Noname manuscript No.
(will be inserted by the editor)

x-Superoptimal Pairings on some Elliptic Curves with Odd Prime Embedding Degrees

Emmanuel Fouotsa · Laurian Azebaze Guimagang · Raoul Ayissi

Received: date / Accepted: date

Abstract The choice of the elliptic curve for a given pairing based protocol is primordial. For many cryptosystems based on pairings such as group signatures and their variants (EPID, anonymous attestation, etc) or accumulators, operations in the first pairing group $\mathbb{G}$ of points of the elliptic curve is more predominant. At 128-bit security level two curves $BW13-P310$ and $BW19-P286$ with odd embedding degrees 13 and 19 suitable for super optimal pairing have been recommended for such pairing based protocols . But a prime embedding degree ($k = 13; 19$) eliminates some important optimisation for the pairing computation. However The Miller loop length of the superoptimal pairing is the half of that of the optimal ate pairing but involve more exponentiations that affect its efficiency. In this work, we successfully develop methods and construct algorithms to efficiently evaluate and avoid heavy exponentiations that affect the efficiency of the superoptimal pairing. This leads to the definition of new bilinear and non degenerate pairing on $BW13-P310$ and $BW19-P286$ called x-superoptimal pairing wchich is about 27.3% and 49% faster than the optimal ate pairing previousely computed on $BW13-P310$ and $BW19-P286$ respectively.

E. Fouotsa
Department of Mathematics
Higher Teacher Training College
The University of Bamenda, Cameroon
E-mail: emmanuelfouotsa@yahoo.fr

L. Azebaze
Department of Mathematics
Faculty of Sciences
The University of Yaounde, Cameroon
E-mail: azebazelaurian@yahoo.fr

R. Ayissi
Department of Mathematics
Faculty of Sciences
The University of Yaounde, Cameroon
E-mail: raoulayissi@yahoo.fr

Keywords Optimal pairing · Superoptimal pairing · x-Superoptimal pairing · Miller function · $BW13$ · $BW19$.

1 Introduction

Elliptic Curve Based Pairings are used in many cryptographic protocols namely aggregate and verifiably encrypted signatures [1], identity-based encryption [2] and Short signature from Weil pairing [3]. Nowadays they are also used for faster public keys compression for isogeny-based cryptosystems (key exchange) [4] and to construct verifiable delay functions from supersingular isogenies [5].

A pairing is a non-degenerate bilinear map e from the cartesian product of two abelian additive groups $\mathbb{G}_1$ and $\mathbb{G}_2$ to an abelian multiplicative group $\mathbb{G}_T$. 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). For elliptic curve pairings the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ consist of points on elliptic curve E, the group $\mathbb{G}_T$ is embedded in a finite extension field $\mathbb{F}_{p^k}$. These groups are usually of prime order r. Parameters r, p, k are chosen in order to ensure that security holds in each group while maintaining the best efficiency of the pairing. By security, we here mean the hardness of the Discrete Logarithm Problem (DLP) on $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$. An efficient computation of a pairing is based on the Miller algorithm wchich involves addition of points and evaluation of functions and which the loop length depends on the parameter r. Vercauteren [6] introduced the concept of an optimal pairing with Miller iterations $\frac{\log_2(r)}{\varphi(k)}$ then, $e(.,.)$ is called an optimal pairing if it can be computed in $\frac{\log_2(r)}{\varphi(k)} + \varepsilon(k)$ basic Miller iterations, with $\varepsilon(k) \leq \log_2(k)$ such as optimal Ate pairing and β-Weil pairing. Pairings with Miller loop length less than $\frac{\log_2(r)}{\varphi(k)}$ are called superoptimal pairings. For example the superoptimal pairing defined by Yanfeng et *al.* in [7]. The advantage of this pairing is that the Miller loop length of the superoptimal pairing is half of that of the optimal Ate pairing thought the Miller loop involves additional exponentiations that may affect the efficiency. In this work, we provide the first application of the superoptimal pairing proposed by Yanfeng et *al.* on $BW13-P310$ and $BW19-P286$ curves. Clarisse et *al.* in [8] show that at 128-bit level of security the curves $BW13-P310$ and $BW19-P286$ are suitable for faster scalar multiplication in the first pairing group $\mathbb{G}_1$. These curves are relevant for cryptographic protocols which extensively use scalar multiplication in the first pairing group such as Enhanced Privacy ID (EPID) scheme introduced by Brickell and Li in [9] and ring signature scheme with pairings [10]. The idea is that in such protocols the main operations are done in $\mathbb{G}_1$. Hence it is more benefit to select a curve where the operations on $\mathbb{G}_1$ is less costly for instance the curves $BW13-P310$ and $BW19-P286$. The efficiency of the ring signature scheme depends on the efficiency of the pairing computation. The

pairings is computed to verify if the signature is correct or not. Tate, Weil, Ate, optimal Ate pairings have long been studied in the literature on curves with embedding degrees of the form $k = 2^i 3^j$ where $i, j \in \mathbb{N}$. On such curves, elliptic curve arithmetic is efficient for $6/k$, $4/k$ and $3/k$. Also, there are factors of the Miller function which belongs to a proper subfields of $\mathbb{F}_{p^k}$ that can be neutralized during the final exponentiation (i.e during the raising of the Miller loop output to the power $(\frac{p^k-1}{r})$, and hence are not computed. In our case, there is not a proper subfields of $\mathbb{F}_{p^{13}}$ or $\mathbb{F}_{p^{19}}$ on which some operations can be carried on. Thus it is urgent to look for a way to lower the cost of the pairings on the curves with prime odd embedding degree. Morever, there are more exponentiations in the superoptimal pairing than other pairings. Our work consists also in developing methods and techniques to reduce the exponentiations and construct algorithms for efficient evaluation of the superoptimal pairing. The bilinearity of the new x-superoptimal pairing has been verified by a Magma script available at [11].

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

- We provided the methods to reduce the inner exponents of the superoptimal pairing. Thus we have proposed a new bilinear non degenerate pairing on $BW13-P310$ and $BW19-P286$ called x-superoptimal pairing.
- In the absence of twist we use the idea of Guillevic et *al.* [12] which consists of separating numerators and denominators during the evaluation of the Miller's function so as to avoid many inversions. In addition we show how to eliminate some undesirable factors in the x-superoptimal pairing evaluation. For the faster evaluation we employed the multifunction technique to save multiplications and squarings.

Our theoretical results show that the x-superoptimal pairing can be computed efficiently than optimal Ate pairing on $BW13-P310$ and $BW19-P286$. The improvement is about 27.3% and 49% faster than the optimal ate pairing previousely computed on $BW13-P310$ and $BW19-P286$ respectively for the Miller loop. The correctness of the formulas for curves with embedding degrees 13 and 19 are ensured by a Magma script.

Roadmap. This paper is organized as follows. The Section 2 describes the ring signature scheme to illustrate required operations as far as operations in the first pairing group are concerned and the pairing evaluation as well. We also define in this sectionthe optimal pairing as well as superoptimal pairing on elliptic curves. Section 3 provides a variant of the superoptimal pairing on $BW13-P310$ and $BW19-P286$ with embedding degrees $k = 13$ and $k = 19$ respectively called x-superoptimal and describes efficient algorithms for its evaluation. Section 4 estimates the theoretical cost of the x-superoptimal pairing on $BW13-P310$ and $BW19-P286$ and compares our results with the optimal ate pairing on the same curves. Section 5 compares our results with those done on previous works. Finally, Section 6 concludes the work.

2 Preliminaries.

In this section, we describe the ring signature schemes and define the optimal pairing as well as superoptimal pairing on elliptic curves.

2.1 Ring Signature Schemes

One of the important issue solved by the ring signature schemes is the problem stated as follows: A member of the government officials wants to leak a secret to the public, however he wants to remain anonymous. On the other hand, he wants the public to be convinced that the secret is actually leaked from one of the many officers and is thus reliable. Given a security parameter $k \in \mathbb{Z}^+$, run the parameter generator on input k to generate a prime r, three groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ of order r, two generators P and Q in $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively, and an admissible pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_T$. Let $H : \{0,1\}^* \longrightarrow \mathbb{Z}_r$ be a cryptographic hash function. The security analysis will view H as a random oracle. The system parameters is $Params = \{r, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P, Q, H\}$. The ring signature proposed by Kyung-Ah Shim [13] consists of three polynomial time algorithms: key generation, ring signature and ring verification. They are deployed as follows:

- Key generation: For a user P_i, pick a random $x_i \in \mathbb{Z}_r$ and compute $PK_i = x_iP \in \mathbb{G}_1$. The user's public/secret key pair is $(PK_i; SK_i) = (x_iP, x_i)$.
- Ring signature: Let $\mathcal{U} = \{PK_1, \cdots, PK_n\}$ be the group of users' public keys. Given a private key pair x_s of P_s, and a message $M \in \{0,1\}^*$
  1. Choose $U_i \in \mathbb{G}_1$, for $i = 1, \cdots, n$ and $i \neq s$.
  2. Compute $h_i = H(U_i, M, \mathcal{U})$ for $i = 1, \cdots, n$ and $i \neq s$.
  3. Choose a random number $a \in \mathbb{Z}_r$ and compute $U_s = aP - \sum_{i \neq s}^{n} [h_iPK_i + U_i] \in \mathbb{G}_1$, $h_s = H(U_s, M, \mathcal{U}) \in \mathbb{Z}_r$, $V = (a + h_sx_s)Q \in \mathbb{G}_2$.
  4. Output the message $\sigma = (U_1, \cdots, U_n, V)$ on M for $\mathcal{U}$.
- Ring verification: Given a signature r of M for a ring $\mathcal{U} = \{PK_1, \cdots, PK_n\}$,
  1. Compute $h_i = H(U_i, M, \mathcal{U})$ for $i = 1, \cdots, n$.
  2. Verify whether $e(P, V) = e(\sum_{i=1}^{n} [h_iPK_i + U_i], Q)$ holds or not. If it holds, accept the signature, otherwise, reject it.

For n users, the ring signer needs $n + 1$ scalar multiplications and the verifier needs n scalar multiplications in $\mathbb{G}_1$ while there are also two pairings to compute for the verification step. The ring signature satisfies the following basic properties

- Correctness: A correct ring-signature must be accepted by any verifier with overwhelming probability;
- Anonymity: Any verifier should not have probability greater $1/n$ to guess the identity of the real signer, $(1/(n-1)$ for insiders);

– Unforgeability or inviolable: Any attacker must not have non-negligible probability of success in forging a valid ring signature for some message M on behalf of a ring that does not contain himself.

Ring signature with additional blindness requirement, finds its relevance in e-voting, e-cash and cryptocurrency.

2.2 Optimal 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). The following theorem gives the results about the construction of an optimal pairing.

Theorem 1 (Theorem 1 [6]) *Let $\lambda = mr$ with $r \nmid m$ and write $\lambda = \sum_{i=0}^{n} c_i p^i$ then*

$$a_{op} : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{G}_3, (Q, P) \longmapsto \left(\prod_{i=0}^{n} f_{c_i,Q}^{p^i}(P) \cdot \prod_{i=0}^{n} \frac{l_{[s_{i+1}]Q,[c_i p^i]Q}(P)}{v_{[s_i]Q}(P)} \right)^{\frac{p^k-1}{r}}$$

with $s_i = \sum_{j=i}^{n} c_j p^j$, defines a bilinear pairing. Furthermore,
if $mkp^{k-1} \not\equiv ((p^k - 1)/r) \cdot \sum_{i=1}^{n} i c_i p^{i-1} \mod r$, then the pairing is non-degenerate.

Since $r/(q^k - 1)$, then the $k-$th cyclotomic polynomial in p verifies $\phi_k(p) = 0 \mod r$, and there exists c_i's such that $c_0 r = \sum_{i=1}^{\Phi(k)-1} c_i p^i$ Such small c_i's can be obtained in general by finding short vectors in the following $\varphi(k)-$dimensional lattice (spanned by the rows)

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

The volume of L is easily seen to be r, so by Minkowski's theorem [14], there exists a short vector $(c_0, ..., c_{\varphi(k)-1})$ with $|c_i| \leq r^{1/\varphi(k)}$. The LLL algorithm applied to the rows of L gives such c_i's.

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.* [7] 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 2 (Theorem 1 [7]) *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*

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

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

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

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

By the theorem of Minkowski $|a_i| \leq r^{\frac{1}{\varphi(3k)}}$. 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. But it is important to notice that the formula in Theorem 2 involves lot of exponentiations (i.e. w^j, λ^j) and various products compared to the formula of the optimal pairing in Theorem 1.

3 Application on the Curve $BW13-P310$ and $BW19-P286$

Under this section, superoptimal pairing are defined on $BW13-P310$ and $BW19-P286$ curves as well as its variant called x-superoptimal pairing on the same curves.

3.1 $BW13-P310$ and $BW19-P286$ curves

The curve $BW13$ is an elliptic curve with embedding degree $k = 13$ and parametrized by the polynomials $p(x) = (\frac{1}{3}) * (x+1)^2(x^{26} - x^{13} + 1) - x^{27}$,

$r(x) = \Phi_{78}(x)$ and $t(x) = -x^{14} + x + 1$. For the seed $x = -2059$ recommended by [15], the corresponding elliptic curve is given as $y^2 = x^3 - 17$ and the bit length of the prime p is 310.

In other hand, the parameters of the curve $BW19$ are the embedding degree $k = 19$ and the polynomials $p(x) = \frac{1}{3}(x+1)^2(x^{38} - x^{19} + 1) - x^{39}$, $r(x) = \Phi_{114}(x)$, and $t(x) = -x^{20} + x + 1$. $p(x)$ plugging in $x = -145$ yields a p of 286 bits and the elliptic curve $BW19$ is defined by the equation $y^2 = x^3 + 31$.

Guillevic in [16] made a thorough security analysis and estimated that the cost of the DLP in the finite field $\mathbb{F}_{p^{13}}$ and $\mathbb{F}_{p^{19}}$ are 140 bits and 160 bits respectively. Hence, these curves have a security of at least 128 bits. These curves are called $BW13-P310$ and $BW19-P286$ as it was generated using the Brezing-Weng strategy [17].

3.2 Superoptimal pairing on $BW13-P310$ and $BW19-P286$ curves

The endomorphisms of elliptic curve are very important to lower the cost of the pairing. Specially when the points mapped to the endomorphism are not costly.

Lemma 1 *Let the endomorphism $\phi : (x, y) \longmapsto (\xi x, y)$ with ξ a primitive third root of unity, such that $\phi(P) = \lambda P$ in $\mathbb{G}_1$ for $\lambda \in \mathbb{Z}/r\mathbb{Z}$ then, $\lambda = \frac{t-f-2}{2f} \mod r$ where, $Df^2 = t^2 - 4p$ with $D = -3$.*

Proof Since $\phi^3 = id_E$, $\lambda^3 = 1$ in $\mathbb{Z}/r\mathbb{Z}$ then $\lambda^2 + \lambda + 1 = 0 \mod r$ for $\lambda \neq 1$. We can take

$$\lambda = \frac{\sqrt{-3} - 1}{2}. \tag{2}$$

Since $r/(p - t + 1)$ and $-3f^2 = t^2 - 4p$ then $-3f^2 \equiv t^2 - 4(t-1) \mod r$ i.e. $-3f^2 \equiv (t-2)^2 \mod r$ i.e. $\sqrt{-3} \equiv (\frac{t-2}{f}) \mod r$. By substituting this value in Equation 2 we obtain $\lambda = \frac{t-2-f}{2f} \mod r$.

In the case of $BW13-P310$, the eigenvalue $\lambda = -x^{13}$ (see [16] curve 3) and the second eigenvalue is $\mu = \lambda^2 = x^{26}$. By using the function LLL in MAGMA $V2.26-8$ calculator, we obtain a short vector of lattice M of the Theorem 2 as

$$[x, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0].$$

The construction of a_i's yields $a_0 = x$, $a_{14} = 1$ and $a_i = 0$ otherwise so, $h(\omega) = x + \omega^{14}$.

Similarly, for $BW19-P286$ curve the eigenvalues are $\lambda = -x^{19}$ and $\mu = x^{38}$. The short vector of the lattice M yields

$$[x, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0]$$

were, $a_0 = x$, $a_{20} = 1$ and $a_i = 0$ otherwise then, $h(\omega) = x + \omega^{20}$.

Corollary 1 *The superoptimal pairing on the curves BW*13−*P*310 *and BW*19−*P*286 *with* $h(\omega) = x + \omega^{14}$ *and* $h(\omega) = x + \omega^{20}$ *respectively gives*

$$a_{sup}(Q,P) = \left(f_{|x|,Q}(P) \cdot f^{\lambda}_{|x|,Q}(\phi^2(P)) \cdot f^{\mu}_{|x|,Q}(\phi(P))\right)^{-\frac{p^k-1}{r}}. \tag{3}$$

Proof For the curve $BW13 - P310$ with $h(\omega) = x + \omega^{14}$, $a_0 = x$, $a_{14} = 1$ and $a_i = 0$ otherwise. Since, $f_{1,Q} \equiv 1$,

$$\prod_{j=0}^{n}\prod_{i=0}^{2}\left[f^{\omega^j}_{a_j,Q}(\phi^{2i}(P))\right]^{\lambda^i} = \prod_{i=0}^{2}\left[f^{\omega^0}_{x,Q}(\phi^{2i}(P)) \cdot f^{\omega^{14}}_{1,Q}(\phi^{2i}(P))\right]^{\lambda^i} = \prod_{i=0}^{2}\left[f_{x,Q}(\phi^{2i}(P))\right]^{\lambda^i}.$$

For every i and $1 \le j \le 12$,

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

For every i and $j = 13$ since, $h(\omega) = 0 \mod r$ then $[x + \omega^{14}]Q = O$ and $[\omega^{14}]Q = -[x]Q$,

$$\frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} = \frac{l_{[x]Q,[\omega^{14}]Q}(\phi^{2i}(P))}{v_{[x+\omega^{14}]Q}(\phi^{2i}(P))} = \frac{l_{[x]Q,-[x]Q}(\phi^{2i}(P))}{v_{[x+\omega^{14}]Q}(\phi^{2i}(P))} \equiv v_{[x]Q}(\phi^{2i}(P)),$$

this is because $v_{[x+\omega^{14}]Q}(\phi^{2i}(P))$ will be sent to 1 during the final exponentiation.

For every i and $j = 14$,

$$\frac{l_{[h^{(j)}]Q,[a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))}{v_{[h^{(j)}+a_{j+1}\omega^{j+1}]Q}(\phi^{2i}(P))} = \frac{l_{[x+\omega^{14}]Q,[0]Q}(\phi^{2i}(P))}{v_{[x+\omega^{14}]Q}(\phi^{2i}(P))} = \frac{v_{[x+\omega^{14}]Q}(\phi^{2i}(P))}{v_{[x+\omega^{14}]Q}(\phi^{2i}(P))} = 1$$

Thus,

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

$$= \left(\prod_{i=0}^{2}\left[f_{x,Q}(\phi^{2i}(P)) \cdot v_{[x]Q}(\phi^{2i}(P))\right]^{\lambda^i}\right)^{\frac{p^k-1}{r}} \tag{5}$$

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, $\lambda^2 = \mu$, then,

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

For the curve $BW19 - P286$ with $h(\omega) = x + \omega^{20}$, in the similar manner as on the curve $BW13 - P310$ we have the Equation 3.

3.3 Lower the Cost of the Inner Exponent

Raising $\mathbb{F}_{p^k}$-elements to the power λ and μ are extremely costly. Here our purpose is to look for a technique to lower this cost.

The Lemma 2 eliminates the exponentiation by μ whereas Lemma 3 transforms the exponentiation to $x\lambda$ into $p - x$.

Lemma 2 *For any $f \in \mathbb{F}^*_{p^k}$ and $1 + \lambda + \mu = 0 \mod r$,*

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

Proof Since $r/(1+\lambda+\mu)$ then, there exists α such that $1+\lambda+\mu = \alpha r$ and for $f \in \mathbb{F}^*_{p^k}$, $f^{1+\lambda+\mu} = f^{\alpha r}$ when raise it to the power $\frac{p^k-1}{r}$ we then have $f^{(1+\lambda+\mu)\frac{p^k-1}{r}} = 1$. So, $f^{\mu \cdot \frac{p^k-1}{r}} = f^{(-1-\lambda)\cdot\frac{p^k-1}{r}}$.

Since one p-Frobenius is 12 multiplications in $\mathbb{F}_p$. Raise to the power $p - x$ is most cheaper than raise to the power $x\lambda = -x^{14}$.

Lemma 3 *For any $f \in \mathbb{F}^*_{p^k}$ and $\lambda = -x^{13}$ (for the curve $BW13 - P310$) or $\lambda = -x^{19}$ (for the curve $BW19 - P286$),*

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

Proof In the case of $BW13 - P310$, $|E(\mathbb{F}_p)| = p + 1 - t = p + 1 - (-x^{14} + x + 1) = p - x(-x^{13} + 1) = p - x\lambda - x$. Since $r/(p - x\lambda - x)$ then, there exists β such that $p - x\lambda - x = \beta r$ and for $f \in \mathbb{F}^*_{p^k}$, $f^{p-x\lambda-x} = f^{\beta r}$ when raising it to the power $\frac{p^k-1}{r}$ we then have that $f^{(p-x\lambda-x)\frac{p^k-1}{r}} = 1$. So, $f^{(x\lambda)\frac{p^k-1}{r}} = f^{(p-x)\frac{p^k-1}{r}}$.

Whereas, in the case of $BW19-P286$, $|E(\mathbb{F}_p)| = p+1-t = p+1-(-x^{20}+x+1) = p - x(-x^{19} + 1) = p - x\lambda - x$. Then the same result follows as in the first case.

We then define a new superoptimal pairing on $BW13 - P310$ and $BW19 - P286$. Note that a fixed non-degenerate power of a pairing is still a pairing.

Theorem 3 *If the $gcd(x, r) = 1$, we derive a new pairing called x-superoptimal pairing defined as*

$$a^x_{sup}(Q,P) = \left(\left(f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))\right)^{-x} \cdot \left(f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))\right)^{p}\right)^{\frac{p^k-1}{r}} \quad (6)$$

For $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. It is a non-degenerate bilinear pairing on $BW13 - P310$ and $BW19 - P286$.

Proof Let $A = f_{|x|,Q}(P)$, $B = f_{|x|,Q}(\phi^2(P))$ and $C = f_{|x|,Q}(\phi(P))$ then, $a_{sup}(Q,P) = \left(A \cdot B^{\lambda} \cdot C^{\mu}\right)^{-\frac{p^k-1}{r}}$ and from Lemma 2, $a_{sup}(Q,P) = \left(A \cdot B^{\lambda} \cdot C^{-1-\lambda}\right)^{-\frac{p^k-1}{r}} = \left(A \cdot C^{-1} \cdot (B \cdot C^{-1})^{\lambda}\right)^{-\frac{p^k-1}{r}}$ by raising to the power x and using Lemma 3, we then obtain $a^x_{sup}(Q,P) = \left((A \cdot C^{-1})^x \cdot (B \cdot C^{-1})^{p-x}\right)^{-\frac{p^k-1}{r}} = \left((A \cdot B^{-1})^{-x} \cdot (B^{-1} \cdot C)^p\right)^{\frac{p^k-1}{r}}$.

Since the inversion operation in $\mathbb{F}_{p^k}$ is too costly, it is desirable to separate numerators and denominators so as to compute only one inversion at the end when computing the Miller's function $f_{x,Q}(P)$. See Algorithm 4.

4 Cost Evaluation of the Superoptimal Pairing

Under this section, basic and special operations for the x-superoptimal pairing on $BW13-P310$ and $BW19-P286$ curves are computed.

4.1 Elliptic Curve Doubling and Elliptic Curve Addition

In Jacobian coordinates the quadruple (X, Y, Z, Z^2) represents the affine point $(X/Z^2; Y/Z^3)$. This saves inversions and multiplications. The formulas for computing the point addition and the corresponding line function in Jacobian coordinates are obtained in [12] see Algorithm 1. Also, Algorithm 2 gives the formulas for computing the point doubling and the corresponding line function, whereas Algorithm 3 provides the vertical line.

Algorithm 1: ADDING LINE [12] Given $S, Q \in \mathbb{G}_2$, compute $S+Q$ and the evaluation of the line (SQ) at $P \in \mathbb{G}_1$

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

4.2 The Miller Function

The vertical line passing through S at P is defined in affine coordinates as $V_S(P) = x_P - x_S$ and $V_S(P) = \dfrac{Z^2 \cdot x_P - X}{Z^2}$ in projective coordinates.

The function $f_{x,Q}(P)$ is evaluated using Algorithm 4.

Algorithm 2: DOUBLING LINE [12] Given $S \in \mathbb{G}_2$, compute $[2]S$ and the evaluation of the tangent at S mapped at $P \in \mathbb{G}_1$

$(X, Y, Z, Z_2) \leftarrow S$ $(x_P, y_P) \leftarrow P$; $t_1 \leftarrow Y^2$ $t_2 \leftarrow 4X \cdot t_1$ **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
  $t_3 \leftarrow 3X^2 + a \cdot Z_2^2$
$\mathbf{X} \leftarrow t_3^2 - 2t_2$
$\mathbf{Y} \leftarrow t_3 \cdot (t_2 - \mathbf{X}) - 8t_1^2$
$\mathbf{Z} \leftarrow Z \cdot 2Y$
$\lambda_d \leftarrow \mathbf{Z}.Z_2$
$t_4 \leftarrow \lambda_d \cdot y_P - 2t_2$
$\lambda_n \leftarrow t_4 - t_3 \cdot (Z_2 \cdot x_P - X)$
return $\lambda_n, \lambda_d, S = (X, Y, Z, Z^2)$

Algorithm 3: VERTICAL LINE [12] Compute the line through S and $-S$ evaluated at P.

$(X, Y, Z, Z_2) \leftarrow S$
$(x_P, y_P) \leftarrow P$
$\mu_n = Z_2 \cdot x_P - X$
$\mu_d = Z_2$
return μ_n, μ_d

Algorithm 4: MillerLoop [12]: To compute $f_{x,Q}(P)$

Input: $|x| = 2^n + \sum_{i=0}^{n-1} s_i 2^i$, where $s_i \in \{0, -1, 1\}$, $P \in E(\mathbb{F}_p)$ and $Q \in E(\mathbb{F}_{p^k})$
Output: numerator and denominator of $f_{x,Q}(P)$ and $[x]Q$

$(m_n, m_d) \leftarrow (1, 1)$; $S \leftarrow Q$
for *i from* $n - 1$ *down to* 0 **do**
  $(\lambda_n, \lambda_d) \leftarrow l_{S,S}(P)$, $S \leftarrow [2]S$ ▷ DOUBLING LINE
  $(\mu_n, \mu_d) \leftarrow v_S(P)$, ▷ VERTICAL LINE
  $(m_n, m_d) \leftarrow (m_n^2 \lambda_n \mu_d, m_d^2 \lambda_d \mu_n)$ ▷ UPDATE 1
  if $s_i = \pm 1$ **then**
    $(\lambda_n, \lambda_d) \leftarrow l_{S,[s_i]Q}(P)$, $S \leftarrow S + [s_i]Q$ ▷ ADDING LINE
    $(\mu_n, \mu_d) \leftarrow v_S(P)$, ▷ VERTICAL LINE
    $(m_n, m_d) \leftarrow (m_n \lambda_n \mu_d, m_d \lambda_d \mu_n)$ ▷ UPDATE 2
if $x < 0$ **then**
  $(m_n, m_d) \leftarrow (m_d, m_n)$
return $\frac{m_n}{m_d}$.

Remark 1 Since, $P = (x, y)$, $\phi(P) = (\xi x, y)$ and $\phi^2(P) = (\xi^2 x, y)$ the functions $f_{|x|,Q}(P)$, $f_{|x|,Q}(\phi(P))$ and $f_{|x|,Q}(\phi^2(P))$ are different only on the $x-$coordinate of P. From Algorithm 1, 2 and 3 since, λ_d and μ_d do not depend on the point P but only on the point Q then, they are identical for all Miller's functions $f_{|x|,Q}(P)$,

$f_{|x|,Q}(\phi(P))$ and $f_{|x|,Q}(\phi^2(P))$. Moreover, $(\frac{\mu_d}{\lambda_d})'s$ are factors of each Miller's functions, therefore $(\frac{\mu_d}{\lambda_d})'s$ cancel their self in the products $f_{|x|,Q}(P)\cdot f^{-1}_{|x|,Q}(\phi^2(P))$ and $f^{-1}_{|x|,Q}(\phi^2(P))\cdot f_{|x|,Q}(\phi(P))$. So, λ_d and μ_d can be removed from the evaluation of Algorithm 4 in the steps: UPDATE 1 and UPDATE 2.

Algorithm 5: Miller Loop for $x-$superoptimal pairing

Input: $|x| = 2^n + \sum_{i=0}^{n-1} s_i 2^i$, where $s_i \in \{0,-1,1\}$, $P \in E(\mathbb{F}_p)$ and $Q \in E(\mathbb{F}_{p^k})$
Output: numerator and denominator of $f_{x,Q}(P)$ and $[x]Q$

$(m_n, m_d) \leftarrow (1,1)$; $S \leftarrow Q$
for *i from* $n-1$ *down to* 0 **do**
  $(\lambda_n, \lambda_d) \leftarrow l_{S,S}(P)$, $S \leftarrow [2]S$ ▷ DOUBLE LINE
  $(\mu_n, \mu_d) \leftarrow v_S(P)$, ▷ VERTICAL LINE
  $(m_n, m_d) \leftarrow (m_n^2\lambda_n, m_d^2\mu_n)$ ▷ UPDATE 1
  if $s_i = \pm 1$ **then**
    $(\lambda_n, \lambda_d) \leftarrow l_{S,[s_i]Q}(P)$, $S \leftarrow S + [s_i]Q$ ▷ ADDITION LINE
    $(\mu_n, \mu_d) \leftarrow v_S(P)$, ▷ VERTICAL LINE
    $(m_n, m_d) \leftarrow (m_n\lambda_n, m_d\mu_n)$ ▷ UPDATE 2
if $x < 0$ **then**
  $(m_n, m_d) \leftarrow (m_d, m_n)$
return $\frac{m_n}{m_d}$.

4.3 Algorithms for Faster Evaluation of the x-superoptimal Pairing.

Algorithms 6 and 7 provide the line functions of every Miller's function used in the x-superoptimal pairing that is, $f_{|x|,Q}(P)$, $f_{|x|,Q}(\phi(P))$ and $f_{|x|,Q}(\phi^2(P))$. Whereas Algorithm 8gives the vertical line function.

Algorithm 6: 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 9 evaluates $f = f_{|x|,Q}(P)\cdot f^{-1}_{|x|,Q}(\phi^2(P))$ and $g = f^{-1}_{|x|,Q}(\phi^2(P))\cdot f_{|x|,Q}(\phi(P))$ at ones using the multifunction technique this saves squarings.

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_p, 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 7: 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
  $t_3 \leftarrow 3X^2 + a \cdot Z_2^2$
$\mathbf{X} \leftarrow t_3^2 - 2t_2$
$\mathbf{Y} \leftarrow t_3 \cdot (t_2 - \mathbf{X}) - 8t_1^2$
$\mathbf{Z} \leftarrow Z \cdot 2Y$
$\lambda_d \leftarrow \mathbf{Z}.Z_2$
$t_4 \leftarrow \lambda_d \cdot y_P - 2t_2$
$\lambda_n \leftarrow t_4 - t_3 \cdot (Z_2 \cdot x_P - X)$
$\lambda_{n1} \leftarrow t_4 - t_3 \cdot (Z_2 \cdot x_{\phi(P)} - X)$
$\lambda_{n2} \leftarrow t_4 - t_3 \cdot (Z_2 \cdot x_{\phi^2(P)} - X)$
return $S = (X, Y, Z, Z^2)\lambda_n, \lambda_{n1}, \lambda_{n2}$

Algorithm 8: 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 9: Miller Loop for faster x-superoptimal pairing.

Input: $|x| = 2^n + \sum_{i=0}^{n-1} s_i 2^i$, where $s_i \in \{0, -1, 1\}$, $P \in E(\mathbb{F}_p)$ and $Q \in E(\mathbb{F}_{p^k})$
Output: $[x]Q$, numerators and denominators of $f = f_{|x|,Q}(P) \cdot f_{|x|,Q}^{-1}(\phi^2(P))$ and $g = f_{|x|,Q}^{-1}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$.

$(n_f, d_f, n_g, d_g) \leftarrow (1, 1, 1, 1)$; $S \leftarrow Q$
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
return $f = \frac{n_f}{d_f}$ and $g = \frac{n_g}{d_g}$

Table 1 Cost estimation of each step of Algorithm 9.

Line	Cost operation
Doubling line	$7M_k + 6S_k + 4kM$
Adding line	$11M_k + 3S_k$
Vertical line	$3kM$
Update 1	$8M_k + 4S_k$
Update 2	$8M_k$

Table 1 gives the cost estimation of each step of Algorithm 9. The following formula gives the cost of the Algorithm 9.

$$\begin{aligned} C = (\log_2(x) - 1)\Big(C_{DBLINE} + C_{VerLINE}\Big) + (\log_2(x) - 2)C_{UPDATE1} \\ + (HW_{2-NAF}(x) - 1)\Big(C_{ADDLINE} + C_{VerLINE} + C_{UPDATE2}\Big). \end{aligned} \tag{7}$$

4.4 Evaluation of x-superoptimal Pairing on $BW13 - P310$

The x-superoptimal pairing on $BW13 - P310$ is given by

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

From the seed $x = -2^{11} - 2^7 - 2^5 - 2^4$, we compute $f = f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))$ and $g = f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$ by executing 10 double line, 10 update1, 3 addition line, 3 update2 and 13 vertical line steps. From [15], $M_{13} = S_{13} = 66M$ and $I_{13} = 350M + I$. Hence,

$$\begin{aligned} C &= 10[(7M_{13} + 6S_{13} + 4 \times 13M) + (3 \times 13M)] + 9[8M_{13} + 4S_{13}] \\ &\quad + 3[(11M_{13} + 3S_{13}) + (3 \times 13M) + 8M_{13}] \\ &= 21091M. \end{aligned}$$

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, 2 inversions, 1 p-Frobenius and 1 exponentiation by $-x$ in $\mathbb{F}_{p^{13}}$. For the cost of $3M_{13} + 2I_{13} + 1F_p + 1E_x = 1834M + 2I$. The total cost of the Miller loop is then $22925M + 2I$. The cost of the final exponentiation is given by Yu Dai et *al.* in [15].

4.5 Evaluation of x-superoptimal Pairing on $BW19 - P286$

The x-superoptimal pairing on $BW19 - P286$ is also given by Equation 4.4. In absence of concrete studies of operation count on $\mathbb{F}_{p^{19}}$ in the literature. We used the idea of Guillevic et *al.* [12] who estimate that, as $k = 19$ is prime, $M_k = S_k = k^{log_2 3}M \simeq 107M$. With a Karatsuba-like implementation and $F_p = (k-1)M = 18M$.

The binary representation of the loop parameter x is $\{-1,0,0,-1,0,0,0,-1\}$. we compute $f = f_{|x|,Q}(P) \cdot f^{-1}_{|x|,Q}(\phi^2(P))$ and $g = f^{-1}_{|x|,Q}(\phi^2(P)) \cdot f_{|x|,Q}(\phi(P))$ by executing 6 double line, 5 update1, 2 addition line, 2 update2 and 8 vertical line steps. Hence, $C = 20386M$.

The last step of the Miller loop costs $3M_{19} + 2I_{19} + 1F_p + 1E_{-x} = 1302M + 2I_{19}$.

The total cost of the Miller loop is then $21688M + 2I_{19}$.

4.6 Evaluation of Superoptimal Pairing on $BW13-P310$ and $BW19-P286$

The superoptimal pairing on $BW13-P310$ and $BW19-P286$ is defined as

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

On $BW13-P310$, using Algorithm 4 the cost evaluation of each of the three Miller's functions $f = f_{|x|,Q}(P)$, $g = f^{\lambda}_{|x|,Q}(\phi^2(P))$ and $h = f^{\mu}_{|x|,Q}(\phi(P))$ is

$$\begin{aligned} C &= 10[(5M_{13} + 6S_{13} + 13M) + (13M)] + 9[4M_{13} + 2S_{13}] \\ &\quad + 3[(10M_{13} + 3S_{13}) + (13M) + 4M_{13}] \\ &= 14489M. \end{aligned}$$

The last step consists to evaluate $(d_f \cdot n_f^{-1}) \cdot (d_g \cdot n_g^{-1} \cdot (d_h \cdot n_h^{-1})^{\lambda})^{\lambda}$ for a cost of $5M_{13} + 3I_{13} + 26E_{-x} = 25404M + 3I$. Where $\lambda = -x^{13}$. Therefore the Miller Loop cost $3 \times 14489 + (25404M + 3I) = 68871M + 3I$.

Similarly, on $BW19-P286$ $C = 14176M$ and the last step cost $37129M + 3I_{19}$. For a total of $79657M + 3I_{19}$.

5 Comparison

Table 2 compares the theoretical costs of the optimal Ate pairing, the superoptimal pairing and the proposed superoptimal pairing. According to this table optimal pairing is at least twice faster that superoptimal pairing on BW-13 and BW-19 curves. However, the variant of the superoptimal pairing called x-superoptimal pairing is about 15.3% and 39.8% faster than the optimal ate pairing on $BW13-P310$ and $BW19-P286$ respectively. The overall improvement (Miller loop and final exponentiation) is about 7% over the other pairing.

6 Conclusion

We found a new pairing faster than optimal ate pairing on $BW13-P310$ and $BW19-P286$ called x-superoptimal pairing which is a power of the superoptimal pairing. Those curves are relevant for cryptographic protocols which extensively use scalar multiplication in the first pairing group such as ring signature scheme. The x-superoptimal pairing is about 15.3% and 39.8% faster

Table 2 Comparison. The cost of the final exponentiation and the Miller loop for the optimal Ate pairing are found in [15] for the curve $BW13-P310$. Whereas for the curve $BW19-P286$ we refer to [8] for these costs.

Curve	Pairing	Miller loop	Final exponentiation	Total cost
$BW13-P310$	optimal Ate [15]	$27074M + 2I$	$28058M + I$	$55132M + 3I$
	superoptimal	$68871M + 3I$		$96929M + 4I$
	x-superoptimal	$22925M + 2I$		$50925M + 3I$
$BW19-P286$	Optimal Ate [8]	$35991M + 2I_{19}$	$160824M + 13I_{19}$	$196815M + 15I_{19}$
	superoptimal	$79657M + 3I_{19}$		$240481M + 16I_{19}$
	x-superoptimal	$21688M + 2I_{19}$		$182512M + 15I_{19}$

than the optimal ate pairing on $BW13-P310$ and $BW19-P286$ respectively. The bilinearity of the new x-superoptimal pairing has been verified by a Magma script available at [11].

References

1. D. Boneh, C. Gentry, B. Lynn, and H. Shacham. Aggregate and verifiably encrypted signatures from bilinear maps. In *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, pages 416–432, 2003.
2. D. Boneh and M.K. Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, pages 213–229, 2001.
3. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil pairing. *J. Cryptol.*, 17(4):297–319, 2004.
4. G. Zanon, M.A. Simplício Jr., G. C. C. F. Pereira, J. Doliskani, and P. S. L. M. Barreto. Faster key compression for isogeny-based cryptosystems. *IEEE Trans. Computers*, 68(5):688–701, 2019.
5. L. D. Feo, S. Masson, C. Petit, and A. Sanso. Verifiable delay functions from supersingular isogenies and pairings. In Steven D. Galbraith and Shiho Moriai, editors, *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, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 248–277. Springer, 2019.
6. F. Vercauteren. Optimal pairings. *IEEE Trans. Inf. Theory*, 56(1):455–461, 2010.
7. Q. Y. Feng, T. C. Ming, G. Baoan, and X. M. Zhi. Super-optimal pairings. In *Mechanical Engineering, Materials and Energy II*, volume 281 of *Applied Mechanics and Materials*, pages 127–133. Trans Tech Publications Ltd, 3 2013.
8. R. Clarisse, S. Duquesne, and O. Sanders. Curves with fast computations in the first pairing group. In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, *Cryptology and Network Security - 19th International Conference, CANS 2020, Vienna, Austria, December 14-16, 2020, Proceedings*, volume 12579 of *Lecture Notes in Computer Science*, pages 280–298. Springer, 2020.
9. E. Brickell and J. Li. Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities. *IEEE Trans. Dependable Secur. Comput.*, 9(3):345–360, 2012.
10. R. L. Rivest, A.Shamir, and Y. Tauman. How to leak a secret. In Colin Boyd, editor, *Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, Proceedings*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.
11. Azebaze Guimagang Laurian, Emmanuel Fouotsa, and Raoul Ayissi. Magma code for the verification of various algorithms/ formulas and bilinearity of pairings. In *http://www.emmanuelfouotsa-prmais.org/Portals/22/codeXsuperopt.txt*, 2022.
12. A. Guillevic, S. Masson, and E. Thomé. Cocks-pinch curves of embedding degrees five to eight and optimal ate pairing computation. *Des. Codes Cryptogr.*, 88(6):1047–1081, 2020.

13. Kyung-Ah Shim. An efficient ring signature scheme from pairings. *Inf. Sci.*, 300:63–69, 2015.
14. H. Minkowski. *Geometrie der Zahlen*, volume Druck und Verlag von B.G. Teubner. Leipzig und Berlin, 1910.
15. Y. Dai, Z. Zhou, F. Zhang, and C. Zhao. Software implementation of optimal pairings on elliptic curves with odd prime embedding degrees. *IACR Cryptol. ePrint Arch.*, page 1162, 2021.
16. A. Guillevic. A short-list of pairing-friendly curves resistant to special TNFS at the 128-bit security level. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part II*, volume 12111 of *Lecture Notes in Computer Science*, pages 535–564. Springer, 2020.
17. F. Brezing and A. Weng. Elliptic curves suitable for pairing based cryptography. *Des. Codes Cryptogr.*, 37(1):133–141, 2005.