Z \cdot Z_2 - Y$;
$t_3 \leftarrow t_1^2$; $t_4 \leftarrow t_1 \cdot t_3$; $t_5 \leftarrow X \cdot t_3$; $\mathbf{X} \leftarrow t_2^2 - (t_4 + 2t_5)$; $\mathbf{Y} \leftarrow t_2 \cdot (t_5 - \mathbf{X}) - Y \cdot t_4$; $\mathbf{Z} \leftarrow Z \cdot t_1$;
$\lambda_d \leftarrow \mathbf{Z}$; $t_6 \leftarrow \lambda_d \cdot (y_P - y_Q)$; $\lambda_n \leftarrow t_6 - t_2 \cdot (x_P - x_Q)$; $\lambda_{n1} \leftarrow t_6 - t_2 \cdot (x_{\phi(P)} - x_Q)$;
$\lambda_{n2} \leftarrow t_6 - t_2 \cdot (x_{\phi^2(P)} - x_Q)$
return $S = (X, Y, Z, Z^2), \lambda_n, \lambda_{n1}, \lambda_{n2}$
```

Algorithm 3 [24] takes as input $S = (X, Y, Z, Z_2) \in \mathbb{G}_2 = E^{'}(\mathbb{F}_{p^{k/2}})[r] \cap ker(\pi_P - [P])$, computes the point doubling $[2]S$ as $\mathbf{S} = (\mathbf{X}, \mathbf{Y}, \mathbf{Z}, \mathbf{Z^2})$ and evaluate the tangent at S mapped at P, $\phi(P)$, $\phi^2(P) \in \mathbb{G}_1 = E(\mathbb{F}_{p^k})[r] \cap ker(\pi_p - [1])$ as $(\lambda_n, \lambda_{n1}, \lambda_{n2})$ where λ_n and λ_{n2} represents the numerator and the denominator respectively for the function $f = f_{|x|,Q}(P) \cdot f_{|x|,Q}^{-1}(\phi^2(P))$, also λ_{n1} and λ_{n2} represents the numerator and the denominator respectively for the function $g = f_{|x|,Q}^{-1}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$.

Algorithm 3 DOUBLING LINE Given $S \in \mathbb{G}_2$, compute $[2]S$ and the evaluation of the tangent S mapped at $P, \phi(P)$ and $\phi^2(P)$ in $\mathbb{G}_1$

```
$(X, Y, Z, Z_2) \leftarrow S$
$(x_P, y_P) \leftarrow P$;
$t_1 \leftarrow Y^2$
$t_2 \leftarrow 4X \cdot t_1$
if $a = -3u^2$for a small $u \in \mathbb{F}_p$ then
    $t_3 \leftarrow 3(X - uZ_2) \cdot (X + uZ_2)$
else
    $t_3 \leftarrow 3X^2 + a \cdot Z_2^2$
    $\mathbf{X} \leftarrow t_3^2 - 2t_2$
    $\mathbf{Y} \leftarrow t_3 \cdot (t_2 - \mathbf{X}) - 8t_1^2$
    $\mathbf{Z} \leftarrow Z \cdot 2Y$
    $\lambda_d \leftarrow \mathbf{Z}.Z_2$
    $t_4 \leftarrow \lambda_d \cdot y_P - 2t_2$
    $\lambda_n \leftarrow t_4 - t_3 \cdot (Z_2 \cdot x_P - X)$
    $\lambda_{n1} \leftarrow t_4 - t_3 \cdot (Z_2 \cdot x_{\phi(P)} - X)$
    $\lambda_{n2} \leftarrow t_4 - t_3 \cdot (Z_2 \cdot x_{\phi^2(P)} - X)$
end if
        return $S = (X, Y, Z, Z^2), \lambda_n, \lambda_{n1}, \lambda_{n2}$
```

Algorithm 4 [24] provides the vertical line passing through S at P, $\phi(P)$ and $\phi^2(P)$ as $(\mu_n, \mu_{n1}, \mu_{n2})$ where μ_n and μ_{n2} represents the numerator and the denominator respectively for the function $f = f_{|x|,Q}(P) \cdot f_{|x|,Q}^{-1}(\phi^2(P))$ defined by $V_S(P) =$

$\dfrac{Z_2 \cdot x_P - X}{Z_2 \cdot x_{\phi^2(P)} - X}$ in projective coordinates, also μ_{n1} and μ_{n2} represents the numerator and the denominator respectively for the function $g = f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$ defined by $V_S(P) = \dfrac{Z_2 \cdot x_{\phi(P)} - X}{Z_2 \cdot x_{\phi^2(P)} - X}$ in projective coordinates.

Algorithm 4 VERTICAL LINE Compute the line through S and $-S$ evaluated at $P, \phi(P)$ and $\phi^2(P)$ in $\mathbb{G}_1$

```
$(X, Y, Z, Z_2) \leftarrow S$; $(x_P, y_P) \leftarrow P$; $\mu_n = Z_2 \cdot x_P - X$; $\mu_{n1} = Z_2 \cdot x_{\phi(P)} - X$; $\mu_{n2} = Z_2 \cdot x_{\phi^2(P)} - X$
return $\mu_n, \mu_{n1}, \mu_{n2}$
```

Algorithm 5 [24] uses the three helper functions that are detailed in Algorithms 2, 3 and 4 and compute the function f and g as $\frac{n_f}{d_f}$ and $\frac{n_g}{d_g}$ respectively. Note that the Algorithms 2, 3, 4 and 5 are running in polynomial time.

Algorithm 5 Miller Loop for faster x-superoptimal pairing.

```
Require: $|x| = 2^n + \sum_{i=0}^{n-1} s_i 2^i$, where $s_i \in \{0, -1, 1\}$, $P \in E(\mathbb{F}_p)$ and $Q \in E^{'}(\mathbb{F}_{p^{k/2}})$
Ensure: $[x]Q$, numerators and denominators of $f = f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))$ and
    $g = f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$.
$(n_f, d_f, n_g, d_g) \leftarrow (1, 1, 1, 1)$; $S \leftarrow Q$
for $i$ from $n-1$ down to 0 do
    $(\lambda_n, \lambda_{n1}, \lambda_{n2}) \leftarrow l_{S,S}(P)$, $S \leftarrow [2]S$          ▷ DOUBLE LINE
    $(\mu_n, \mu_{n1}, \mu_{n2}) \leftarrow v_S(P)$                                ▷ VERTICAL LINE
    $(n_f, d_f) \leftarrow (n_f^2 \lambda_n \mu_{n2}, d_f^2 \mu_n \lambda_{n2})$
    $(n_g, d_g) \leftarrow (n_g^2 \mu_{n2} \lambda_{n1}, d_g^2 \lambda_{n2} \mu_{n1})$                ▷ UPDATE 1
    if $s_i = \pm 1$ then
        $(\lambda_n, \lambda_{n1}, \lambda_{n2}) \leftarrow l_{S,[s_i]Q}(P)$, $S \leftarrow S + [s_i]Q$    ▷ ADDITION LINE
        $(\mu_n, \mu_{n1}, \mu_{n2}) \leftarrow v_S(P)$                            ▷ VERTICAL LINE
        $(n_f, d_f) \leftarrow (n_f \lambda_n \mu_{n2}, d_f \mu_n \lambda_{n2})$
        $(n_g, d_g) \leftarrow (n_g \mu_{n2} \lambda_{n1}, d_g \lambda_{n2} \mu_{n1})$            ▷ UPDATE 2
    end if
end for
    return $f = \frac{n_f}{d_f}$ and $g = \frac{n_g}{d_g}$
```

The following formula gives the cost of the Algorithm 5.

$$\begin{aligned} C &= (\log_2(x) - 1)\big(C_{DBLINE} + C_{VerLINE}\big) + (\log_2(x) - 2)C_{UPDATE1} \\ &\quad + (HW_{2-NAF}(x) - 1)\big(C_{ADDLINE} + C_{VerLINE} + C_{UPDATE2}\big). \end{aligned} \tag{9}$$

4.2 Evaluation cost of Algorithm 5

In this subsection, we evaluate the cost of Algorithm 5. Let M, S and I denote the cost of the multiplication, squaring and inversion in $\mathbb{F}_p$, whereas, M_k, S_k, I_k, f_k^i, E_x denote the cost of the multiplication, squaring, inversion, $p-th$ Frobenius operation and the power of x in F_{p^k} respectively.

Algorithm 5 is made of five steps that are DOUBLE LINE, VERTICAL LINE, UPDATE 1, ADDITION LINE and UPDATE 2. For this fact, the DOUBLE LINE step use the Algorithm 3 and cost 7 multiplications in $\mathbf{F}_{p^{k/2}}$, 6 squaring in $\mathbf{F}_{p^{k/2}}$ and 4 multiplications in $\mathbf{F}_{p^k}$ that is $4k$ multiplications in $\mathbf{F}_p$. Similarly, the ADDITION LINE step use the Algorithm 2 and cost 11 multiplications in $\mathbf{F}_{p^{k/2}}$ and 3 squaring in $\mathbf{F}_{p^{k/2}}$. The UPDATE 1 step cost 8 multiplications in $\mathbf{F}_{p^{k/2}}$ and 4 squaring in $\mathbf{F}_{p^{k/2}}$. The UPDATE 2 STEP step cost just 8 multiplications in $\mathbf{F}_{p^{k/2}}$ and finally the VERTICAL LINE step use the Algorithm 4 and it is cost free since the BW10-511 and BW14-351 curves admit a quadratic twist which enable computations to be done in the subfields $\mathbb{F}_{p^5}$ and $\mathbb{F}_{p^7}$ respectively.

The following Table 1 summarizes the cost estimation of each step of Algorithm 5.

Table 1 Cost estimation of each step of Algorithm 5.

Line (embedding degree k = 10, 14)	Cost operation
Doubling line	$7M_{k/2} + 6S_{k/2} + 4kM$
Adding line	$11M_{k/2} + 3S_{k/2}$
Vertical line	0
Update 1	$8M_{k/2} + 4S_{k/2}$
Update 2	$8M_{k/2}$

4.3 Arithmetic in $\mathbb{F}_{p^5}$, $\mathbb{F}_{p^7}$, $\mathbb{F}_{p^{10}}$ and $\mathbb{F}_{p^{14}}$

In this section, we present the arithmetic cost in $\mathbb{F}_{p^5}$, $\mathbb{F}_{p^7}$, $\mathbb{F}_{p^{10}}$ and $\mathbb{F}_{p^{14}}$.

In [21], the authors El Mrabet et *al* have reduced the multiplication in finite field extensions of degree 5 and 7 through the Newton's interpolation method where $M_5 = 9M + 137A_p$ and $M_7 = 13M + 271A_p$ and A_p is the cost of addition in $\mathbb{F}_p$.

So if we neglect the addition cost in $\mathbb{F}_p$, then we have the optimal cost in $\mathbb{F}_{p^5}$ and $\mathbb{F}_{p^7}$ [21].

Table 2 Operations cost by El Mrabet et *al.*

k	M_k	S_k	I_k	f_k^i
5	$9M$	$9M$	$65M$	$4M$
7	$13M$	$13M$	$102M$	$6M$

Where $I_5 = 3f_5^i + 2M_5 + I_1 + 10M$, $I_7 = 4f_7^i + 3M_7 + I_1 + 14M$, $I_1 = 25M$ and $f_k^i = (k-1)M$ if k is prime [8].

Also according to [20], Yu Dai et *al.* presented the following costs of arithmetic operations in the field $\mathbb{F}_{p^{10}}$ and $\mathbb{F}_{p^{14}}$ for the curves BW10-511 and BW14-351 respectively :

Table 3 Operation costs by Yu Dai et *al.*

k	M_k	S_k	I_k	f_k^i
10	$2M_5$	$3M_5$	$I_5 + 2M_5 + 2S_5$	$8M$
14	$2M_7$	$3M_7$	$I_7 + 2M_7 + 2S_7$	$12M$

Note that in the table 3, the costs is obtained from [20] by neglecting some additions and modular reduction in $\mathbb{F}_{p^5}$ and $\mathbb{F}_{p^7}$, also by supposing that $M_u = M$ and $S_u = S$ in $\mathbb{F}_p$ where M_u and S_u represent the multiplication without reduction and the squaring without reduction in $\mathbb{F}_p$ respectively.

4.4 Evaluation of x-superoptimal Pairing on $BW10-511$ and $BW14-351$

The x-superoptimal pairing on $BW10-511$ from Theorem 2 is given by

$$a^x_{sup_1}(Q,P) = \left(\left(f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P)) \right)^{-x} \cdot \left(f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P)) \right)^{p^2} \right)^{\frac{p^k-1}{r}}.$$

From the seed $x = 2^7 + 2^{13} + 2^{26} - 2^{32}$, we have $\log_2(x) = 32$, $HW_{2-NAF}(x) = 4$ and $|x| = 2^{32} - 2^{26} - 2^{13} - 2^7$.

By using the formula of Eq. 9, we compute $f = f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))$ and $g = f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$ as follow :

$$\begin{aligned} C &= 31[(7M_5 + 6S_5 + 4 \times 10M) +] + 30[8M_5 + 4S_5] \\ &\quad + 3[(11M_5 + 3S_5) + 8M_5] \\ &= 8701M. \end{aligned}$$

The last step consists to compute $(n_f \cdot d_f^{-1})^{-x} \cdot (n_g \cdot d_g^{-1})^{p^2}$ at cost of 3 multiplications, 2 inversions, 1 p^2-Frobenius and 1 exponentiation by $-x$ in $\mathbb{F}_{p^{10}}$. For the cost of $3M_{10} + 2I_{10} + 1f_k^i + 1E_{-x} = 3M_{10} + 2I_{10} + 1f_{10}^i + 32M_{10} + 3S_{10} = 921M$. The total cost of the Miller loop is then $9622M$.

Similarly, the x-superoptimal pairing on $BW14-351$ from Theorem 2 is given by

$$a^x_{sup_2}(Q,P)=\left(\left(f_{|x|,Q}(P)\cdot f^{-1}_{|x|,Q}(\phi^2(P))\right)^{-x}\cdot\left(f^{-1}_{|x|,Q}(\phi^2(P))\cdot f_{|x|,Q}(\phi(P))\right)^{-p}\right)^{\frac{p^k-1}{r}}.$$

From the seed $x=2^6-2^{12}-2^{14}-2^{22}$, we have $\log_2(x)=22$, $HW_{2-NAF}(x)=4$ and $|x|=2^{22}+2^{14}+2^{12}-2^6$.

By using the formula of Eq. 9, we compute $f=f_{|x|,Q}(P)\cdot f^{-1}_{|x|,Q}(\phi^2(P))$ and $g=f^{-1}_{|x|,Q}(\phi^2(P))\cdot f_{|x|,Q}(\phi(P))$ as follow :

$$\begin{aligned} C &= 21[(7M_7+6S_7+4\times 14M)+]+20[8M_7+4S_7]\\ &\quad+3[(11M_7+3S_7)+8M_7]\\ &= 8703M. \end{aligned}$$

The last step consists to compute $(n_f\cdot d_f^{-1})^{-x}\cdot(n_g\cdot d_g^{-1})^{-p}$ at cost of 3 multiplications, 3 inversions, 1 p-Frobenius and 1 exponentiation by $-x$ in $\mathbb{F}_{p^{14}}$. For the cost of $3M_{14}+3I_{14}+1f^i_k+1E_{-x}=3M_{14}+3I_{14}+1f^i_{14}+22M_{14}+3S_{14}=1241M$. The total cost of the Miller loop is then $9944M$.

5 Comparison

In Table 4, we compare the theoretical costs of the optimal ate pairing done by Yu Dai et *al.* and the x-superoptimal pairing done in this paper for the BW10-511 and BW14-351 curves.

Table 4 Comparison of the computation cost of the x-superoptimal pairing of our work with the optimal ate pairing done by Yu Dai et *al.* on BW10-511 and BW14-351 curve at 128-bit security level.

Curve	Pairing	Miller loop	Final exponentiation	Total cost
$BW10-511$	optimal Ate [20]	$11123M$	$16060M+I_1$	$27183M+I_1$
	x-superoptimal(this work)	$9622M$	$16060M+I_1$	$25682M+I_1$
$BW14-351$	optimal Ate [20]	$12681M$	$19190M+I_1$	$31871M+I_1$
	x-superoptimal (this work)	$9944M$	$19190M+I_1$	$29134M+I_1$

Note that in the Table 4, the costs of the miller loop and final exponentiation of the optimal ate pairings for BW10-511 and BW14-351 [20] is obtained by neglecting some additions and modular reduction in $\mathbb{F}_{p^7}$, also by supposing that $M_u=S_u=M$ in $\mathbb{F}_p$ where M_u and S_u represent the multiplication without reduction and the squaring without reduction in $\mathbb{F}_p$ respectively.

From Table 4, we observe that the Miller loop of the new formula of x-superoptimal pairing is about 13.5% and 21.6% faster than the optimal ate pairing on $BW10-511$ and $BW14-351$ curves respectively done by Yu Dai et *al.* [20] and the overall improvement (Miller loop and final exponentiation) is about 5.5% and 8.6% over their optimal ate pairing respectively.

6 Conclusion

In this paper, We found two new formulas of x-superoptimal pairing faster than optimal ate pairing on BW10-511 and BW14-351 curves. Their Miller loop is about 13.5% and 21.6% faster than the optimal ate pairing on $BW10 - 511$ and $BW14 - 351$ respectively done by Yu Dai et *al.* The overall improvement (Miller loop and final exponentiation) is about 5.5% and 8.6% respectively over the other pairing. We also implemented the x-superoptimal pairing on BW10-511 and BW14-351 curves in the MAGMA software to ensure correctness of our formulas.

References

[1] Weil, A.: Variétés Abéliennes et Courbes algébriques. Publ. Inst. Math. Univ. Strasbourg, vol. 8 (1948)

[2] Menezes, A., Okamoto, T., Vanstone., S.: Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory **vol. 39(5)**, 1639–1646 (1993)

[3] Zanon, G., Simplício, M.A., Jr., Pereira, G.C.C.F., Doliskani, J., Barreto, P.S.L.M.: Faster key compression for isogeny-based cryptosystems. IEEE Trans. Comput., 68–56887012019

[4] De Feo, L., Masson, S., Petit, C., Sanso, A.: Verifable delay functions from supersingular isogenies and pairings. In Steven D.G., Shiho M., eds. Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8–12, 2019, Proceedings **11921**, 248–277 (2019)

[5] Brickell, E., Li, J.: Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities. IEEE Trans. Dependable Secur. Comput. **9**(3), 345–360 (2012) https://doi.org/10.1109/TDSC.2011.63

[6] Boneh, D., Franklin, M.K.: Identity-based encryption from the weil pairing. SIAM J. Comput. **32**(3), 586–615 (2003) https://doi.org/10.1137/S0097539701398521

[7] Joux, A.: A one round protocol for tripartite diffie-hellman. J. Cryptol. **17**(4), 263–276 (2004) https://doi.org/10.1007/S00145-004-0312-Y

[8] Guillevic, A., Masson, S., Thomé, E.: Cocks-Pinch curves of embedding degrees five to eight and optimal ate pairing computation. Des. Codes Cryptogr. **88**(6), 1047–1081 (2020) https://doi.org/10.1007/S10623-020-00727-W

[9] Aranha, D.F., Fuentes-Castañeda, L., Knapp, E., Menezes, A., Rodríguez-Henríquez, F.: Implementing pairings at the 192-bit security level. In: Abdalla, M., Lange, T. (eds.) Pairing-Based Cryptography – Pairing 2012, pp. 177–195. Springer, Berlin, Heidelberg (2013)

[10] Ghammam, L., Fouotsa, E.: On the computation of the optimal ate pairing at the 192-bit security level. IACR Cryptol. ePrint Arch., 130 (2016)

[11] Mbang, N.B., Freitas Aranha, D., Fouotsa, E.: Computing the optimal ate pairing over elliptic curves with embedding degrees 54 and 48 at the 256-bit security level. Int. J. Appl. Cryptogr. **4**(1), 45–59 (2020) https://doi.org/10.1504/IJACT.2020.107167

[12] Iida, T., Ikesaka, K., Kodera, Y., Kusaka, T., Nogami, Y.: Improvement of optimal-ate pairing on cocks-pinch curve with embedding degree 6 in affine coordinates. In: 2022 Tenth International Symposium on Computing and Networking, CANDAR 2022 - Workshops, Himeji, Japan, November 21-24, 2022, pp. 309–315 (2022). https://doi.org/10.1109/CANDARW57323.2022.00043

[13] Mbang, N.B., Fouotsa, E., Lélé, C.: Parallel computation of optimal ate cryptographic pairings at the 128, 192 and 256-bit security levels using elliptic net algorithm. CoRR **abs/2003.11286** (2020) 2003.11286

[14] Cai, S., Hu, Z., Zhao, C.: Faster final exponentiation on the KSS18 curve. IEICE Trans. Fundam. Electron. Commun. Comput. Sci. **105-A**(8), 1162–1164 (2022) https://doi.org/10.1587/TRANSFUN.2021EAL2086

[15] Fotiadis, G., Martindale, C.: Optimal tnfs-secure pairings on elliptic curves with even embedding degree. IACR Cryptol. ePrint Arch., 969 (2018)

[16] Ghammam, L., Fouotsa, E.: Adequate elliptic curves for computing the product of n pairings. In: Duquesne, S., Petkova-Nikova, S. (eds.) Arithmetic of Finite Fields - 6th International Workshop, WAIFI 2016, Ghent, Belgium, July 13-15, 2016, Revised Selected Papers. Lecture Notes in Computer Science, vol. 10064, pp. 36–53 (2016). https://doi.org/10.1007/978-3-319-55227-9_3

[17] Duquesne, S., Mrabet, N.E., Fouotsa, E.: Efficient computation of pairings on jacobi quartic elliptic curves. Journal of Mathematical Cryptology **8**(4), 331–362 (2014) https://doi.org/10.1515/jmc-2013-0033

[18] Feng, Q.Y., Ming, T.C., Baoan, G., Zhi, X.M.: Super-optimal pairings. In: Mechanical Engineering, Materials and Energy II. Applied Mechanics and Materials, vol. 281, pp. 127–133 (2013). https://doi.org/10.4028/www.scientific.net/AMM.281.127

[19] Vercauteren, F.: Optimal pairings. IEEE Trans. Inf. Theory **56**(1), 455–461 (2010) https://doi.org/10.1109/TIT.2009.2034881

[20] Dai, Y., He, D., Peng, C., Yang, Z., Zhao, C.: Revisiting pairing-friendly curves with embedding degrees 10 and 14. IACR Cryptol. ePrint Arch., 1958 (2023)

[21] El Mrabet, N., Guillevic, A., Ionica, S.: Efficient multiplication in finite field extensions of degree 5. In: Nitaj, A., Pointcheval, D. (eds.) Progress in Cryptology - AFRICACRYPT 2011 - 4th International Conference on Cryptology in Africa, Dakar, Senegal, July 5-7, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6737, pp. 188–205 (2011). https://doi.org/10.1007/978-3-642-21969-6_12

[22] Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptol. **23**(2), 224–280 (2010) https://doi.org/10.1007/s00145-009-9048-z

[23] Minkowski, H.: Geometrie der Zahlen vol. Druck und Verlag von B.G. Teubner, (1910)

[24] Fouotsa, E., Azebaze, L.G., Ayissi, R.: x-superoptimal pairings on some elliptic curves with odd prime embedding degrees. AAECC (2023). https://doi.org/10.1007/s00200-023-00596-5