Afrika Matematika (2019) 30:371–388
https://doi.org/10.1007/s13370-019-00653-8

Beta Weil pairing revisited

Emmanuel Fouotsa[1] · Aminatou Pecha[2] · Nadia El Mrabet[3]

Received: 24 May 2017 / Accepted: 7 January 2019 / Published online: 16 January 2019

Abstract
In this paper, we extend the β-Weil pairing, initially introduced in the setting of ordinary elliptic curves with even embedding degree by Aranha et al. [2], to ordinary elliptic curves of any embedding degree. We also propose a new optimal pairing which is the product of some rational functions with the same Miller loop and having a simple final exponentiation. The new pairing is appropriated for using the multi-pairing technique for an efficient implementation. We focus our computation at high security level. Exploiting the fact that the β-Weil pairing is suitable for parallel execution, we first show that calculating the extended β-Weil pairing over pairing-friendly elliptic curves with embedding degree 27 is more efficient than calculating the optimal ate pairing. Finally we show that calculating our new pairing over Barreto–Lynn–Scott curves with embedding degree 12 (BLS12) and pairing-friendly elliptic curves with embedding degree 15 is more efficient than calculating the optimal ate pairing.

Keywords Optimal pairings · β-Weil pairing · Miller's algorithm · Multi-pairing technique · Pairing computation

Mathematics Subject Classification 14H52 · 1990S

The first and second authors acknowledge support from The Simons Foundations through Pole of Research in Mathematics with applications to Information Security, Sub-Saharan Africa.

✉ Nadia El Mrabet
nadia.el-mrabet@emse.fr

Emmanuel Fouotsa
emmanuelfouotsa@yahoo.fr

Aminatou Pecha
aminap2001@yahoo.fr

[1] Higher Teacher Training College, University of Bamenda, P.O Box 39, Bambili, Bamenda, Cameroon

[2] National Advanced School of Engineering, University of Maroua, P.O. Box 46, Maroua, Cameroon

[3] Mines Saint-Etienne, CEA-Tech, Centre CMP, Departement SAS, F-13541 Gardanne, France

1 Introduction

Nowadays, one can enumerate many cryptographic protocols which are based on pairings such as: Joux's one round three party key agreement protocol [20], the Identity-Based Cryptosystem [9], Identity-Based Encryption [12], the Identity-Based undeniable signature [22], short signatures [10] or Broadcast encryption [16]. A pairing is a non-degenerate bilinear map of the form $b : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_3$ i.e. b is linear in each component and for each $P \in \mathbb{G}_1$ there exists $Q \in \mathbb{G}_2$ such that $b(P, Q) \neq 1$, where we consider $\mathbb{G}_1, \mathbb{G}_2$ to be additive groups and $\mathbb{G}_3$ a multiplicative group. The first pairings used in cryptography were the Weil [24] and Tate pairings. The majority of papers proposed in the literature concentrates on improving efficiency of the computation of Tate-type pairings because Tate pairing and its variants offer more effectiveness than the Weil pairing [7,14,21,29,32]. Recently, Aranha et al. [2] introduced an optimal pairing in the form of Weil-type pairing which is appropriate for parallel execution and called the β-Weil pairing. Let E be an ordinary elliptic curve over $\mathbb{F}_p$ where $\mathbb{F}_p$ is a prime field, p an odd prime. Let r be a large prime divisor of $\sharp E(\mathbb{F}_p)$, the order of the group of rational points of the elliptic curve E. Let k be the embedding degree i.e. the smallest positive integer such that r divides $p^k - 1$. The definition of β-Weil pairing proposed by Aranha et al. focusses only on ordinary elliptic curves with even embedding degree. On the other hand, one notes that in many cryptographic protocols, the evaluation of the products of s pairings (s an integer ≥ 1) is required instead of the evaluation of single pairing [1,8,11,30]. For efficient implementation of these products of pairing, separately Scott [28] and Granger et al. [18] proposed an efficient method for their computation, and some curves are suitable for its computation [15]. This method is usually named multi-pairing technique which only requires a single squaring in the extension field per doubling instead of s squarings in the naive way. Also, the multi-pairing technique can be used to calculate a single pairing defined as the products of some rational functions with the same Miller loop.
The few works that applied the multi-pairing technique to calculate a single pairing are those of Sakemi et al. [26] and Zhang et al. [32]. Sakemi et al. applied the multi-pairing technique to improve the computation of the twisted ate pairing on the Barreto–Naehrig curves. On the other hand, Zhang et al. suggested a new pairing and pairing lattices on pairing-friendly curves defined over an extension field when assuming their existence, on which the multi-pairing technique is adequate for acquiring efficient implementation.

In this work, we show that when we consider any proper divisor of the embedding degree k, the β-Weil pairing can be extended to the ordinary elliptic curves with any embedding degree. Also, we show that calculating the β-Weil pairing over pairing-friendly elliptic curves with embedding degree 27 is more efficient than calculating the optimal ate pairing. We also propose a new optimal pairing which is defined as the product of some rational functions with the same Miller loop. The computation of this new pairing requires a simple final exponentiation. We then show that calculating the proposed pairing over BLS12 and pairing-friendly elliptic curves with embedding degree 15 is more efficient than calculating the optimal ate pairing. Note that we compare the different pairings computed in this work by the number of elementary operations.

The rest of this paper is organized as follows: Sect. 2 recalls the mathematical background on pairings over elliptic curves. In Sect. 3, we first recall the definition of β-Weil pairing proposed by Aranha et al. then we show how to extend the β-Weil pairing on ordinary elliptic curves with any embedding degree, we compute the β-Weil pairing on pairing-friendly elliptic curves with embedding degree 27 and compare its cost versus the optimal ate pairing cost on the same curve. In Sect. 4, we propose a new optimal pairing on ordinary elliptic curves

of embedding degree 12 (BLS12) and pairing-friendly curves with embedding degree 15. In particular we show that calculating the proposed pairing over Barreto–Lynn–Scott curves with embedding degree 12 (BLS12) and pairing-friendly elliptic curves with embedding degree 15 is more efficient than calculating the optimal ate pairing.

2 Mathematical background

In this section, we recall the definition of the reduced Tate pairing, the Weil pairing, an optimal pairing, the optimal ate pairing and the β-Weil pairing which has been introduced by Aranha et al. [2] and defined only on curves with even embedding degree.

2.1 Definitions and notations

Let E be an ordinary elliptic curve over $\mathbb{F}_p$ and $\mathcal{O}$ be the neutral element of the group of rational points of E, l a proper divisor of k, t the trace of Frobenius and $\rho = \log p/\log r$. Denote by μ_r the group of rth roots of unity in $\mathbb{F}_{p^k}^{\times}$. For $m \in \mathbb{Z}$, the multiplication by m is denoted by $[m]$ and defined as $[m] : E \to E : S \mapsto mS$. Denote by $E[r]$ the set of r-torsion points on E i.e. the set of the points $S \in E$ such that $rS = \mathcal{O}$.

Let π_p be the Frobenius endomorphism, $\pi_p : E \to E : (x, y) \mapsto (x^p, y^p)$. Set $\mathbb{G}_1 = E[r] \cap Ker(\pi_p - [1])$, $\mathbb{G}_2 = E[r] \cap Ker(\pi_p - [p])$, let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. Denote by $E^{(p^i)}$ the curve defined by raising the coefficients of the equation of E to the p^i-power for some i. Let π_{p^i} be the p^i-power Frobenius isogeny from E to $E^{(p^i)}$. By isogeny, we mean that π_{p^i} is a morphism satisfying $\pi_{p^i}(\mathcal{O}) = \mathcal{O}$, its dual is denoted $\hat{\pi}_{p^i}$ and $\pi^*_{p^i}$ is the pullback of π_{p^i}. Let E' over $\mathbb{F}_p$ be a twist of degree d of E i.e. E' is an elliptic curve defined over $\mathbb{F}_p$ which is isomorphic to E over an algebraic closure of $\mathbb{F}_p$ and d is the smallest integer such that E and E' are isomorphic over $\mathbb{F}_{p^d}$. Let $n = gcd(k, d)$ and $e = k/n$. For each $a \in \mathbb{Z}$ and $S \in E[r]$, let $f_{a,S}$ be the normalized $\mathbb{F}_{p^k}$-rational function with divisor $div(f_{a,S}) = a(S) - ([a]S) - (a-1)(\mathcal{O})$. Let $h(z) = \sum_{i=0}^{c} h_i z^i \in \mathbb{Z}[z]$ an optimal polynomial obtained by using a lattice-based method such that $h(p) \equiv 0 (mod\ \ r)$. Denote by $f_{a,h,S}$ the extended Miller function to be the normalized rational function with divisor $\sum_{i=0}^{c} h_i((a^i S) - (\mathcal{O}))$.
Denote $s_\lambda = p^\lambda \ \ (mod\ \ r)$, where $1 \leq \lambda \leq k-1$.

Define $\theta_{s_\lambda} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left(\frac{f_{s_\lambda,P}(Q)}{f_{s_\lambda,Q}(P)}\right)^{p^l-1}$ and

$\theta_{s_\lambda,h} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left(\frac{f_{s_\lambda,h,P}(Q)}{f_{s_\lambda,h,Q}(P)}\right)^{p^l-1}$.

In this paper, we assume that all elliptic curves are pairing-friendly elliptic curves defined by a parameterized family $(p(x), r(x), t(x))$ [13] where $x \in \mathbb{Z}$.

And we consider the following notations:

M_k, S_k, I_k : Cost of multiplication, squaring and inversion in the field $\mathbb{F}_{p^k}$, for any integer k.

Definition 1 The reduced tate pairing

The reduced Tate pairing [5] t_r is a non-degenerate bilinear map defined as

$$t_r : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto f_{r,P}(Q)^{\frac{p^k-1}{r}}$$

Definition 2 The Weil pairing

Let $R, S \in E[r]$ and $R \neq S$. Let $f_{r,R}$ and $f_{r,S}$ two rational functions on E such that $div(f_{r,R}) = r(R) - r(\mathcal{O})$ and $div(f_{r,S}) = r(S) - r(\mathcal{O})$. The Weil pairing [24] is a non-degenerate bilinear map defined as

$$e_w : E[r] \times E[r] \longrightarrow \mu_r \quad (R, S) \mapsto (-1)^r \frac{f_{r,R}(S)}{f_{r,S}(R)}.$$

Definition 3 The optimal pairing

Let $b : \mathbb{G}_1 \times \mathbb{G}_2 \longrightarrow \mathbb{G}_3$ be a non degenerate, bilinear pairing with $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_3$ subgroups of order r where $\mathbb{G}_3 \subset \mathbb{F}_{p^k}^{\times}$, then $b(.,.)$ is an optimal pairing [29] if it can be computed approximately in $log_2 r/\varphi(k) + \epsilon(k)$ basic Miller iterations, with $\epsilon(k) \leq log_2 k$.

The following theorem from [29] explains the construction of an optimal ate pairing.

Theorem 1 ([29],Theorem 1)

Let $\lambda = mr$ be a multiple of r such that $r \nmid m$ and write $\lambda = \sum_{i=0}^{l} c_i p^i = h(p)$, $(h(z) \in \mathbb{Z}[z])$. For $i = 0, \cdots l$ set $s_i = \sum_{j=i}^{l} c_j p^j$; then

$$\begin{aligned} b_o : \mathbb{G}_2 \times \mathbb{G}_1 &\rightarrow \mu_r \\ (Q, P) &\longmapsto \left(\prod_{i=0}^{l} f_{c_i,Q}^{p^i}(P) \cdot \prod_{i=0}^{l-1} h_{[s_{i+1}]Q,[c_i p^i]Q}(P) \right)^{\frac{p^k-1}{r}} \end{aligned} \tag{1}$$

defines a bilinear pairing which is non degenerate if $mkp^{k-1} \neq ((p^k - 1)/r) \cdot \sum_{i=0}^{l} i c_i p^{i-1} \bmod r$.

Note that the coefficients c_i, with $i \in \{0, \ldots, l\}$, can be obtained from the short vector obtained from the lattice

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

Therefore, an optimal polynomial $h(z)$ can be obtained such that $|c_i| \leq r^{1/\varphi(k)}$ by applying a lattice-based method.

The following theorem from [2] gives the definition of the β-Weil pairing. Note that the β-Weil pairing is a variant of the Weil pairing which is suitable for parallel execution and the domain of the pairing is $\mathbb{G}_1 \times \mathbb{G}_2$.

Theorem 2 ([2], Theorem 3)

There exists $h = \sum_{i=0}^{c} h_i z^i \in \mathbb{Z}[z]$ such that $|h_i| \leq r^{1/\varphi(k)}$ and

$$\beta : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \prod_{i=0}^{e-1} \left(\frac{f_{s_\lambda,h,[p^i]P}(Q)}{f_{s_\lambda,h,Q}([p^i]P)} \right)^{(p^{k/2}-1)p^{e-1-i}}$$

is a pairing.

3 Extended β-Weil pairing

In order to extend the β-Weil pairing to curves with any embedding degree; we now show that when we consider any proper divisor of k, it is possible to define the β-Weil pairing to curves with any embedding degree. For, we first recall some useful results.

Lemma 1 *Let $R \in E$ and let u, v, w, s be integers. Then we have:*

1. $f_{uv,R} = f^u_{v,R} \cdot f_{u,[v]R} = f^v_{u,R} \cdot f_{v,[u]R}$
2. $f_{u,[v][w]R} = f_{u,[v]([w]R)}$
3. *In particular, if $R \in E[r]$ then $f^s_{r,R} = f_{sr,R}$*

Proof 1. We have that $div(f_{uv,R}) = uv(R) - ([uv]R) - (uv-1)(\mathcal{O})$, $div(f^u_{v,R}) = udiv(f_{v,R}) = uv(R) - u([v]R) - u(v-1)(\mathcal{O})$ and $div(f_{u,[v]R}) = u([v]R) - ([u][v]R) - (u-1)(\mathcal{O})$. Since $div(f^u_{v,R} f_{u,[v]R}) = div(f^u_{v,R}) + div(f_{u,[v]R})$ and $[uv] = [u][v]$, it follows that $div(f_{uv,R}) = div(f^u_{v,R} f_{u,[v]R})$; Hence $f_{uv,R} = f^u_{v,R} f_{u,[v]R}$.
2. This equality holds because $[v][w]R = [v]([w]R)$.
3. Assume that $R \in E[r]$ i.e. $rR = \mathcal{O}$, according to the property (1) above, we have that $f_{sr,R} = f^s_{r,R} \cdot f_{s,[r]R} = f^s_{r,R}$ since $f_{s,[r]R} = f_{s,\mathcal{O}} = 1$.

□

Corollary 1 ([34], Theorem 1) *Let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, the following map*

$$\tilde{b} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left(\frac{f_{p^e,P}(Q)}{f_{p^e,Q}(P)} \right)^{p^l - 1} \text{ is a pairing.}$$

Lemma 2 ([17], Lemma 6) *Let $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$ then if $lc_\infty(f_{p,Q}) = 1$ with respect to any $\mathbb{F}_p$-rational uniformizer u_∞ at $\mathcal{O}$ then $f_{p,Q}(P)$ is a pairing where the leading coefficient of $f_{p,Q}$ at $\mathcal{O}$ is denoted by $lc_\infty(f_{p,Q})$.*

Theorem 3 ([33], Theorem 1) *Let $\mathbb{G}_1$, $\mathbb{G}_2$ and μ_r be defined as above. Let I be a pairing from $\mathbb{G}_1 \times \mathbb{G}_2$ to μ_r satisfying $I(P, Q) = 1_{\mu_r}$ where $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$ and 1_{μ_r} is the identity in μ_r. Then the set of all pairings from $\mathbb{G}_1 \times \mathbb{G}_2$ to μ_r is a multiplicative group with identity I.*

Lemma 3 *For $1 \le \lambda \le k-1$, the map $\mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left(\prod_{i=0}^{e-1} \left(\frac{f_{s_\lambda,[p^i]P}(Q)}{f_{s_\lambda,[p^i]Q}(P)} \right)^{p^{e-1-i}} \right)^{p^l-1}$ is a pairing and the following identity holds: $\left(\prod_{i=0}^{e-1} \left(\frac{f_{s_\lambda,[p^i]P}(Q)}{f_{s_\lambda,[p^i]Q}(P)} \right)^{p^{e-1-i}} \right)^{p^l-1} = \prod_{i=0}^{e-1} \theta_{s_\lambda}([p^i]P, Q)^{p^{e-1-i}}$.*

Proof According to the results in Corollary 1, the map $(P, Q) \mapsto \left(\frac{f_{p^e,P}(Q)}{f_{p^e,Q}(P)} \right)^{p^l-1}$ is a pairing. Using the fact that $f_{ab,R} = f^a_{b,R} f_{a,bR}$ from Lemma 1 with a, b integers and $R \in E$, we have that

$$f_{p^e,P} = \prod_{i=0}^{e-1} \left(f_{p,[p^i P]} \right)^{p^{e-1-i}}.$$

Since $s_\lambda = p^\lambda \pmod r$ and $f_{p^\lambda,P} = \prod_{j=0}^{\lambda-1} \left(f_{p,[p^j]P}\right)^{p^{\lambda-1-j}}$, we have that:

$$\prod_{i=0}^{e-1} \left(f_{p^\lambda,[p^i]P}\right)^{p^{e-1-i}} = \prod_{i=0}^{e-1} \left(\prod_{j=0}^{\lambda-1} (f_{p,[p^i][p^j]P})^{p^{\lambda-1-j}} \right)^{p^{e-1-i}}$$
$$= \prod_{i=0}^{e-1} \left(\prod_{j=0}^{\lambda-1} (f_{p,[p^i][p^j]P})^{p^{\lambda-1-j} p^{e-1-i}} \right).$$

Set $a_{ij} = (f_{p,[p^i][p^j]P})^{p^{\lambda-1-j} p^{e-1-i}}$

$$\text{So, } \prod_{i=0}^{e-1} \left(f_{p^\lambda,[p^i]P}\right)^{p^{e-1-i}} = \prod_{i=0}^{e-1} \left(\prod_{j=0}^{\lambda-1} a_{ij} \right)$$
$$= \prod_{j=0}^{\lambda-1} \left(\prod_{i=0}^{e-1} a_{ij} \right)$$
$$= \prod_{j=0}^{\lambda-1} \left(\prod_{i=0}^{e-1} (f_{p,[p^i]([p^j]P)})^{p^{e-1-i}} \right)^{p^{\lambda-1-j}}$$
$$= \prod_{j=0}^{\lambda-1} (f_{p^e,[p^j]P})^{p^{\lambda-1-j}}.$$

Hence,

$$\prod_{i=0}^{e-1} \left(f_{p^\lambda,[p^i]P}\right)^{p^{e-1-i}} = \prod_{j=0}^{\lambda-1} \left(f_{p^e,[p^j]P}\right)^{p^{\lambda-1-j}} \tag{3}$$

It follows from (3) that

$$\left(\prod_{i=0}^{e-1} \left(\frac{f_{p^\lambda,[p^i]P}(Q)}{f_{p^\lambda,[p^i]Q}(P)} \right)^{p^{e-1-i}} \right)^{p^l-1} = \left(\prod_{j=0}^{\lambda-1} \left(\frac{f_{p^e,[p^j]P}(Q)}{f_{p^e,[p^j]Q}(P)} \right)^{p^{\lambda-1-j}} \right)^{p^l-1} \tag{4}$$

and

$$\left(\prod_{j=0}^{\lambda-1} \left(\frac{f_{p^e,[p^j]P}(Q)}{f_{p^e,[p^j]Q}(P)} \right)^{p^{\lambda-1-j}} \right)^{p^l-1} = \left(\prod_{j=0}^{\lambda-1} \left(\frac{f_{p^e,[p^j]P}(Q)}{f_{p^e,Q}([p^j]P)} \right)^{p^{\lambda-1-j}} \right)^{p^l-1} \tag{5}$$

the equality of (5) holds because $f_{p^e,[p^j]Q}(P) = f_{p^e,Q}([p^j]P)$ since the map $(P, Q) \mapsto f_{p^e,Q}(P)$ is a pairing by the Lemma 2.

Thus $\left(\prod_{i=0}^{e-1} \left(\frac{f_{p^\lambda,[p^i]P}(Q)}{f_{p^\lambda,[p^i]Q}(P)} \right)^{p^{e-1-i}} \right)^{p^l-1}$ is a product of pairings since the map $(P, Q) \mapsto \left(\frac{f_{p^e,P}(Q)}{f_{p^e,Q}(P)} \right)^{p^l-1}$ is a pairing. So the first part of lemma holds by Theorem 3. Furthermore, since the map $(P, Q) \mapsto f_{p^\lambda,Q}(P)$ is a pairing by the Lemma 2, we have that:

$$\left(\prod_{i=0}^{e-1}\left(\frac{f_{p^\lambda,[p^i]P}(Q)}{f_{p^\lambda,[p^i]Q}(P)}\right)^{p^{e-1-i}}\right)^{p^l-1} = \left(\prod_{i=0}^{e-1}\left(\frac{f_{p^\lambda,[p^i]P}(Q)}{f_{p^\lambda,Q}([p^i]P)}\right)^{p^{e-1-i}}\right)^{p^l-1} \text{ and}$$

$$\left(\prod_{i=0}^{e-1}\left(\frac{f_{p^\lambda,[p^i]P}(Q)}{f_{p^\lambda,Q}([p^i]P)}\right)^{p^{e-1-i}}\right)^{p^l-1} = \prod_{i=0}^{e-1}\theta_{p^\lambda}([p^i]P, Q)^{p^{e-1-i}}. \quad \square$$

The main result of this section is summarized in the following theorem.

Theorem 4 (Extended β-Weil Pairing) *There exists a polynomial h such that $|h_i| \leq r^{1/\varphi(k)}$ and the map $\beta_k : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \prod_{i=0}^{e-1}\theta_{p,h}([p^i]P, Q)^{p^{e-1-i}}$ is a pairing. More precisely, If $r \nmid sp^{e-1-i}$ and $r \nmid h_j$, for all $0 \leq i \leq e-1$ and $0 \leq j \leq n$, then the map β_k is non-degenerate.*

Proof Let $h(z) = \sum_{i=0}^{n} h_i z^i$ an optimal polynomial such that $h(p) = rs$. Since $f_{r,P}^s = f_{p,h,P}.\prod_{j=0}^{n} f_{p^j,P}^{h_j}$, we have that

$$\left(\frac{f_{r,P}(Q)}{f_{r,Q}(P)}\right)^s = \frac{f_{r,h,P}(Q)}{f_{r,h,Q}(P)}.\prod_{j=0}^{n}\left(\frac{f_{p^j,P}(Q)}{f_{p^j,Q}(P)}\right)^{h_j}$$

$$\text{i.e. } \left(\frac{f_{r,P}(Q)}{f_{r,Q}(P)}\right)^{s(p^l-1)} = \left(\frac{f_{r,h,P}(Q)}{f_{r,h,Q}(P)}\right)^{p^l-1}.\left(\prod_{j=0}^{n}\left(\frac{f_{p^j,P}(Q)}{f_{p^j,Q}(P)}\right)^{h_j}\right)^{p^l-1}$$

$$\text{i.e. } \theta_r(P, Q)^s = \theta_{p,h}(P, Q).\prod_{j=0}^{n}\theta_{p^j}(P, Q)^{h_j}.\text{Thus}$$

$$\beta_k(P, Q) = \prod_{i=0}^{e-1}\theta_{p,h}([p^i]P, Q)^{p^{e-1-i}} \text{ and}$$

$$\prod_{i=0}^{e-1}\theta_{p,h}([p^i]P, Q)^{p^{e-1-i}} = \prod_{i=0}^{e-1}\left(\theta_r([p^i]P, Q)^s.\prod_{j=0}^{n}\theta_{p^j}([p^i]P, Q)^{-h_j}\right)^{p^{e-1-i}}$$

$$\text{i.e. } \beta_k(P, Q) = \prod_{i=0}^{e-1}\theta_r([p^i]P, Q)^{sp^{e-1-i}}.\prod_{j=0}^{n}\left(\prod_{i=0}^{e-1}\theta_{p^j}([p^i])P, Q)^{p^{e-1-i}}\right)^{-h_j}.$$

Hence the map β_k is a product of pairings by Lemma 3 ; so β_k is a pairing by Theorem 3. On the other hand, β_k is non-degenerate if $r \nmid sp^{e-1-i}$ and $r \nmid h_j$, for all $0 \leq i \leq e-1$ and $0 \leq j \leq n$ since the map $\theta_r([p^i]P, Q)$ is a fixed power of the Weil pairing and $\prod_{i=0}^{e-1}\theta_{p^j}([p^i])P, Q)^{p^{e-1-i}}$ is a pairing according to Lemma 3. $\square$

Remark 1 In this remark, we establish that the application of Theorem 4 on elliptic curves with even embedding degree coincides to the definition of β-Weil proposed by Aranha et al. in [2]. We choose the Barreto–Lynn–Scott curves with embedding degree 24 (BLS 24) [6] for this verification. This family of elliptic curves is defined in $\mathbb{F}_p$ by the following polynomials:

$$\begin{aligned} p(x) &= (x-1)^2(x^8 - x^4 + 1)/3 + x \\ r(x) &= x^8 - x^4 + 1 \\ t(x) &= x + 1 \end{aligned} \tag{6}$$

and has ρ-value 1.25 and a twist order 6. According to Table 3 in [2], the optimal function $h(z) = x - z \in \mathbb{Z}[z]$. Since $k = 24$, we have $e = k/gcd(k, d) = 4$. We can take $l = 12$ since 12 is a proper divisor of k. Applying the Theorem 4, we obtain the following result: The β-pairing over the pairing-friendly curves with $k = 24$, denote by β_{24}, is bilinear and non degenerate map:

$$\beta_{24} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left[\prod_{i=0}^{3}\left(\frac{f_{x,[p^i]P}(Q)}{f_{x,Q}([p^i]P)}\right)^{p^{3-i}}\right]^{(p^{12}-1)}$$

Furthermore, since $r \nmid p^4+1$, then $\beta_{24}(P, Q)^{p^4+1} = \left[\prod_{i=0}^{3}\left(\frac{f_{x,[p^i]P}(Q)}{f_{x,Q}([p^i]P)}\right)^{p^{3-i}}\right]^{(p^{12}-1)(p^4+1)}$ is also a pairing. And $\beta_{24}(P, Q)^{p^4+1}$ is the β-Weil pairing defined on BLS24-curves by Aranha et al. in [2].

3.1 The extended β-Weil pairing on pairing-friendly curves with $k = 27$

The parameterized elliptic curves with embedding degree 27 is defined in [6]. This family has ρ-value 10/9 and is parameterized by the following polynomials:

$$\begin{aligned} p(x) &= (x-1)^2(x^{18} + x^9 + 1)/3 + x \\ r(x) &= (x^{18} + x^9 + 1)/3 \\ t(x) &= x + 1 \end{aligned} \tag{7}$$

Zhang and Lin [31] found the optimal function $h(z) = \sum_{i=0}^{17} c_i z^i = x - z \in \mathbb{Z}[z]$ such that $h(p) \equiv 0 \pmod r$ for elliptic curves with $k = 27$. We then have $f_{p,h,R} = f_{p,x-p,R} = f_{x,R}$ with $R \in E[r]$. Note that this family of elliptic curves has a cubic twist, i.e., $d = 3$. Since $k = 27$, we have $e = k/gcd(k, d) = 9$. We can take $l = 3$ since 3 is a proper divisor of k. Applying the Theorem 4, we obtain the following result:

Proposition 1 *The Extended β-Weil pairing over the pairing-friendly curves with $k = 27$ is the bilinear and non degenerate map:*

$$\beta_{27} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left[\prod_{i=0}^{8}\left(\frac{f_{x,[p^i]P}(Q)}{f_{x,Q}([p^i]P)}\right)^{p^{8-i}}\right]^{(p^3-1)}$$

According to the previous work in [25] on elliptic curves with $k = 27$ at the 192-bit security level, Fouotsa et al. found the value $x = 2^{25} + 2^{14} + 2^{17} + 2^4 + 1$ so that r has a prime factor of 410 bits length and the prime p has a bit length of 511. Recall that $f_{x,P}(Q)$ and $f_{x,Q}(P)$ are called Miller lite and full Miller respectively. The computation of the Miller lite $f_{x,P}(Q)$ and full Miller $f_{x,Q}(P)$ are done by execution of Miller's Algorithm. In this case, for $k = 27$, we compute the Miller function in affine coordinates, since the affine formulas provide a fast pairing computation [31].

In Algorithm 1, $l_{R,S}$ is the straight line containing R and S and v_{R+S} is the corresponding vertical line passing through $R + S$ with R and S two arbitrary points on the elliptic curve. So the Miller Lite loop $f_{x,P}(Q)$ and Full Miller loop $f_{x,Q}(P)$ requires 25 doublings step, 4 additions step, 24 squarings in $\mathbb{F}_{p^{27}}$, 27 multiplications in $\mathbb{F}_{p^{27}}$. We assume that the points $[p^i]P$, $(1 \le i \le 8)$ are precomputed. We consider the following additional notations.
MLite := the cost of the Miller lite loop

Algorithm 1: Miller's algorithm

Input: $n=\sum_{j=0}^{s} n_j 2^j \in \mathbb{N}, n_j \in \{-1, 0, 1\}, P \in \mathbb{G}_1, Q \in \mathbb{G}_2$
Output: $f_{n,Q}(P), [n]Q$

```
f ← 1, T ← Q
for j from s − 1 downto 0 do
    f ← f^2 . l_{T,T}(P)/v_{[2]T}(P); T ← [2]T        Doubling step
    if n_j = 1 then
        f ← f . l_{T,Q}(P)/v_{T+Q}(P); T ← T + Q      Addition step
    if n_j = −1 then
        f ← f . l_{T,−Q}(P)/v_{T−Q}(P); T ← T − Q     Addition step
return f.
```

FullM := the cost of full Miller loop
FS := the cost of the final step
FE := the cost of the final exponentiation

3.1.1 Final exponentiation by $(p^3 - 1)$ and final step

We use the costs of the arithmetic given in Table 2 in [25]. The final exponentiation costs : 1 p^3-Frobenius, 1 multiplication in $\mathbb{F}_{p^{27}}$ and 1 inversion in $\mathbb{F}_{p^{27}}$; therefore: $18M_1 + 1M_{27} + 1I_{27} = 18M_1 + 216M_1 + 1I_1 + 387M_1 + 62S_1 = 1I_1 + 621M_1 + 62S_1$. The 18 Miller functions of extended β Weil pairing defined above can be computed in parallel using 6 processors. Each processor computes three Miller functions. We denote by f_1, f_2 and f_3 the functions computed by the first processor, the second processor and the third processor. And g_1, g_2, g_3 the functions computed by the fourth processor, the fifth processor and the sixth processor. The execution path for computing the extended β Weil pairing for elliptic curves with $k = 27$ on 6 processors is the following:

1. The first processor computes $f_1 = f_{x,P}^{p^8}(Q).f_{x,[p]P}^{p^7}(Q).f_{x,[p^2]P}^{p^6}(Q)$; so it executes three Miller lite loops, one p^8-Frobenius, one p^7-Frobenius, one p^6-Frobenius and 2 multiplications in $\mathbb{F}_{p^{27}}$. ie. $3 \times MLite + 2 \times 26M_1 + 18M_1 + 2M_{27} = 3 \times MLite + 502M_1$.
2. The second processor computes $f_2 = f_{x,[p^3]P}^{p^5}(Q).f_{x,[p^4]P}^{p^4}(Q).f_{x,[p^5]P}^{p^3}(Q)$; so it executes three Miller lite loops, one p^5-Frobenius, one p^4-Frobenius, one p^3-Frobenius and 2 multiplications in $\mathbb{F}_{p^{27}}$. ie. $3 \times MLite + 2 \times 26M_1 + 18M_1 + 2M_{27} = 3 \times MLite + 502M_1$.
3. The third processsor computes $f_3 = f_{x,[p^6]P}^{p^2}(Q).f_{x,p^7]P}^{p}(Q).f_{x,[p^8]P}(Q)$; so it executes three Miller lite loops, one p^2-Frobenius, one p-Frobenius and 2 multiplications in $\mathbb{F}_{p^{27}}$. ie. $3 \times MLite + 2 \times 26M_1 + 2M_{27} = 3 \times MLite + 484M_1$.
4. The 4^{th} processor computes $g_1 = f_{x,Q}^{p^8}(P).f_{x,Q}^{p^7}([p]P).f_{x,Q}^{p^6}([p^2]P)$; so it executes three full Miller loops, one p^8-Frobenius, one p^7-Frobenius, one p^6-Frobenius and 2 multiplications in $\mathbb{F}_{p^{27}}$. ie. $3 \times FullM + 2 \times 26M_1 + 18M_1 + 2M_{27} = 3 \times FullM + 502M_1$.
5. The 5^{th} processor computes $g_2 = f_{x,Q}^{p^5}([p^3]P).f_{x,Q}^{p^4}([p^4]P).f_{x,Q}^{p^3}([p^5]P)$; so it executes three full Miller loops, one p^5-Frobenius, one p^4-Frobenius, one p^3-Frobenius and 2 multiplications in $\mathbb{F}_{p^{27}}$. ie. $3 \times FullM + 2 \times 26M_1 + 18M_1 + 2M_{27} = 3 \times FullM + 502M_1$.

Table 1 Cost of the full Miller loop in affine coordinates, the final step and the final exponentiation

Full Miller loop	Final step	Final exponentiation
$29I_1 + 11052M_1 + 4798S_1$ [25]	$1I_1 + 1467M_1 + 62S_1$ (this work)	$1I_1 + 621M_1 + 62S_1$ (this work)

Table 2 Cost comparison of the extended β-Weil pairing and the optimal ate pairing in affine coordinates

Coordinates system	G_1+FS+FE	Optimal ate pairing
Affine	$31I_1 + 18062M_1$ (this work)	$30I_1 + 94628M_1$ [25]

6. The 6th processor computes $g_3 = f_{x,Q}^{p^2}([p^6]P).f_{x,Q}^{p}([p^7]P).f_{x,Q}([p^8]P)$; so it executes three full Miller loops, one p^2-Frobenius, one p-Frobenius and 2 multiplications in $\mathbb{F}_{p^{27}}$. ie. $3 \times FullM + 2 \times 26M_1 + 2M_{27} = 3 \times FullM + 484M_1$.

So the final step consists of the computation of $(f_1 \times f_2 \times f_3) \times (g_1 \times g_2 \times g_3)^{-1}$ which costs 1 inversion and 5 multiplications in $\mathbb{F}_{p^{27}}$ ie. $1I_1 + 1467M_1 + 62S_1$.

Since the cost of Miller lite is cheaper than the cost of full Miller, we will ignore the cost of Miller lite in the rest of this work. We summarize in Table 1, the cost of the full Miller obtained in [25] in affine coordinates, the cost of the final step and the cost of the final exponentiation.

3.2 Comparison

In order to compare optimal ate and extended β-Weil pairing for curves with embedding degree $k = 27$, our comparison focuses only on the overall cost of optimal ate pairing with the cost of g_1 to which is added the final step and the final exponentiation by $(p^3 - 1)$ since the cost of g_1 is the most costly. If we assume that the cost of a squaring is the same as the cost of a multiplication ($m_k = s_k$). Denote by G_1 the cost of g_1.

Table 2 gives a comparison of the cost of the extended β-Weil pairing obtained in this work on curve with embedding degree 27 and the cost of the optimal ate pairing on the same curve proposed in [25]. From Table 2, we remark that our computation of extended β-Weil pairing saves 76,566 multiplications minus 1 inversion in $\mathbb{F}_p$, about 49,05% multiplications in $\mathbb{F}_p$.

4 A new optimal pairing

4.1 Definition of the new optimal pairing $\hat{\beta}_k$

We note that when the polynomial $h(z) = x - z$, we can define another pairing which is more efficient than the β_k pairing defined in Theorem 4. The following theorem summarises this result.

Theorem 5 *For all parameterized pairing-friendly curves $p(x), r(x), t(x)$ where the Vercauteren polynomial is of the form $h(z) = x - z$ such that $h(p) \equiv 0 (mod\ \ r)$, the map*

$\tilde{\beta}_k : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left(\prod_{i=0}^{e-1} f_{x,[p^i]P}(Q)^{p^{e-1-i}}\right)^{p^l-1}$ *is a pairing. More precisely if* $r \nmid (p^l - 1)p^{e-1}$, *then the new pairing* $\tilde{\beta}_k$ *is non-degenerate.*

Proof Since $h(z) = x - z$ and $h(p) \equiv 0 \pmod{r}$, the extended Miller function $f_{p,h,R} = f_{p,x-p,R} = f_{x,R}$; in this case, we have that $\beta_k(P, Q) = \prod_{i=0}^{e-1} \left(\frac{f_{x,[p^i]P}(Q)}{f_{x,Q}([p^i]P)}\right)^{(p^l-1)p^{e-1-i}}$. Since β_k and the map $(P, Q) \mapsto f_{x,Q}(P)$ are pairings respectively by the Theorem 4 and Lemma 2, we have that: $\prod_{i=0}^{e-1} f_{x,[p^i]P}(Q)^{(p^l-1)p^{e-1-i}} = \beta_k(P, Q) \cdot \prod_{i=0}^{e-1} f_{x,Q}([p^i]P)^{(p^l-1)p^{e-1-i}}$ is a pairing by Theorem 3. Furthermore, $\prod_{i=0}^{e-1} f_{x,[p^i]P}(Q)^{(p^l-1)p^{e-1-i}} = \left(\prod_{i=0}^{e-1} f_{x,[p^i]P}(Q)^{p^{e-1-i}}\right)^{p^l-1} = \tilde{\beta}_k(P, Q)$. On the other hand, $\tilde{\beta}_k$ is non-degenerate if $r \nmid (p^l - 1)p^{e-1}$ since the map β_k and $f_{x,Q}([p^i]P)$ are non-degenerate. □

Lemma 4 ([32], Theorem 3) *For* $P \in \mathbb{G}_1$ *and* $Q \in \mathbb{G}_2$, *then* $f_{p,[p^i]P}(Q) = f_{p,\hat{\pi}_{p^i}(P)}(\pi_{p^{k-i}}(Q))^{p^i}$.

Finally, using the relation from Lemma 4, the new pairing in Theorem 5 can be modified as the products of some rational functions with the same Miller loop.

Theorem 6 *For all parameterized pairing-friendly curves* $p(x), r(x), t(x)$ *where the Vercauteren polynomial is of the form* $h(z) = x - z$ *such that* $h(p) \equiv 0 (mod \ r)$, *the map* $\hat{\beta}_k : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left(\prod_{i=0}^{e-1} f_{x,\hat{\pi}_{p^i}(P)}(\pi_{p^{k-i}}(Q))\right)^{(p^l-1)p^{e-1}}$ *is a pairing.*

Remark 2 1. Since $\hat{\pi}_{p^i} \circ \pi_{p^i} = [p^i]$ on E, it follows that $\hat{\pi}_{p^i} \circ \pi_{p^i}(P) = [p^i]P$ and since $\pi_{p^i}(P) = P$; then we have that $\hat{\pi}_{p^i}(P) = [p^i]P$.
2. Note that we can used the multi-pairing technique (see Algorithm 2) to calculate our new pairing $\hat{\beta}_k$ since it is defined as the product of some rational functions with the same Miller loop.

In Algorithm 2, $l_{R,S}$ is the straight line containing R and S and v_{R+S} is the corresponding vertical line passing through $R + S$ with R and S two arbitrary points on the elliptic curve.

4.2 Computation of the new optimal pairing $\hat{\beta}_k$

Set $P_i = [p^i]P$ and $Q_i = \pi_{p^{k-i}}(Q)$ for $0 \le i \le e - 1$. In order to compute $\hat{\beta}_k$, we assume that the points P_i and Q_i for $1 \le i \le e-1$ are precomputed. The computation of $\hat{\beta}_k$ involves two mains steps: the product of e Miller functions and the simple final exponentiation. In this case, the Miller function consists of the computing of $f_{x,P_i}(Q_i)$. Since our new pairing $\hat{\beta}_k$ is the product of several rational functions with the same Miller loop, we can used the multi-pairing technique for computing $\hat{\beta}_k$. So to evaluate the cost of the computation of $\hat{\beta}_k$, we have to compute at first:

C_1: Full squarings in the Miller loop;
C_2: Other operations in the Miller loop (point operations and line evaluations);
C_3: the cost of simple final exponentiation by $(p^l - 1)p^{e-1}$

Then the overall cost of $\hat{\beta}_k$ is the sum of C_1, eC_2 and C_3.

Algorithm 2: Miller's algorithm for multi-pairing

Input: $\mathrm{n}=\sum_{j=0}^{L} n_j 2^j \in \mathbb{N}, n_j \in \{-1,0,1\}, \{P_1, P_2, ..., P_{e-1}\}, \{Q_1, Q_2, ..., Q_{e-1}\}$

Output: $\prod_{i=0}^{e-1} f_{n,P_i}(Q_i), \{[n]P_0, [n]P_2, ..., [n]P_{e-1}\}$

$f \leftarrow 1$
for i *from* $e-1$ *downto* 0 **do**
  $T_i \leftarrow P_i$
for j *from* $L-1$ *downto* 0 **do**
  $f \leftarrow f^2$
  for i *from* $e-1$ *downto* 0 **do**
    $f \leftarrow f.l_{T_i,T_i(Q_i)}/v_{[2]T_i}(Q_i)$; $T_i \leftarrow [2]T_i$
  if $n_j = 1$ **then**
    for i *from* $e-1$ *downto* 0 **do**
      $f \leftarrow f.l_{T_i,P_i}(Q_i)/v_{T_i+P_i}(Q_i)$; $T_i \leftarrow T_i + P_i$
  if $n_j = -1$ **then**
    for i *from* $e-1$ *downto* 0 **do**
      $f \leftarrow f.l_{T_i,-P_i}(Q_i)/v_{T_i-P_i}(Q_i)$; $T_i \leftarrow T_i - P_i$
return f.

4.3 The new $\hat{\beta}_k$ pairing on pairing-friendly curves with $k = 15$ and on BLS12 curves

In this section, we apply Theorem 6 on pairing-friendly curves with embedding degrees $k = 15$ and $k = 12$ at 128-bit security level.

4.3.1 Computation on pairing-friendly curves with $k = 15$

This family of elliptic curves has embedding degree 15 and a ρ-value 1.5 and is parameterized by :

$$\begin{aligned} p(x) &= (x^{12} - 2x^{11} + x^{10} + x^7 - 2x^6 + x^5 + x^2 + x + 1)/3 \\ r(x) &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \\ t(x) &= x + 1 \end{aligned} \tag{8}$$

The Vercauteren approach described in [29] enabled us to obtain the following optimal function $h(z) = x - z \in \mathbb{Z}[z]$. Notice that this family of elliptic curves has a cubic twist, i.e., $d = 3$. Since $k = 15$, we have $e = \frac{k}{(k,d)} = 5$. We can take $l = 3$ since 3 is a proper divisor of k. According to Theorem 6, we obtain this following result:

Proposition 2 *The $\hat{\beta}_k$-pairing over pairing-friendly curves with $k = 15$ is bilinear and non degenerate map:*

$$\hat{\beta_{15}} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left(\prod_{i=0}^{4} f_{x,P_i}(Q_i)\right)^{(p^3-1)p^4}.$$

Following the recommendation from Table 4 in [25] at the 128-bit security level,Fouotsa et al. find with a Pari/GP code the value $x = 2^{31} + 2^{19} + 2^5 + 2^2$ so that $r(x)$ is a prime of 249 bits and $p(x)$ is a prime of 371 bits. In this case, the Miller function consists of

the computing of $f_{x,P_i}(Q_i)$. So the Miller loop executes 31 point doubling with associated line evaluations, 3 point additions with line evaluations, 30 squarings in $\mathbb{F}_{p^{15}}$ and 33 sparse multiplications in $\mathbb{F}_{p^{15}}$. Following the above explanation, we have that for evaluating the cost of the computation of $\hat{\beta_{15}}$, we have to compute at first:

C_1: Full squarings in the Miller loop;
C_2: Other operations in the Miller loop (point operations and line evaluations);
C_3: the cost of simply final exponentiation by $(p^3-1)p^4$

Then to find the overall cost of $\hat{\beta_{15}}$, we have to sum C_1, $5C_2$, and C_3. Using the cost of arithmetic operations in Table 4 in [25]. In this case, for $k = 15$, we compute the Miller function in projective coordinates, since the projective formulas allow a fast pairing computation according Aranha et al. [2]. Following the cost of Doubling and addition step in the Table 3 in projective coordinates, we obtain a Miller loop cost of $31(9S_1 + 37M_1) + 3(5S_1 + 53M_1) + 30S_{15} + 33M_{15} = 2791M_1 + 1644S_1 = 4435M_1$ (when we assume that $1S_1 = 1M_1$) and the full squaring in Miller loop costs C_1 is $30S_{15} = 30 \times 45S_1 = 1350S_1 = 1350M_1$; thus $C_2 = 3085M_1$. Finally, the final exponentiation requires 1 p^3-Frobenius map, 1 p^4-Frobenius map, 1 inversion in $\mathbb{F}_{p^{15}}$ and 1 multiplication in $\mathbb{F}_{p^{15}}$. Thus, $C_3 = 2 \times 14M_1 + 1I_1 + 149M_1 + 45M_1 = 1I_1 + 222M_1$. The overall cost of $\hat{\theta}$ is $C_1 + 5C_2 + C_3 = 1350M_1 + 5 \times 3085M_1 + 222M_1 + I_1 = 16997M_1 + I_1$.

4.3.2 Computation on pairing-friendly curves with $k = 12$ (BLS12)

In 2002, Barreto, Lynn and Scott proposed in [6] a method to generate pairing-friendly elliptic curves over a prime field $\mathbb{F}_p$ with embedding degree $k = 12$. BLS12 are defined over $\mathbb{F}_p$ by following polynomials:

$$\begin{aligned} p(x) &= (x-1)^2(x^4 - x^2 + 1)/3 + x \\ r(x) &= x^4 - x^2 + 1 \\ t(x) &= x + 1 \end{aligned} \tag{9}$$

The Vercauteren approach described in [29] enabled us to obtain the following optimal function $h(z) = x - z \in \mathbb{Z}[z]$. Notice that this family of elliptic curves has a sextic twist, i.e., $d = 6$. Since $k = 12$, we have $e = \frac{k}{(k,d)} = 2$. We can take $l = 6$ since 6 is a proper divisor of k. According to Theorem 6, we obtain this following result:

Proposition 3 *The $\hat{\beta}_k$-pairing over pairing-friendly curves with $k = 12$ is bilinear and non degenerate map:*

$$\hat{\beta_{12}} : \mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r : (P, Q) \mapsto \left(\prod_{i=0}^{1} f_{x,P_i}(Q_i) \right)^{p(p^6-1)}.$$

According to recent works of Barbulescu et al. in [4], they found the new parameters and recommend to use $x = -2^{77} + 2^{50} + 2^{33}$. This gives $p(x)$ a prime of 461 bits and a prime factor of $r(x)$ of 273 bits. In this case, the Miller function consists of the computation of $f_{x,P_i}(Q_i)$. So the Miller loop executes 77 point doublings with associated line evaluations, 2 point additions with line evaluations, 76 squarings in $\mathbb{F}_{p^{12}}$ and 78 sparse multiplications in $\mathbb{F}_{p^{12}}$. Following the above explanation, we have that for evaluating the cost of the computation of $\hat{\beta_{12}}$, we have to compute:

Table 3 Cost of doubling and addition step in the Miller lite loop in projective coordinates

Cost	Dbl point	Evaluation of Miller function	Miller dbl step	Add point	Evaluation of Miller function	Miller Add step
Proj	$5S_1 + 2M_1$	$4S_1 + 35M_1$	$9S_1 + 37M_1$	$2S_1 + 13M_1$	$3S_1 + 40M_1$	$5S_1 + 53M_1$

Table 4 Cost of doubling and addition step in the Miller lite loop in projective coordinates

Cost	Dbl point	evaluation of Miller function	Miller dbl step	Add point	Evaluation of Miller function	Miller Add step
Proj	$5S_1 + 2M_1$	$10M_1$	$5S_1 + 12M_1$	$2S_1 + 13M_1$	$14M_1$	$2S_1 + 27M_1$

Table 5 Efficiency comparison of the computation of optimal ate and $\hat{\beta}_k$ pairings for BLS12 and pairing-friendly curves with k=15

Curves	Pairings	Overall cost of pairing
BLS12-curves	optimal ate	$16003M_1 + I_1$ [4]
	$\hat{\beta}_k$**-pairing**	$\mathbf{12082}\boldsymbol{M_1} + \boldsymbol{I_1}$ (this work)
Pairing-friendly with k=15	optimal ate	$25919M_1 + I_1$ [25]
	$\hat{\beta}_k$**-pairing**	$\mathbf{16997}\boldsymbol{M_1} + \boldsymbol{I_1}$ (this work)

C_1: Full squarings in the Miller loop;
C_2: Other operations in the Miller loop (point operations and line evaluations);
C_3: the cost of simply final exponentiation by $p(p^6 - 1)$.

Then to find the overall cost of $\hat{\beta_{12}}$, we have to sum C_1, $2C_2$ and C_3. Using the cost of arithmetic operations in Table 4 in [2]. In this case, for $k = 12$, we compute the Miller function in projective coordinates, since the projective formulas allow a fast pairing computation according Aranha et al. [2]. Following the cost of doubling and addition step in the Table 4 in projective coordinates, we obtain a Miller loop cost of $77(7S_1 + 12M_1) + 3(2S_1 + 27M_1) + 76(36M_1) + 78(39M_1) = 6783M_1 + 545S_1 = 7328M_1$ and the full squaring in Miller loop costs C_1 is $76S_{12} = 76 \times 36M_1 = 2736M_1$; thus $C_2 = 4592M_1$. Finally, the final exponentiation requires 1 p-Frobenius map, 1 multiplication in $\mathbb{F}_{p^{12}}$ and 1 inversion in $\mathbb{F}_{p^{12}}$ since raising to the power p^6 is equivalent to one conjugation [7]. Thus $C_3 = 11M_1 + 1I_1 + 97M_1 + 54M_1 = 1I_1 + 162M_1$. The overall cost of $\hat{\theta} = C_1 + 2C_2 + C_3 = 2736M_1 + 2 \times 4592M_1 + 162M_1 + I_1 = 12082M_1 + I_1$.

4.4 General comparison

In order to compare the new pairing $\hat{\beta}_k$ and optimal ate pairing, we summarize the overall cost of the computation of these pairing in the Table 5. Table 5 gives a comparison of the cost of $\hat{\beta}_k$ pairings for BLS12 and pairing-friendly curves with $k = 15$ obtained in this work against the cost of the optimal ate pairing on pairing-friendly curves with $k = 15$ proposed in [25] and optimal ate on BLS12 proposed in [4]. From Table 5, we remark that our computation of our new optimal pairing saves $3921M_1$ for BLS12 and $8922M_1$ for pairing-friendly curves with $k = 15$.

5 Conclusion

In this paper, we first extended the β-Weil pairing to ordinary elliptic curves with any embedding degree and we propose a new optimal pairing which is suitable for multi-pairing technique for efficient implementation. We then show that the proposed new optimal pairing is more efficient than optimal ate pairing and the extended β-Weil pairing is more efficient than optimal ate pairing as well.

References

1. Abdalla, M., Catalano, D., Dent, A. W., Malone-Lee, J., Neven, G., Smart, N.P.: Identity-based encryption gone wild. In: Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10–14, 2006, Proceedings, Part II, pp. 300–311 (2006)
2. Aranha, D.F., Fuentes-Castañeda, L., Knapp, E., Menezes, A., Rodriguez-Henriquez, F.: Implementing pairings at the 192-bit security level. In: Pairing-Based Cryptography-Pairing 2012—5th International Conference, Cologne, Germany, May 16–18, 2012, Revised Selected Papers, pp. 177–195 (2012)
3. Aranha, D.F., Knapp, E., Menezes, A., Rodriguez-Henriquez, F.: Parallelizing the Weil and Tate pairings. Crytogr. Coding LNCS **7089**, 275–295 (2011)
4. Barbulescu, R., Duquesne, S.: Updating key size estimations for pairings. J. Cryptol. (2018)
5. Barreto, P.S.L.M., Kim, H.Y., Lynn, B., Scott, M.: Efficient algorithms for pairing-based cryptosystems. In: Advances in Cryptology-Crypto'2002, vol. 2442 of Lecture Notes in Computer Science, pp. 354–368. Springer, Berlin (2002)
6. Barreto, P.S.L.M., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees, security in communication networks. In: Third International Conference, pp. 257–267, Amalfi, Italy, September 11–13, (2002) **(Revised Papers)**
7. Beuchat, J.-L., González-Díaz, J.E., Mitsunari, S., Okamoto, E., Rodríguez-Henríquez, F., Teruya, T.: High-Speed software implementation of the optimal ate pairing over Barreto-Naehrig curves. In: Joye, M., Miyaji, A., Otsuka, A. (eds.) Pairing 2010. LNCS, vol. 6487, pp. 21–39. Springer, Heidelberg (2010)
8. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Advances in Cryptology—CRYPTO 2004, 24th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15–19, 2004, Proceedings, pp. 41–55 (2004)
9. Boneh, D., Franklin, M.: Identity-based Encryption from the Weil pairing. Adv. Cryptol. CRYPTO 01 LNCS **2139**, 231–2129 (2001)
10. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. J. Cryptol. **17**(4), 297–319 (2004)
11. Chen, L., Cheng, Z., Smart, N.P.: A built-in decisional function and security proof of id-based key agreement protocols from pairings. IACR Cryptol. **2006**, 160 (2006). **(ePrint Archive)**
12. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Cryptography and Coding, 8th IMA International Conference, Cirencester, UK, December 17–19, 2001, Proceedings, pp. 360–363 (2001)
13. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptol. **23**(2), 224280 (2010)
14. Ghammam, L., Fouotsa, E.: Improving the computation of the optimal ate pairing for a high security level. Int. J. Appl. Math. Comput. https://doi.org/10.1007/s12190-018-1167-y (2018)
15. 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. WAIFI 2016. Lecture Notes in Computer Science, vol. 10064. Springer, Cham (2016)
16. Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for ne-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, October 30–November 3, 2006, p. 8998 (2006)
17. Granger, R., Hess, F., Oyono, R., Thériault, N., Vercauteren, F.: Ate pairing on hyperelliptic curves, Advances in Cryptology—EUROCRYPT 2007. LNCS **4515**, 430–447 (2007)
18. Granger, R., Smart, N.P.: On computing products of pairings. Cryptology ePrint Archive Report 2006/172. Preprint available at http://eprint.iacr.org/2006/172 (2006)
19. Hess, F., Smart, N.P., Vercauteren, F.: The Eta pairing revisited. IEEE Trans. Inf. Theory **52**, 4595–4602 (2006)
20. Joux, A.: A One Round Protocol for Tripartite Diffie Hellman. In: Proceedings of ANTS 4, LNCS 1838, pp. 385–394 (2000)
21. Lauter, v., Montgomery, P.L., Naehrig, M.: An analysis of affine coordinates for pairing computation. In: Proceedings of the 4th International Conference on Pairing-based Cryptography. Pairing'10. Berlin, Heidelberg, Springer (2010)
22. Libert, B., Quisquater, J.-J.: Identity based undeniable signatures. In: Topics in Cryptology CT-RSA 2004, the Cryptographer Track at the RSA Conference 2004, San Francisco, CA, USA, February 23–27, 2004, Proceedings, p. 112125 (2004)
23. Menezes, A., Sarkar, P., Singh, S.: Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography. IACR Cryptology ePrint Archive: Report 2016/1102 (2016)
24. Miller, V.S.: The Weil pairing and its efficient calculation. J. Cryptol. **17**, 235–261 (2004)

25. Fouotsa, E., EL Mrabet, N., Pecha, A.: Computing optimal ate pairing on elliptic curves with embedding Degree 9, 15, 27, IACR Cryptology ePrint Archive, **2016**, 1187 (2016). https://eprint.iacr.org/2016/1187
26. Sakemi, Y., Takeuchi, S., Nogami, Y., Morikawa, Y.: Accelering twisted ate pairing with Frobenius map, small scalar multiplication, and multi-pairing. In: ICISC 2009, LNCS 5984, pp. 47–64. Springer (2010)
27. Silverman, J.H.: The Arithmetic of Elliptic Curves, 2nd edn. Springer, New York (2009)
28. Scott, M.: On the efficient implementation of pairing-based protocols. In: Cryptography and Coding 2011, LNCS 7089, pp. 296–308. Springer (2011)
29. Vercauteren, F.: Optimal pairings. IEEE Trans. Inf. Theory **56**, 455–461 (2010)
30. Waters, B.: Efficient identity-based encryption without random oracles. In: Advances in Cryptology—EUROCRYPT 2005, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, May 22–26, 2005, Proceedings, pp. 114–127 (2005)
31. Zhang, X., Lin, D.: Analysis of optimum pairing products at high security levels. In: Galbraith, S., Nandi, M. (eds.) INDOCRYPT 2012, LNCS 7668, pp. 412–430. Springer, Berlin Heidelberg (2012)
32. Zhang, X., Wang, X., Lin, D.: On efficient pairings on elliptic curves over extension field, pairing-based cryptography- pairing 2012. Lect. Notes Comput. Sci. **7708**, 1–18 (2013)
33. Zhao, C.-A., Zhang, F., Huang, J.: All pairings are in a group. IEICE Trans. Fundamentals **E91–A**(10), 3084–3087 (2008)
34. Zhao, C.-A, Zhang, F., Xie, D.: Reducing the complexity of the Weil pairing computation. Cryptology ePrint, Report 212 (2008)