Efficient Optimal Ate Pairing at 128-bit Security Level

Md Al-Amin Khandaker, Yuki Nanjo, Loubna Ghammam, Sylvain Duquesne, Yasuyuki Nogami, Yuta Kodera

Efficient Optimal Ate Pairing at 128-bit Security Level

Md. Al-Amin Khandaker[1(✉)][0000−0001−7330−138X], Yuki Nanjo[1], Loubna Ghammam[2], Sylvain Duquesne[3][0000−0002−3854−8253], Yasuyuki Nogami[1][0000−0001−6247−0719], and Yuta Kodera[1][0000−0002−6482−6122]

[1] Faculty of Engineering, Okayama University, 7008530, Okayama, Japan
{khandaker,yuki.nanjo,yuta.kodera}@s.okayama-u.ac.jp,
yasuyuki.nogami@okayama-u.ac.jp
[2] Normandie Université, UNICAEN, ENSICAEN, CNRS, GREYC,
14000 Caen, France
ghammam.loubna@yahoo.fr
[3] Univ Rennes, CNRS, IRMAR - UMR 6625, F-35000 Rennes, France
sylvain.duquesne@univ-rennes1.fr

Abstract. Following the emergence of Kim and Barbulescu's new number field sieve (exTNFS) algorithm at CRYPTO'16 [21] for solving discrete logarithm problem (DLP) over the finite field; pairing-based cryptography researchers are intrigued to find new parameters that confirm standard security levels against exTNFS. Recently, Barbulescu and Duquesne have suggested new parameters [3] for well-studied pairing-friendly curves i.e., Barreto-Naehrig (BN) [5], Barreto-Lynn-Scott (BLS-12) [4] and Kachisa-Schaefer-Scott (KSS-16) [19] curves at 128-bit security level (twist and sub-group attack secure). They have also concluded that in the context of Optimal-Ate pairing with their suggested parameters, BLS-12 and KSS-16 curves are more efficient choices than BN curves. Therefore, this paper selects the atypical and less studied pairing-friendly curve in literature, i.e., KSS-16 which offers quartic twist, while BN and BLS-12 curves have sextic twist. In this paper, the authors optimize Miller's algorithm of Optimal-Ate pairing for the KSS-16 curve by deriving efficient sparse multiplication and implement them. Furthermore, this paper concentrates on the Miller's algorithm to experimentally verify Barbulescu et al.'s estimation. The result shows that Miller's algorithm time with the derived pseudo 8-sparse multiplication is most efficient for KSS-16 than other two curves. Therefore, this paper defends Barbulescu and Duquesne's conclusion for 128-bit security.

Keywords: KSS-16 curve, Optimal-Ate pairing, sparse multiplication

1 Introduction

Since the inception by Sakai et al. [25], pairing-based cryptography has gained much attention to cryptographic researchers as well as to mathematicians. It gives flexibility to protocol researcher to innovate applications with provable

security and at the same time to mathematicians and cryptography engineers to find efficient algorithms to make pairing implementation more efficient and practical. This paper tries to efficiently carry out the basic operation of a specific type of pairing calculation over certain pairing-friendly curves.

Generally, a pairing is a bilinear map e typically defined as $\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive cyclic sub-groups of order r on a certain elliptic curve E over a finite extension field $\mathbb{F}_{p^k}$ and $\mathbb{G}_T$ is a multiplicative cyclic group of order r in $\mathbb{F}^*_{p^k}$. Let $E(\mathbb{F}_p)$ be the set of rational points over the prime field $\mathbb{F}_p$ which forms an additive Abelian group together with the point at infinity $\mathcal{O}$. The total number of rational points is denoted as $\#E(\mathbb{F}_p)$. Here, the order r is a large prime number such that $r|\#E(\mathbb{F}_p)$ and $\gcd(r, p) = 1$. The embedding degree k is the smallest positive integer such that $r|(p^k - 1)$. Two basic properties of pairing are

- bilinearity is such that $\forall P_i \in \mathbb{G}_1$ and $\forall Q_i \in \mathbb{G}_2$, where $i = 1, 2$, then $e(Q_1 + Q_2, P_1) = e(Q_1, P_1).e(Q_2, P_1)$ and $e(Q_1, P_1 + P_2) = e(Q_1, P_1).e(Q_1, P_2)$,
- and e is non-degenerate means $\forall P \in \mathbb{G}_1$ there is a $Q \in \mathbb{G}_2$ such that $e(Q, P) \neq 1$ and $\forall Q \in \mathbb{G}_2$ there is a $P \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$.

Such properties allows researchers to come up with various cryptographic applications including ID-based encryption [8], group signature authentication [7], and functional encryption [24]. However, the security of pairing-based cryptosystems depends on

- the difficulty of solving elliptic curve discrete logarithm problem (ECDLP) in the groups of order r over $\mathbb{F}_p$,
- the infeasibility of solving the discrete logarithm problem (DLP) in the multiplicative group $\mathbb{G}_T \in \mathbb{F}^*_{p^k}$,
- and the difficulty of pairing inversion.

To maintain the same security level in both groups, the size of the order r and extension field p^k is chosen accordingly. If the desired security level is δ then $\log_2 r \geq 2\delta$ is desirable due to Pollard's rho algorithm. For efficient pairing, the ratio $\rho = \log_2 p^k / \log_2 r \approx 1$, is expected (usually $1 \leq \rho \leq 2$). In practice, elliptic curves with small embedding degrees k and large r are selected and commonly are knows as "pairing-friendly" elliptic curves.

Galbraith et al. [15] have classified pairings as three major categories based on the underlying group's structure as

- Type 1, where $\mathbb{G}_1 = \mathbb{G}_2$, also known as symmetric pairing.
- Type 2, where $\mathbb{G}_1 \neq \mathbb{G}_2$, known as asymmetric pairing. There exists an efficiently computable isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ but none in reverse direction.
- Type 3, which is also asymmetric pairing, i.e., $\mathbb{G}_1 \neq \mathbb{G}_2$. But no efficiently computable isomorphism is known in either direction between $\mathbb{G}_1$ and $\mathbb{G}_2$.

This paper chooses one of the Type 3 variants of pairing named as Optimal-Ate [29] with Kachisa-Schaefer-Scott (KSS) [19] pairing-friendly curve of embedding degree $k = 16$. Few previous works have been done on this curve. Zhang et al.

[31] have shown the computational estimation of the Miller's loop and proposed efficient final exponentiation for 192-bit security level in the context of Optimal-Ate pairing over KSS-16 curve. A few years later Ghammam et al. [16] have shown that KSS-16 is the best suited for multi-pairing (i.e., the product and/or the quotient) when the number of pairing is more than two. Ghammam et al. [16] also corrected the flaws of proposed final exponentiation algorithm by Zhang et al. [31] and proposed a new one and showed the vulnerability of Zhang's parameter settings against small subgroup attack. The recent development of NFS by Kim and Barbulescu [21] requires updating the parameter selection for all the existing pairings over the well known pairing-friendly curve families such as BN [5], BLS [13] and KSS [19]. The most recent study by Barbulescu et al. [3] have shown the security estimation of the current parameter settings used in well-studied curves and proposed new parameters, resistant to small subgroup attack.

Barbulescu and Duquesne's study finds that the current parameter settings for 128-bit security level on BN-curve studied in literature can withstand for 100-bit security. Moreover, they proposed that BLS-12 and surprisingly KSS-16 are the most efficient choice for Optimal-Ate pairing at the 128-bit security level. Therefore, the authors focus on the efficient implementation of the less studied KSS-16 curve for Optimal-Ate pairing by applying the most recent parameters. Mori et al. [23] and Khandaker et al. [20] have shown a specific type of sparse multiplication for BN and KSS-18 curve respectively where both of the curves supports sextic twist. The authors have extended the previous works for quartic twisted KSS-16 curve and derived pseudo-8 sparse multiplication for line evaluation step in the Miller's algorithm. As a consequence, the authors made the choice to concentrate on Miller's algorithm's execution time and computational complexity to verify the claim of [3]. The implementation shows that Miller's algorithm time has a tiny difference between KSS-16 and BLS-12 curves. However, they both are more efficient and faster than BN curve.

2 Fundamentals of Elliptic Curve and Pairing

2.1 Kachisa-Schaefer-Scott (KSS) Curve

In [19], Kachisa, Schaefer, and Scott proposed a family of non super-singular pairing-friendly elliptic curves of embedding degree $k = \{16, 18, 32, 36, 40\}$, using elements in the cyclotomic field. In what follows, this paper considers the curve of embedding degree $k = 16$, named as *KSS-16*, defined over extension field $\mathbb{F}_{p^{16}}$ as follows:

$$E/\mathbb{F}_{p^{16}} : Y^2 = X^3 + aX, \quad (a \in \mathbb{F}_p) \text{ and } a \neq 0, \tag{1}$$

where $X, Y \in \mathbb{F}_{p^{16}}$. Similar to other pairing-friendly curves, *characteristic* p, *Frobenius trace* t and *order* r of this curve are given by the following polynomials

of integer variable u.

$$p(u) = (u^{10} + 2u^9 + 5u^8 + 48u^6 + 152u^5 + 240u^4 + 625u^2 + 2398u + 3125)/980, \tag{2a}$$

$$r(u) = (u^8 + 48u^4 + 625)/61255, \tag{2b}$$

$$t(u) = (2u^5 + 41u + 35)/35, \tag{2c}$$

where u is such that $u \equiv 25$ or $45 \pmod{70}$ and the ρ value is $\rho = (\log_2 p/\log_2 r) \approx 1.25$. The total number of rational points $\#E(\mathbb{F}_p)$ is given by Hasse's theorem as, $\#E(\mathbb{F}_p) = p + 1 - t$. When the definition field is the k-th degree extension field $\mathbb{F}_{p^k}$, rational points on the curve E also form an additive Abelian group denoted as $E(\mathbb{F}_{p^k})$. Total number of rational points $\#E(\mathbb{F}_{p^k})$ is given by Weil's theorem [30] as $\#E(\mathbb{F}_{p^k}) = p^k + 1 - t_k$, where $t_k = \alpha^k + \beta^k$. α and β are complex conjugate numbers.

2.2 Extension Field Arithmetic and Towering

Pairing-based cryptography requires performing the arithmetic operation in extension fields of degree $k \geq 6$ [28]. Consequently, such higher degree extension field needs to be constructed as a tower of sub-fields [6] to perform arithmetic operation cost efficiently. Bailey et al. [2] have explained optimal extension field by towering by using irreducible binomials.

Towering of $\mathbb{F}_{p^{16}}$ extension field: For KSS-16 curve, $\mathbb{F}_{p^{16}}$ construction process given as follows using tower of sub-fields.

$$\begin{cases} \mathbb{F}_{p^2} = \mathbb{F}_p[\alpha]/(\alpha^2 - c), \\ \mathbb{F}_{p^4} = \mathbb{F}_{p^2}[\beta]/(\beta^2 - \alpha), \\ \mathbb{F}_{p^8} = \mathbb{F}_{p^4}[\gamma]/(\gamma^2 - \beta), \\ \mathbb{F}_{p^{16}} = \mathbb{F}_{p^8}[\omega]/(\omega^2 - \gamma), \end{cases} \tag{3}$$

where $p \equiv 5 \bmod 8$ and c is a quadratic non residue in $\mathbb{F}_p$. This paper considers $c = 2$ along with the value of the parameter u as given in [3].

Towering of $\mathbb{F}_{p^{12}}$ extension field: Let $6|(p-1)$, where p is the characteristics of BN or BLS-12 curve and -1 is a quadratic and cubic non-residue in $\mathbb{F}_p$ since $p \equiv 3 \bmod 4$. In the context of BN or BLS-12, where $k = 12$, $\mathbb{F}_{p^{12}}$ is constructed as a tower of sub-fields with irreducible binomials as follows:

$$\begin{cases} \mathbb{F}_{p^2} = \mathbb{F}_p[\alpha]/(\alpha^2 + 1), \\ \mathbb{F}_{p^6} = \mathbb{F}_{p^2}[\beta]/(\beta^3 - (\alpha + 1)), \\ \mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}[\gamma]/(\gamma^2 - \beta). \end{cases} \tag{4}$$

Table 1. Number of arithmetic operations in extension field based on Eq. (3)

$M_{p^2} = 3M_p + 5A_p + 1m_\alpha \rightarrow 3M_p$	$S_{p^2} = 3S_p + 4A_p + 1m_\alpha \rightarrow 3S_p$
$M_{p^4} = 3M_{p^2} + 5A_{p^2} + 1m_\beta \rightarrow 9M_p$	$S_{p^4} = 3S_{p^2} + 4A_p p^2 + 1m_\beta \rightarrow 9S_p$
$M_{p^8} = 3M_{p^4} + 5A_{p^4} + 1m_\gamma \rightarrow 27M_p$	$S_{p^8} = 3S_{p^4} + 4A_{p^4} + 1m_\gamma \rightarrow 27S_p$
$M_{p^{16}} = 3M_{p^8} + 5A_{p^8} + 1m_\omega \rightarrow 81M_p$	$S_{p^{16}} = 3M_{p^8} + 4A_{p^8} + 1m_\omega \rightarrow 81S_p$

Table 2. Number of arithmetic operations in $\mathbb{F}_{p^{12}}$ based on Eq. (4)

$M_{p^2} = 3M_p + 5A_p + 1m_\alpha \rightarrow 3M_p$	$S_{p^2} = 2S_p + 3A_p \rightarrow 2S_p$
$M_{p^6} = 6M_{p^2} + 15A_{p^2} + 2m_\beta \rightarrow 18M_p$	$S_{p^6} = 2M_{p^2} + 3S_{p^2} + 9A_{p^2} + 2m_\beta \rightarrow 12S_p$
$M_{p^{12}} = 3M_{p^6} + 5A_{p^6} + 1m_\gamma \rightarrow 54M_p$	$S_{p^{12}} = 2M_{p^6} + 5A_{p^6} + 2m_\gamma \rightarrow 36S_p$

Extension Field Arithmetic of $\mathbb{F}_{p^{16}}$ and $\mathbb{F}_{p^{12}}$ Among the arithmetic operations multiplication, squaring and inversion are regarded as expensive operation than addition/subtraction. The calculation cost, based on number of prime field multiplication M_p and squaring S_p is given in Table 1. The arithmetic operations in $\mathbb{F}_p$ are denoted as M_p for a multiplication, S_p for a squaring, I_p for an inversion and m with suffix denotes multiplication with basis element. However, squaring is more optimized by using Devegili et al.'s [11] complex squaring technique which cost $2M_p + 4A_p + 2m_\alpha$ for one squaring operation in $\mathbb{F}_{p^2}$. In total it costs $54M_p$ for one squaring in $\mathbb{F}_{p^{16}}$. Table 1 shows the operation estimation for $\mathbb{F}_{p^{16}}$.

Table 2 shows the operation estimation for $\mathbb{F}_{p^{12}}$ according to the towering shown in Eq. (4). The algorithms for $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$ multiplication and squaring given in [12] have be used in this paper to construct the $\mathbb{F}_{p^{12}}$ extension field arithmetic.

2.3 Ate and Optimal-Ate On KSS-16, BN, BLS-12 Curve

A brief of pairing and it's properties are described in Sect.1. In the context of pairing on the targeted pairing-friendly curves, two additive rational point groups $\mathbb{G}_1, \mathbb{G}_2$ and a multiplicative group $\mathbb{G}_T$ of order r are considered. $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are defined as follows:

$$\begin{aligned} \mathbb{G}_1 &= E(\mathbb{F}_p)[r] \cap \mathrm{Ker}(\pi_p - [1]), \\ \mathbb{G}_2 &= E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\pi_p - [p]), \\ \mathbb{G}_T &= \mathbb{F}^*_{p^k}/(\mathbb{F}^*_{p^k})^r, \\ e &: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T, \end{aligned} \tag{5}$$

where e denotes Ate pairing [9]. $E(\mathbb{F}_{p^k})[r]$ denotes rational points of order r and $[n]$ denotes n times scalar multiplication for a rational point. π_p denotes the Frobenius endomorphism given as $\pi_p : (x, y) \mapsto (x^p, y^p)$.

Table 3. Optimal Ate pairing formulas for target curves

Curve	Miller's Algo.	Final Exp.
KSS-16	$(f_{u,Q}(P) \cdot l_{[u]Q,[p]Q}(P))^{p^3} \cdot l_{Q,Q}(P)$	$(p^{16}-1)/r$
BN	$f_{6u+2,Q}(P) \cdot l_{[6u+2]Q,[p]Q}(P) \cdot l_{[6u+2+p]Q,[p2]Q}(P)$	$(p^{12}-1)/r$
BLS-12	$f_{u,Q}(P)$	$(p^{12}-1)/r$

KSS-16 Curve: In what follows, we consider $P \in \mathbb{G}_1 \subset E(\mathbb{F}_p)$ and $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{16}})$ for KSS-16 curves. Ate pairing $e(Q,P)$ is given as follows:

$$e(Q,P) = f_{t-1,Q}(P)^{\frac{p^{16}-1}{r}}, \tag{6}$$

where $f_{t-1,Q}(P)$ symbolizes the output of Miller's algorithm and $\lfloor \log_2(t-1) \rfloor$ is the loop length. The bilinearity of Ate pairing is satisfied after calculating the final exponentiation $(p^k-1)/r$.

Vercauteren proposed more efficient variant of Ate pairing named as Optimal-Ate pairing [29] where the Miller's loop length reduced to $\lfloor \log_2 u \rfloor$. The previous work of Zhang et al. [31] has derived the optimal Ate pairing on the KSS-16 curve which is defined as follows with $f_{u,Q}(P)$ is the Miller function evaluated on P:

$$e_{opt}(Q,P) = ((f_{u,Q}(P) \cdot l_{[u]Q,[p]Q}(P))^{p^3} \cdot l_{Q,Q}(P))^{\frac{p^{16}-1}{r}}. \tag{7}$$

The formulas for Optimal-Ate pairing for the target curves are given in Table 3.

The naive calculation procedure of Optimal-Ate pairing is shown in Alg. 1. In what follows, the calculation steps from 1 to 11, shown in Alg.1, is identified as Miller's Algorithm (MA) and step 12 is the final exponentiation (FE). Steps 2-7 are specially named as Miller's loop. Steps 3, 5, 7 are the line evaluation together with elliptic curve doubling (ECD) and addition (ECA) inside the Miller's loop and steps 9, 11 are the line evaluation. These line evaluation steps are the key steps to accelerate the loop calculation. The authors extended the work of [23],[20] for KSS-16 curve to calculate *pseudo 8-sparse multiplication* described in Sect. 3. The ECA and ECD are also calculated efficiently in the twisted curve. The $Q_2 \leftarrow [p]Q$ term of step 8 is calculated by applying one skew Frobenius map over $\mathbb{F}_{p^4}$ and $f_1 \leftarrow f^{p^3}$ of step 10 is calculated by applying one Frobenius map in

$\mathbb{F}_{p^{16}}$. Step 12, FE is calculated by applying Ghammam et al.'s work for KSS-16 curve [16].

Algorithm 1: Optimal Ate pairing on KSS-16 curve

Input: $u, P \in \mathbb{G}_1, Q \in \mathbb{G}_2'$
Output: (Q, P)
1 $f \leftarrow 1, T \leftarrow Q$
2 **for** $i = \lfloor \log_2(u) \rfloor$ **downto** 1 **do**
3 $\quad f \leftarrow f^2 \cdot l_{T,T}(P)$, $T \leftarrow [2]T$
4 $\quad$ **if** $u[i] = 1$ **then**
5 $\quad\quad f \leftarrow f \cdot l_{T,Q}(P)$, $T \leftarrow T + Q$
6 $\quad$ **if** $u[i] = -1$ **then**
7 $\quad\quad f \leftarrow f \cdot l_{T,-Q}(P)$, $T \leftarrow T - Q$
8 $Q_1 \leftarrow [u]Q$, $Q_2 \leftarrow [p]Q$
9 $f \leftarrow f \cdot l_{Q_1,Q_2}(P)$
10 $f_1 \leftarrow f^{p^3}$, $f \leftarrow f \cdot f_1$
11 $f \leftarrow f \cdot l_{Q,Q}(P)$
12 $f \leftarrow f^{\frac{p^{16}-1}{r}}$
13 **return** f

2.4 Twist of KSS-16 Curves

In the context of Type 3 pairing, there exists a *twisted curve* with a group of rational points of order r, isomorphic to the group where rational point $Q \in E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\pi_p - [p])$ belongs to. This sub-field isomorphic rational point group includes a twisted isomorphic point of Q, typically denoted as $Q' \in E'(\mathbb{F}_{p^{k/d}})$, where k is the embedding degree and d is the twist degree.

Since points on the twisted curve are defined over a smaller field than $\mathbb{F}_{p^k}$, therefore ECA and ECD become faster. However, when required in the Miller's algorithm's line evaluation, the points can be quickly mapped to points on $E(\mathbb{F}_{p^k})$. Since the pairing-friendly KSS-16 [19] curve has CM discriminant of $D = 1$ and $4|k$; therefore, quartic twist is available.

Quartic twist Let β be a certain quadratic non-residue in $\mathbb{F}_{p^4}$. The quartic twisted curve E' of KSS-16 curve E defined in Eq. (1) and their isomorphic mapping ψ_4 are given as follows:

$$\begin{aligned} &E' : y^2 = x^3 + ax\beta^{-1}, \quad a \in \mathbb{F}_p, \\ &\psi_4 : E'(\mathbb{F}_{p^4})[r] \longmapsto E(\mathbb{F}_{p^{16}})[r] \cap \mathrm{Ker}(\pi_p - [p]), \\ &\qquad (x, y) \longmapsto (\beta^{1/2}x, \beta^{3/4}y), \end{aligned} \tag{8}$$

where $\mathrm{Ker}(\cdot)$ denotes the kernel of the mapping and π_p denotes Frobenius mapping for rational point.

Table 4. Vector representation of $Q = (x_Q, y_Q) \in \mathbb{G}_2 \subset \mathbb{F}_{p^{16}}$

	1	α	β	$\alpha\beta$	γ	$\alpha\gamma$	$\beta\gamma$	$\alpha\beta\gamma$	ω	$\alpha\omega$	$\beta\omega$	$\alpha\beta\omega$	$\gamma\omega$	$\alpha\gamma\omega$	$\beta\gamma\omega$	$\alpha\beta\gamma\omega$
x_Q	0	0	0	0	b_4	b_5	b_6	b_7	0	0	0	0	0	0	0	0
y_Q	0	0	0	0	0	0	0	0	0	0	0	0	b_{12}	b_{13}	b_{14}	b_{15}

Table 4 shows the vector representation of $Q = (x_Q, y_Q) = (\beta^{1/2} x_{Q'}, \beta^{3/4} y_{Q'}) \in \mathbb{F}_{p^{16}}$ according to the given towering in Eq. (3). Here, $x_{Q'}$ and $y_{Q'}$ are the coordinates of rational point Q' on quartic twisted curve E'.

3 Proposal

3.1 Overview: Sparse and Pseudo-Sparse Multiplication

Aranha et al. [1, Section 4] and Costello et al. [10] have well optimized the Miller's algorithm in Jacobian coordinates by 6-sparse multiplication [4] for BN curve. Mori et al. [23] have shown the pseudo 8-sparse multiplication [5] for BN curve by adapting affine coordinates where the sextic twist is available. It is found that pseudo 8-sparse was efficient than 7-sparse and 6-sparse in Jacobian coordinates.

Let us consider $T = (\gamma x_{T'}, \gamma\omega y_{T'})$, $Q = (\gamma x_{Q'}, \gamma\omega y_{Q'})$ and $P = (x_P, y_P)$, where $x_p, y_p \in \mathbb{F}_p$ given in affine coordinates on the curve $E(\mathbb{F}_{p^{16}})$ such that $T' = (x_{T'}, y_{T'})$, $Q' = (x_{Q'}, y_{Q'})$ are in the twisted curve E' defined over $\mathbb{F}_{p^4}$. Let the elliptic curve doubling of $T + T = R(x_R, y_R)$. The 7-sparse multiplication for KSS-16 can be derived as follows.

$$l_{T,T}(P) = (y_p - y_{T'}\gamma\omega) - \lambda_{T,T}(x_P - x_{T'}\gamma), \quad \text{when } T = Q,$$
$$\lambda_{T,T} = \frac{3x_{T'}^2\gamma^2 + a}{2y_{T'}\gamma\omega} = \frac{3x_{T'}^2\gamma\omega^{-1} + a(\gamma\omega)^{-1}}{2y_{T'}} = \frac{(3x_{T'}^2 + ac^{-1}\alpha\beta)\omega}{2y_{T'}} = \lambda'_{T,T}\omega,$$
$$\text{since } \gamma\omega^{-1} = \omega, (\gamma\omega)^{-1} = \omega\beta^{-1}, \quad \text{and}$$
$$a\beta^{-1} = (a + 0\alpha + 0\beta + 0\alpha\beta)\beta^{-1} = a\beta^{-1} = ac^{-1}\alpha\beta, \quad \text{where } \alpha^2 = c.$$

Now the line evaluation and ECD are obtained as follows:

$$l_{T,T}(P) = y_p - x_p\lambda'_{T,T}\omega + (x_{T'}\lambda'_{T,T} - y_{T'})\gamma\omega,$$
$$x_{2T'} = (\lambda'_{T,T})^2\omega^2 \ - 2x_{T'}\gamma = ((\lambda'_{T,T})^2 \ - 2x_{T'})\gamma$$
$$y_{2T'} = (x_{T'}\gamma - x_{2T'}\gamma)\lambda'_{T,T}\omega - y_{T'}\gamma\omega = (x_{T'}\lambda'_{T,T} - x_{2T'}\lambda'_{T,T} - y_{T'})\gamma\omega.$$

[4] 6-Sparse refers the state when in a vector (multiplier/multiplicand), among the 12 coefficients 6 of them are zero.

[5] Pseudo 8-sparse refers to a certain length of vector's coefficients where instead of 8 zero coefficients, there are seven 0's and one 1 as coefficients.

The above calculations can be optimized as follows:

$$A = \frac{1}{2y_{T'}}, B = 3x_{T'}^2 + ac^{-1}, C = AB, D = 2x_{T'}, x_{2T'} = C^2 - D,$$
$$E = Cx_{T'} - y_{T'}, y_{2T'} = E - Cx_{2T'},$$
$$l_{T,T}(P) = y_P + E\gamma\omega - Cx_P\omega = y_P + F\omega + E\gamma\omega, \tag{9}$$

where $F = -Cx_P$.

The elliptic curve addition phase ($T \neq Q$) and line evaluation of $l_{T,Q}(P)$ can also be optimized similar to the above procedure. Let the elliptic curve addition of $T + Q = R(x_R, y_R)$.

$$l_{T,Q}(P) = (y_p - y_{T'}\gamma\omega) - \lambda_{T,Q}(x_P - x_{T'}\gamma), \quad T \neq Q,$$
$$\lambda_{T,Q} = \frac{(y_{Q'} - y_{T'})\gamma\omega}{(x_{Q'} - x_{T'})\gamma} = \frac{(y_{Q'} - y_{T'})\omega}{x_{Q'} - x_{T'}} = \lambda'_{T,Q}\omega,$$
$$x_R = (\lambda'_{T,Q})^2\omega^2 \ - x_{T'}\gamma - x_{Q'}\gamma = ((\lambda'_{T,Q})^2 \ - x_{T'} - x_{Q'})\gamma$$
$$y_R = (x_{T'}\gamma - x_R\gamma)\lambda'_{T,Q}\omega - y_{T'}\gamma\omega = (x_{T'}\lambda'_{T,Q} - x_{R'}\lambda'_{T,Q} - y_{T'})\gamma\omega.$$

Representing the above line equations using variables as following :

$$A = \frac{1}{x_{Q'} - x_{T'}}, B = y_{Q'} - y_{T'}, C = AB, D = x_{T'} + x_{Q'},$$
$$x_{R'} = C^2 - D, E = Cx_{T'} - y_{T'}, y_{R'} = E - Cx_{R'},$$
$$l_{T,Q}(P) = y_P + E\gamma\omega - Cx_P\omega = y_P + F\omega + E\gamma\omega, \tag{10}$$
$$F = -Cx_P,$$

Here all the variables (A, B, C, D, E, F) are calculated as $\mathbb{F}_{p^4}$ elements. The position of the y_P, E and F in $\mathbb{F}_{p^{16}}$ vector representation is defined by the basis element 1, $\gamma\omega$ and ω as shown in Table 4. Therefore, among the 16 coefficients of $l_{T,T}(P)$ and $l_{T,Q}(P) \in \mathbb{F}_{p^{16}}$, only 9 coefficients $y_P \in \mathbb{F}_p$, $Cx_P \in \mathbb{F}_{p^4}$ and $E \in \mathbb{F}_{p^4}$ are non-zero. The remaining 7 zero coefficients leads to an efficient multiplication, usually called sparse multiplication. This particular instance in KSS-16 curve is named as 7-sparse multiplication.

3.2 Pseudo 8-Sparse Multiplication for BN and BLS-12 Curve

Here we have followed Mori et al.'s [23] procedure to derive pseudo 8-sparse multiplication for the parameter settings of [3] for BN and BLS-12 curves. For the new parameter settings, the towering is given as Eq. (4) for both BN and BLS-12 curve. However, the curve form $E : y^2 = x^3 + b, \ b \in \mathbb{F}_p$ is identical for both BN and BLS-12 curve. The sextic twist obtained for these curves are also identical. Therefore, in what follows this paper will denote both of them as E_b defined over $\mathbb{F}_{p^{12}}$.

Sextic twist of BN and BLS-12 curve: Let $(\alpha + 1)$ be a certain quadratic and cubic non-residue in $\mathbb{F}_{p^2}$. The sextic twisted curve E'_b of curve E_b and their

Table 5. Vector representation of $Q = (x_Q, y_Q) \in \mathbb{G}_2 \subset \mathbb{F}_{p^{12}}$ vector representation

	1	α	β	$\alpha\beta$	β^2	$\alpha\beta^2$	γ	$\alpha\gamma$	$\beta\gamma$	$\alpha\beta\gamma$	$\beta^2\gamma$	$\alpha\beta^2\gamma$
x_Q	0	0	0	0	b_4	b_5	0	0	0	0	0	0
y_Q	0	0	0	0	0	0	0	0	b_8	b_9	0	0

isomorphic mapping ψ_6 are given as follows:

$$\begin{aligned} E'_b &: y^2 = x^3 + b(\alpha+1), \quad b \in \mathbb{F}_p, \\ \psi_6 &: E'_b(\mathbb{F}_{p^2})[r] \longmapsto E_b(\mathbb{F}_{p^{12}})[r] \cap \mathrm{Ker}(\pi_p - [p]), \\ &(x, y) \longmapsto ((\alpha+1)^{-1}x\beta, (\alpha+1)^{-1}y\beta^2\gamma). \end{aligned} \tag{11}$$

The line evaluation and ECD/ECA can be obtained in affine coordinate for the rational point P and $Q', T' \in E'_b(\mathbb{F}_{p^2})$ as follows:

Elliptic curve addition when $T' \neq Q'$ and $T' + Q' = R'(x_{R'}, y_{R'})$

$$\begin{aligned} A = \tfrac{1}{x_{Q'} - x_{T'}}, B = y_{Q'} - y_{T'}, C = AB, D = x_{T'} + x_{Q'}, \\ x_{R'} = C^2 - D, E = Cx_{T'} - y_{T'}, y_{R'} = E - Cx_{R'}, \\ l_{T',Q'}(P) = y_P + (\alpha+1)^{-1}E\beta\gamma - (\alpha+1)^{-1}Cx_P\beta^2\gamma, \qquad (12a) \\ y_P^{-1}l_{T',Q'}(P) = 1 + (\alpha+1)^{-1}Ey_P^{-1}\beta\gamma - (\alpha+1)^{-1}Cx_Py_P^{-1}\beta^2\gamma, \qquad (12b) \end{aligned}$$

Elliptic curve doubling when $T' = Q'$

$$\begin{aligned} A = \tfrac{1}{2y_{T'}}, B = 3x_{T'}^2, C = AB, D = 2x_{T'}, x_{2T'} = C^2 - D, \\ E = Cx_{T'} - y_{T'}, y_{2T'} = E - Cx_{2T'}, \\ l_{T',T'}(P) = y_P + (\alpha+1)^{-1}E\beta\gamma - (\alpha+1)^{-1}Cx_P\beta^2\gamma, \qquad (13a) \\ y_P^{-1}l_{T',T'}(P) = 1 + (\alpha+1)^{-1}Ey_P^{-1}\beta\gamma - (\alpha+1)^{-1}Cx_Py_P^{-1}\beta^2\gamma, \qquad (13b) \end{aligned}$$

The line evaluations of Eq. (12b) and Eq. (13b) are identical and more sparse than Eq. (12a) and Eq. (13a). Such sparse form comes with a cost of computation overhead. But such overhead can be minimized by the following isomorphic mapping, which also accelerates the Miller's loop iteration.

Isomorphic mapping of $P \in \mathbb{G}_1 \mapsto \hat{P} \in \mathbb{G}'_1$:

$$\begin{aligned} \hat{E} &: y^2 = x^3 + b\hat{z}, \\ &\hat{E}(\mathbb{F}_p)[r] \longmapsto E(\mathbb{F}_p)[r], \\ &(x, y) \longmapsto (\hat{z}^{-1}x, \hat{z}^{-3/2}y), \end{aligned} \tag{14}$$

where $\hat{z} \in \mathbb{F}_p$ is a quadratic and cubic residue in $\mathbb{F}_p$. Eq. (14) maps rational point P to $\hat{P}(x_{\hat{P}}, y_{\hat{P}})$ such that $(x_{\hat{P}}, y_{\hat{P}}^{-1}) = 1$. The twist parameter $\hat{z}$ is obtained as:

$$\hat{z} = (x_P y_P^{-1})^6. \tag{15}$$

From the Eq. (15) $\hat{P}$ and $\hat{Q'}$ is given as

$$\hat{P}(x_{\hat{P}}, y_{\hat{P}}) = (x_P z^{-1}, y_P z^{-3/2}) = (x_P^3 y_P^{-2}, x_P^3 y_P^{-2}), \tag{16a}$$

$$\hat{Q'}(x_{\hat{Q'}}, y_{\hat{Q'}}) = (x_P^2 y_P^{-2} x_{Q'}, x_P^3 y_P^{-3} y_{Q'}). \tag{16b}$$

Using Eq. (16a) and Eq. (16b) the line evaluation of Eq. (13b) becomes

$$y_{\hat{P}}^{-1} l_{\hat{T'},\hat{T'}}(\hat{P}) = 1 + (\alpha+1)^{-1} E y_{\hat{P}}^{-1} \beta\gamma - (\alpha+1)^{-1} C x_{\hat{P}} y_{\hat{P}}^{-1} \beta^2\gamma,$$

$$\hat{l}_{\hat{T'},\hat{T'}}(\hat{P}) = 1 + (\alpha+1)^{-1} E y_{\hat{P}}^{-1} \beta\gamma - (\alpha+1)^{-1} C \beta^2\gamma. \tag{17a}$$

The Eq. (12b) becomes similar to Eq. (17a). The calculation overhead can be reduced by pre-computation of $(\alpha+1)^{-1}$, $y_{\hat{P}}^{-1}$ and $\hat{P}$, $\hat{Q'}$ mapping using x_P^{-1} and y_P^{-1} as shown by Mori et al. [23].

Finally, pseudo 8-sparse multiplication for BN and BLS-12 is given in

Algorithm 2: Pseudo 8-sparse multiplication for BN and BLS-12 curves

Input: $a, b \in \mathbb{F}_{p^{12}}$
$a = (a_0 + a_1\beta + a_2\beta^2) + (a_3 + a_4\beta + a_5\beta^2)\gamma$, $b = 1 + b_4\beta\gamma + b_5\beta^2\gamma$
where $a_i, b_j, c_i \in \mathbb{F}_{p^2} (i = 0, \cdots, 5, j = 4, 5)$
Output: $c = ab = (c_0 + c_1\beta + c_2\beta^2) + (c_3 + c_4\beta + c_5\beta^2)\gamma \in \mathbb{F}_{p^{12}}$
1 $c_4 \leftarrow a_0 \times b_4$, $t_1 \leftarrow a_1 \times b_5$, $t_2 \leftarrow a_0 + a_1$, $S_0 \leftarrow b_4 + b_5$
2 $c_5 \leftarrow t_2 \times S_0 - (c_4 + t_1)$, $t_2 \leftarrow a_2 \times b_5$, $t_2 \leftarrow t_2 \times (\alpha + 1)$
3 $c_4 \leftarrow c_4 + t_2$, $t_0 \leftarrow a_2 \times b_4$, $t_0 \leftarrow t_0 + t_1$
4 $c_3 \leftarrow t_0 \times (\alpha + 1)$, $t_0 \leftarrow a_3 \times b_4$, $t_1 \leftarrow a_4 \times b_5$, $t_2 \leftarrow a_3 + a_4$
5 $t_2 \leftarrow t_2 \times S_0 - (t_0 + t_1)$
6 $c_0 \leftarrow t_2 \times (\alpha + 1)$, $t_2 \leftarrow a_5 \times b_4$, $t_2 \leftarrow t_1 + t_2$
7 $c_1 \leftarrow t_2 \times (\alpha + 1)$, $t_1 \leftarrow a_5 \times b_5$, $t_1 \leftarrow t_1 \times (\alpha + 1)$
8 $c_2 \leftarrow t_0 + t_1$
9 $c \leftarrow c + a$
10 return $c = (c_0 + c_1\beta + c_2\beta^2) + (c_3 + c_4\beta + c_5\beta^2)\gamma$

3.3 Pseudo 8-sparse Multiplication for KSS-16 Curve

The main idea of *pseudo 8-sparse multiplication* is finding more sparse form of Eq. (9) and Eq. (10), which allows to reduce the number of multiplication of $\mathbb{F}_{p^{16}}$ vector during Miller's algorithm evaluation. To obtains the same, y_P^{-1} is multiplied to both side of Eq. (9) and Eq. (10), since y_P remains the same through the Miller's algorithms loop calculation.

$$y_P^{-1} l_{T,P}(P) = 1 - C x_P y_P^{-1} \omega + E y_P^{-1} \gamma\omega, \tag{18a}$$

$$y_P^{-1} l_{T,Q}(P) = 1 - C x_P y_P^{-1} \omega + E y_P^{-1} \gamma\omega, \tag{18b}$$

Although the Eq. (18a) and Eq. (18b) do not get more sparse, but 1st coefficient becomes 1. Such vector is titled as *pseudo sparse form* in this paper. This

form realizes more efficient $\mathbb{F}_{p^{16}}$ vectors multiplication in Miller's loop. However, the Eq. (18b) creates more computation overhead than Eq. (10), i.e., computing $y_P^{-1} l_{T,Q}(P)$ in the left side and $x_P y_P^{-1}$, $E y_P^{-1}$ on the right. The same goes between Eq. (18a) and Eq. (9). Since the computation of Eq. (18a) and Eq. (18b) are almost identical, therefore the rest of the paper shows the optimization technique for Eq. (18a). To overcome these overhead computations, the following techniques can be applied.

- $x_P y_P^{-1}$ is omitted by applying further isomorphic mapping of $P \in \mathbb{G}_1$.
- y_P^{-1} can be pre-computed. Therefore, the overhead calculation of $E y_P^{-1}$ will cost only 2 $\mathbb{F}_p$ multiplication.
- $y_P^{-1} l_{T,T}(P)$ doesn't effect the pairing calculation cost since the final exponentiation cancels this multiplication by $y_P^{-1} \in \mathbb{F}_p$.

To overcome the $C x_P y_P^{-1}$ calculation cost, $x_P y_P^{-1} = 1$ is expected. To obtain $x_P y_P^{-1} = 1$, the following isomorphic mapping of $P = (x_P, y_P) \in \mathbb{G}_1$ is introduced.

Isomorphic map of $\boldsymbol{P = (x_P, y_P) \rightarrow \bar{P} = (x_{\bar{P}}, y_{\bar{P}})}$. Although the KSS-16 curve is typically defined over $\mathbb{F}_{p^{16}}$ as $E(\mathbb{F}_{p^{16}})$, but for efficient implementation of Optimal-Ate pairing, certain operations are carried out in a quartic twisted isomorphic curve E' defined over $\mathbb{F}_{p^4}$ as shown in Sec. 2.4. For the same, let us consider $\bar{E}(\mathbb{F}_{p^4})$ is isomorphic to $E(\mathbb{F}_{p^4})$ and certain $z \in \mathbb{F}_p$ as a quadratic residue (QR) in $\mathbb{F}_{p^4}$. A generalized mapping between $E(\mathbb{F}_{p^4})$ and $\bar{E}(\mathbb{F}_{p^4})$ can be given as follows:

$$\begin{aligned} \bar{E} : y^2 &= x^3 + az^{-2}x, \\ \bar{E}(\mathbb{F}_{p^4})[r] &\longmapsto E(\mathbb{F}_{p^4})[r], \\ (x, y) &\longmapsto (z^{-1}x, z^{-3/2}y), \\ &\textbf{where } z, z^{-1}, z^{-3/2} \in \mathbb{F}_p. \end{aligned} \tag{19}$$

The mapping considers $z \in \mathbb{F}_p$ is a quadratic residue over $\mathbb{F}_{p^4}$ which can be shown by the fact that $z^{(p^4-1)/2} = 1$ as follows:

$$\begin{aligned} z^{(p^4-1)/2} &= z^{(p-1)(p^3+p^2+p+1)/2} \\ &= 1^{(p^3+p^2+p+1)/2} \\ &= 1 \quad \text{QR} \in \mathbb{F}_{p^4} \ . \end{aligned} \tag{20}$$

Therefore, z is a quadratic residue over $\mathbb{F}_{p^4}$.
Now based on $P = (x_P, y_P)$ be the rational point on curve E, the considered isomorphic mapping of Eq. (19) can find a certain isomorphic rational point $\bar{P} = (x_{\bar{P}}, y_{\bar{P}})$ on curve $\bar{E}$ as follows:

$$\begin{aligned} y_P^2 &= x_P^3 + ax_P, \\ y_P^2 z^{-3} &= x_P^3 z^{-3} + ax_P z^{-3}, \\ (y_P z^{-3/2})^2 &= (x_P z^{-1})^3 + az^{-2} x_P z^{-1}, \end{aligned} \tag{21}$$

where $\bar{P} = (x_{\bar{P}}, y_{\bar{P}}) = (x_P z^{-1}, y_P z^{-3/2})$ and the general form of the curve $\bar{E}$ is given as follows:

$$y^2 = x^3 + az^{-2}x. \tag{22}$$

To obtain the target relation $x_{\bar{P}} y_{\bar{P}}^{-1} = 1$ from above isomorphic map and rational point $\bar{P}$, let us find isomorphic twist parameter z as follows:

$$\begin{aligned} x_{\bar{P}} y_{\bar{P}}^{-1} &= 1 \\ z^{-1} x_P (z^{-3/2} y_P)^{-1} &= 1 \\ z^{1/2} (x_P . y_P^{-1}) &= 1 \\ z &= (x_P^{-1} y_P)^2. \end{aligned} \tag{23}$$

Now using $z = (x_P^{-1} y_P)^2$ and Eq. (21), $\bar{P}$ can be obtained as

$$\bar{P}(x_{\bar{P}}, y_{\bar{P}}) = (x_P z^{-1}, y_P z^{-3/2}) = (x_P^3 y_P^{-2}, x_P^3 y_P^{-2}), \tag{24}$$

where the x and y coordinates of $\bar{P}$ are equal. For the same isomorphic map we can obtain $\bar{Q}$ on curve $\bar{E}$ defined over $\mathbb{F}_{p^{12}}$ as follows:

$$\bar{Q}(x_{\bar{Q}}, y_{\bar{Q}}) = (z^{-1} x_{Q'} \gamma, z^{-3/2} y_{Q'} \gamma \omega), \tag{25}$$

where from Eq. (8), $Q'(x_{Q'}, y_{Q'})$ is obtained in quartic twisted curve E'.

At this point, to use $\bar{Q}$ with $\bar{P}$ in line evaluation we need to find another isomorphic map that will map $\bar{Q} \mapsto \bar{Q}'$, where $\bar{Q}'$ is the rational point on curve $\bar{E}'$ defined over $\mathbb{F}_{p^4}$. Such $\bar{Q}'$ and $\bar{E}'$ can be obtained from $\bar{Q}$ of Eq. (25) and curve $\bar{E}$ from Eq. (22) as follows:

$$\begin{aligned} (z^{-3/2} y_{Q'} \gamma \omega)^2 &= (z^{-1} x_{Q'} \gamma)^3 + a z^{-2} z^{-1} x_{Q'} \gamma, \\ (z^{-3/2} y_{Q'})^2 \gamma^2 \omega^2 &= (z^{-1} x_{Q'})^3 \gamma^3 + a z^{-2} z^{-1} x_{Q'} \gamma, \\ (z^{-3/2} y_{Q'})^2 \beta \gamma &= (z^{-1} x_{Q'})^3 \beta \gamma + a z^{-2} z^{-1} x_{Q'} \gamma, \\ (z^{-3/2} y_{Q'})^2 &= (z^{-1} x_{Q'})^3 + a z^{-2} \beta^{-1} z^{-1} x_{Q'}. \end{aligned}$$

From the above equations, $\bar{E}'$ and $\bar{Q}'$ are given as,

$$\bar{E}' : \; y_{\bar{Q}'}^2 = x_{\bar{Q}'}^3 + a(z^2\beta)^{-1} x_{\bar{Q}'}. \tag{26}$$

$$\begin{aligned} \bar{Q}'(x_{\bar{Q}'}, y_{\bar{Q}'}) &= (z^{-1} x_{Q'}, z^{-3/2} y_{Q'}) \\ &= (x_{Q'} x_P^2 y_P^{-2}, y_{Q'} x_P^3 y_P^{-3}). \end{aligned} \tag{27}$$

Now, applying $\bar{P}$ and $\bar{Q}'$, the line evaluation of Eq. (18b) becomes as follows:

$$\begin{aligned} y_{\bar{P}}^{-1} l_{\bar{T}', \bar{Q}'}(\bar{P}) &= 1 - C(x_{\bar{P}} y_{\bar{P}}^{-1})\gamma + E y_{\bar{P}}^{-1} \gamma \omega \\ \bar{l}_{\bar{T}', \bar{Q}'}(\bar{P}) &= 1 - C\gamma + E(x_P^{-3} y_P^2)\gamma\omega, \end{aligned} \tag{28}$$

where $x_{\bar{P}} y_{\bar{P}}^{-1} = 1$ and $y_{\bar{P}}^{-1} = z^{3/2} y_P^{-1} = (x_P^{-3} y_P^2)$. The Eq. (18a) becomes the same as Eq. (28). Compared to Eq. (18b), the Eq. (28) will be faster while using in Miller's loop in combination of the pseudo 8-sparse multiplication shown in Alg.2. However, to get the above form, we need the following pre-computations once in every Miller's Algorithm execution.

– Computing $\bar{P}$ and $\bar{Q}'$,
– $(x_P^{-3} y_P^2)$ and
– z^{-2} term from curve $\bar{E}'$ of Eq. (26).

The above terms can be computed from x_P^{-1} and y_P^{-1} by utilizing Montgomery trick [22], as shown in Alg. 3. The pre-computation requires 21 multiplication, 2 squaring and 1 inversion in $\mathbb{F}_p$ and 2 multiplication, 3 squaring in $\mathbb{F}_{p^4}$.

Algorithm 3: Pre-calculation and mapping $P \mapsto \bar{P}$ and $Q' \mapsto \bar{Q}'$

Input: $P = (x_P, y_P) \in \mathbb{G}_1, Q' = (x_{Q'}, y_{Q'}) \in \mathbb{G}_2'$
Output: $\bar{Q}', \bar{P}, y_P^{-1}, (z)^{-2}$
1 $A \leftarrow (x_P y_P)^{-1}$
2 $B \leftarrow A x_P^2$
3 $C \leftarrow A y_P$
4 $D \leftarrow B^2$
5 $x_{\bar{Q}'} \leftarrow D x_{Q'}$
6 $y_{\bar{Q}'} \leftarrow BD y_{Q'}$
7 $x_{\bar{P}}, y_{\bar{P}} \leftarrow D x_P$
8 $y_P^{-1} \leftarrow C^3 y_P^2$
9 $z^{-2} \leftarrow D^2$
10 **return** $\bar{Q}' = (x_{\bar{Q}'}, y_{\bar{Q}'}), \bar{P} = (x_{\bar{P}}, y_{\bar{P}}), y_P^{-1}, z^{-2}$

The overall mapping and the curve obtained in the twisting process is shown in the Fig. 1.

Finally the Alg.4 shows the derived pseudo 8-sparse multiplication.

Algorithm 4: Pseudo 8-sparse multiplication for KSS-16 curve

Input: $a, b \in \mathbb{F}_{p^{16}}$
$a = (a_0 + a_1\gamma) + (a_2 + a_3\gamma)\omega$, $b = 1 + (b_2 + b_3\gamma)\omega$
$a = (a_0 + a_1\omega + a_2\omega^2 + a_3\omega^3)$, $b = 1 + b_2\omega + b_3\omega^3$
Output: $c = ab = (c_0 + c_1\gamma) + (c_3 + c_4\gamma)\omega \in \mathbb{F}_{p^{16}}$
1 $t_0 \leftarrow a_3 \times b_3 \times \beta, t_1 \leftarrow a_2 \times b_2, t_4 \leftarrow b_2 + b_3, c_0 \leftarrow (a_2 + a_3) \times t_4 - t_1 - t_0$
2 $c_1 \leftarrow t_1 + t_0 \times \beta$
3 $t_2 \leftarrow a_1 \times b_3, t_3 \leftarrow a_0 \times b_2, c_2 \leftarrow t_3 + t_2 \times \beta$
4 $t_4 \leftarrow (b_2 + b_3), c_3 \leftarrow (a_0 + a_1) \times t_4 - t_3 - t_2$
5 $c \leftarrow c + a$
6 return $c = (c_0 + c_1\gamma) + (c_3 + c_4\gamma)\omega$

3.4 Final Exponentiation

Scott et al. [27] show the process of efficient final exponentiation (FE) $f^{p^k - 1/r}$ by decomposing the exponent using cyclotomic polynomial Φ_k as

$$(p^k - 1)/r = (p^{k/2} - 1) \cdot (p^{k/2} + 1)/\Phi_k(p) \cdot \Phi_k(p)/r \tag{29}$$

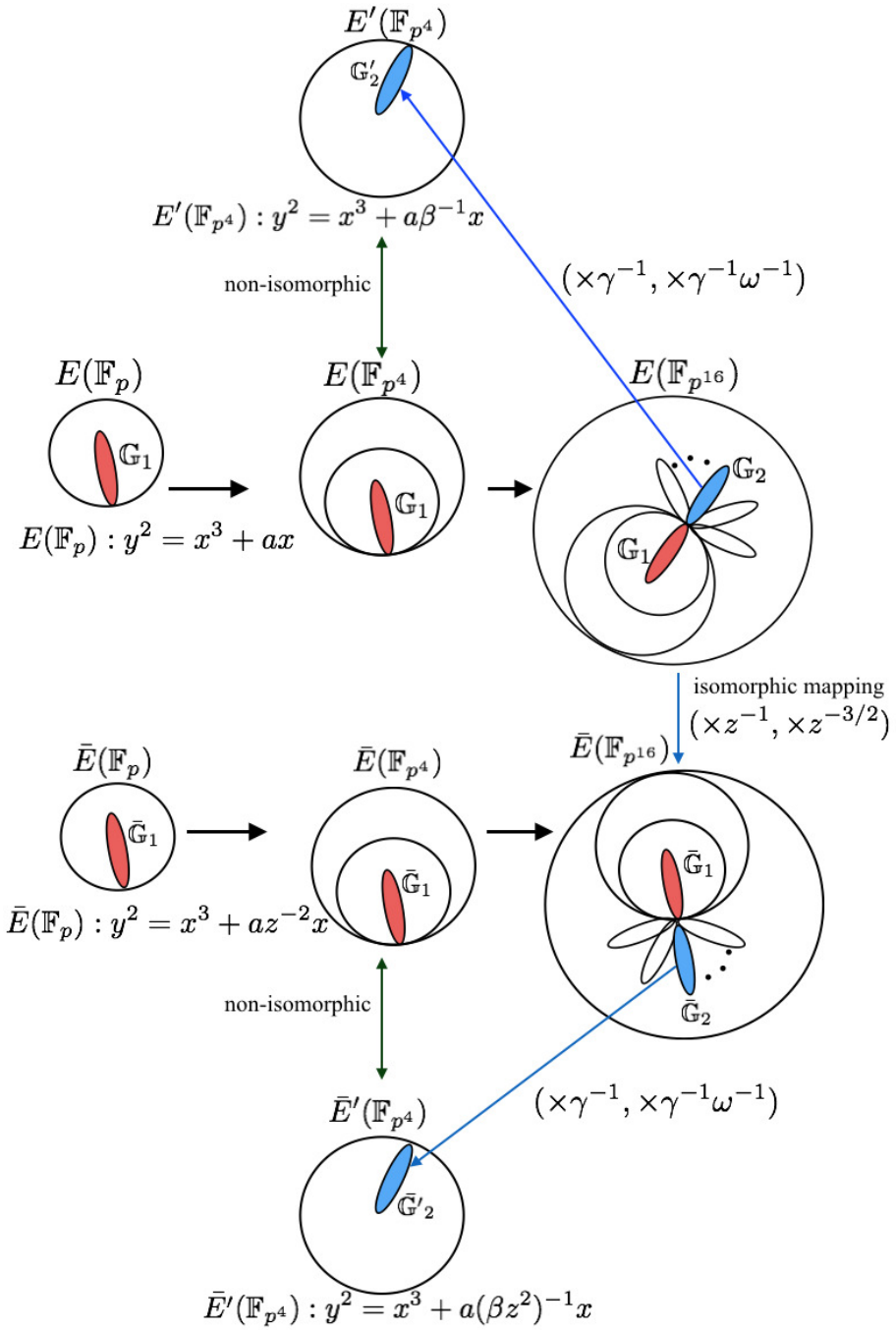

Fig. 1. Overview of the twisting process to get pseudo sparse form in KSS-16 curve.

The 1st two terms of the right part are denoted as easy part since it can be easily calculated by Frobenius mapping and one inversion in affine coordinates. The last term is called hard part which mostly affects the computation performance. According to Eq. (29), the exponent decomposition of the target curves is shown in Table 6.

Table 6. Exponents of final exponentiation in pairing

Curve	Final exponent	Easy part	Hard part
KSS-16	$\frac{p^{16}-1}{r}$	p^8-1	$\frac{p^8+1}{r}$
BN, BLS-12	$\frac{p^{12}-1}{r}$	$(p^6-1)(p^2+1)$	$\frac{p^4-p^2+1}{r}$

This paper carefully concentrates on Miller's algorithm for comparison and making pairing efficient. However, to verify the correctness of the bilinearity property, the authors made a "not state-of-art" implementation of Fuentes et al.'s work [14] for BN curve case and Ghammam's et al.'s works [16,17] for KSS-16 and BLS-12 curves. For scalar multiplication by prime p, i.e., $p[Q]$ or $[p^2]Q$, skew Frobenius map technique by Sakemi et al. [26] is adapted.

4 Experimental Result Evaluation

This section gives details of the experimental implementation. The source code can be found in Github[6]. The code is not an optimal code, and the sole purpose of it compare the Miller's algorithm among the curve families and validate the estimation of [3]. Table 7 shows implementation environment. Parameters

Table 7. Computational Environment

CPU*	Memory	Compiler	OS	Language	Library
Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz	4GB	GCC 5.4.0	Ubuntu 16.04 LTS	C	GMP v 6.1.0 [18]

*Only single core is used from two cores.

chosen from [3] is shown in Table 8. Table 9 shows execution time for Miller's algorithm implementation in millisecond for a single Optimal-Ate pairing. Results here are the average of 10 pairing operation. From the result, we find that Miller's algorithm took the least time for KSS-16. And the time is almost closer to BLS-12. The Miller's algorithm is about 1.7 times faster in KSS-16 than BN

[6] https://github.com/eNipu/pairingma128.git

Table 8. Selected parameters for 128-bit security level [3]

Curve	u	HW(u)	$\lfloor \log_2 u \rfloor$	$\lfloor \log_2 p(u) \rfloor$	$\lfloor \log_2 r(u) \rfloor$	$\lfloor \log_2 p^k \rfloor$
KSS-16	$u = 2^{35} - 2^{32} - 2^{18} + 2^8 + 1$	5	35	339	263	5424
BN	$u = 2^{114} + 2^{101} - 2^{14} - 1$	4	115	462	462	5535
BLS-12	$u = -2^{77} + 2^{50} + 2^{33}$	3	77	461	308	5532

Table 9. Comparative results of Miller's Algorithm in [ms].

	KSS-16	BN	BLS-12
Miller's Algorithm	4.41	7.53	4.91

curve. Table 12 shows that the complexity of this implementation concerning the number of $\mathbb{F}_p$ multiplication and squaring and the estimation of [3] are almost coherent for Miller's algorithm. Table 12 also show that our derived pseudo 8-sparse multiplication for KSS-16 takes fewer $\mathbb{F}_p$ multiplication than Zhang et al.'s estimation [31]. The execution time of Miller's algorithm also goes with this estimation [3], that means KSS-16 and BLS-12 are more efficient than BN curve. Table 10 shows the complexity of Miller's algorithm for the target curves in$\mathbb{F}_p$ operations count.

The operation counted in Table 10 are based on the counter in implementation code. For the implementation of big integer arithmetic `mpz_t` data type of GMP [18] library has been used. For example, multiplication between 2 `mpz_t` variables are counted as $\mathbb{F}_p$ multiplication and multiplication between one `mpz_t` and one "unsigned long" integer can also be treated as $\mathbb{F}_p$ multiplication. Basis multiplication refers to the vector multiplication such as $(a_o + a_1\alpha)\alpha$ where $a_0, a_1 \in \mathbb{F}_p$ and α is the basis element in $\mathbb{F}_{p^2}$.

Table 10. Complexity of this implementation in $\mathbb{F}_p$ for Miller's algorithm [single pairing operation]

	Multiplication		Squaring	Addition/ Subtraction	Basis Multiplication	Inversion
	mpz_t * mpz_t	mpz_t * ui				
KSS-16	6162	144	903	23956	3174	43
BN	10725	232	157	35424	3132	125
BLS-12	6935	154	113	23062	2030	80

As said before, this work is focused on Miller's algorithm. However, the authors made a "not state-of-art" implementation of some final exponentiation algorithms [16,14,17]. Table 11 shows the total final exponentiation time in [ms]. Here final exponentiation of KSS-16 is slower than BN and BLS-12. We have applied square and multiply technique for exponentiation by integer u in the hard part since the integer u given in the sparse form. However, Barbulescu et al. [3] mentioned that availability of compressed squaring [1] for KSS-16 will lead a fair comparison using final exponentiation.

Table 11. Final exponentiation time (not state-of-art) in [ms]

	KSS-16	BN	BLS-12
Final exponentiation	17.32	11.65	12.03

Table 12. Complexity comparison of Miller's algorithm between this implementation and Barbulescu et al.'s [3] estimation [Multiplication + Squaring in $\mathbb{F}_p$]

	KSS-16	BN	BLS-12
Barbulescu et al. [3]	$7534M_p$	$12068M_p$	$7708M_p$
This implementation	$7209M_p$	$11114M_p$	$7202M_p$

5 Conclusion and Future Work

This paper has presented two major ideas.

- Finding efficient Miller's algorithm implementation technique for Optimal-Ate pairing for the less studied KSS-16 curve. The author's presented pseudo 8-sparse multiplication technique for KSS-16. They also extended such multiplication for BN and BLS-12 according to [23] for the new parameter.
- Verifying Barbulescu and Duquesne's conclusion [3] for calculating Optimal-Ate pairing at 128-bit security level; that is, BLS-12 and less studied KSS-16 curves are more efficient choices than well studied BN curves for new parameters. This paper finds that Barbulescu and Duquesne's conclusion on BLS-12 is correct as it takes the less time for Miller's algorithm. Applying the derived pseudo 8-sparse multiplication, Miller's algorithm in KSS-16 is also more efficient than BN.

As a prospective work authors would like to evaluate the performance by finding compressed squaring for KSS-16's final exponentiation along with scalar multiplication of $\mathbb{G}_1$, $\mathbb{G}_2$ and exponentiation of $\mathbb{G}_T$. The execution time for the target

environment can be improved by a careful implementation using assembly language for prime field arithmetic.

Acknowledgment

This work was partially supported by the Strategic Information and Communications R&D Promotion Programme (SCOPE) of Ministry of Internal Affairs and Communications, Japan and The French projects ANR-16-CE39-0012 "SafeTLS" and ANR-11-LABX-0020-01 "Centre Henri Lebesgue".

References

1. Aranha, D.F., Karabina, K., Longa, P., Gebotys, C.H., López, J.: Faster explicit formulas for computing pairings over ordinary curves. In: Eurocrypt. vol. 6632, pp. 48–68. Springer (2011)
2. Bailey, D.V., Paar, C.: Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. Journal of cryptology 14(3), 153–176 (2001)
3. Barbulescu, R., Duquesne, S.: Updating key size estimations for pairings. Cryptology ePrint Archive, Report 2017/334 (2017), http://eprint.iacr.org/2017/334
4. Barreto, P.S., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: Security in Communication Networks, pp. 257–267. Springer (2002)
5. Barreto, P.S., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: International Workshop on Selected Areas in Cryptography, SAC 2005. pp. 319–331. Springer (2005)
6. Benger, N., Scott, M.: Constructing tower extensions of finite fields for implementation of pairing-based cryptography. In: Arithmetic of finite fields, pp. 180–195. Springer (2010)
7. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Advances in Cryptology–CRYPTO 2004. pp. 41–55. Springer (2004)
8. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Advances in CryptologyASIACRYPT 2001, pp. 514–532. Springer (2001)
9. Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of elliptic and hyperelliptic curve cryptography. CRC press (2005)
10. Costello, C., Lange, T., Naehrig, M.: Faster pairing computations on curves with high-degree twists. In: International Workshop on Public Key Cryptography. pp. 224–242. Springer (2010)
11. Devegili, A.J., O'hEigeartaigh, C., Scott, M., Dahab, R.: Multiplication and squaring on pairing-friendly fields. IACR Cryptology ePrint Archive 2006, 471 (2006)
12. Duquesne, S., Mrabet, N.E., Haloui, S., Rondepierre, F.: Choosing and generating parameters for low level pairing implementation on bn curves. Cryptology ePrint Archive, Report 2015/1212 (2015), http://eprint.iacr.org/2015/1212
13. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Journal of cryptology 23(2), 224–280 (2010)
14. Fuentes-Castañeda, L., Knapp, E., Rodríguez-Henríquez, F.: Faster hashing to ${\mathbb G}_2$. In: Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers. pp. 412–430 (2011), https://doi.org/10.1007/978-3-642-28496-0_25

15. Galbraith, S.D., Paterson, K.G., Smart, N.P.: Pairings for cryptographers. Discrete Applied Mathematics 156(16), 3113–3121 (2008)
16. Ghammam, L., Fouotsa, E.: Adequate elliptic curves for computing the product of n pairings. In: International Workshop on the Arithmetic of Finite Fields. pp. 36–53. Springer (2016)
17. Ghammam, L., Fouotsa, E.: On the computation of the optimal ate pairing at the 192-bit security level. Cryptology ePrint Archive, Report 2016/130 (2016), http://eprint.iacr.org/2016/130
18. Granlund, T., the GMP development team: GNU MP: The GNU Multiple Precision Arithmetic Library, 6.1.0 edn. (2015), http://gmplib.org
19. Kachisa, E., Schaefer, E., Scott, M.: Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field. Pairing-Based Cryptography–Pairing 2008 pp. 126–135 (2008)
20. Khandaker, M.A.A., Ono, H., Nogami, Y., Shirase, M., Duquesne, S.: An improvement of optimal ate pairing on KSS curve with pseudo 12-sparse multiplication. In: International Conference on Information Security and Cryptology. pp. 208–219. Springer (2016)
21. Kim, T., Barbulescu, R.: Extended tower number field sieve: A new complexity for the medium prime case. In: Advances in Cryptology - CRYPTO 2016 - Proceedings, Part I. pp. 543–571. Springer (2016)
22. Montgomery, P.L.: Speeding the pollard and elliptic curve methods of factorization. Mathematics of computation 48(177), 243–264 (1987)
23. Mori, Y., Akagi, S., Nogami, Y., Shirase, M.: Pseudo 8–sparse multiplication for efficient ate–based pairing on barreto–naehrig curve. In: Pairing-Based Cryptography–Pairing 2013, pp. 186–198. Springer (2013)
24. Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Annual Cryptology Conference. pp. 191–208. Springer (2010)
25. Sakai, R.: Cryptosystems based on pairing. In: The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, Jan. pp. 26–28 (2000)
26. Sakemi, Y., Nogami, Y., Okeya, K., Kato, H., Morikawa, Y.: Skew frobenius map and efficient scalar multiplication for pairing–based cryptography. In: International Conference on Cryptology and Network Security. pp. 226–239. Springer (2008)
27. Scott, M., Benger, N., Charlemagne, M., Perez, L.J.D., Kachisa, E.J.: On the final exponentiation for calculating pairings on ordinary elliptic curves. In: Pairing-Based Cryptography - Pairing 2009, Third International Conference, Palo Alto, CA, USA, August 12-14, 2009, Proceedings. pp. 78–88 (2009), https://doi.org/10.1007/978-3-642-03298-1_6
28. Silverman, J.H., Cornell, G., Artin, M.: Arithmetic geometry. Springer (1986)
29. Vercauteren, F.: Optimal pairings. Information Theory, IEEE Transactions on 56(1), 455–461 (2010)
30. Weil, A., et al.: Numbers of solutions of equations in finite fields. Bull. Amer. Math. Soc 55(5), 497–508 (1949)
31. Zhang, X., Lin, D.: Analysis of optimum pairing products at high security levels. In: Progress in Cryptology - INDOCRYPT 2012. pp. 412–430. Springer (2012)