Efficient Implementation of Super-optimal Pairings on Curves with Small Prime Fields at the 192-bit Security Level

Jianming Lin[1], Chang-An Zhao[1,2], and Yuhao Zheng[1]

[1] School of Mathematics, Sun Yat-sen University,
Guangzhou 510275, P.R.China
linjm28@mail2.sysu.edu.cn
zhaochan3@mail.sysu.edu.cn
zhengyh57@mail2.sysu.edu.cn
[2] Guangdong Key Laboratory of Information Security,
Guangzhou 510006, P.R. China

Abstract. For many pairing-based cryptographic protocols such as Direct Anonymous Attestation (DAA) schemes, the arithmetic on the first pairing subgroup $\mathbb{G}_1$ is more fundamental. Such operations heavily depend on the sizes of prime fields. At the 192-bit security level, Gasnier and Guillevic presented a curve named GG22D7-457 with CM-discriminant $D = 7$ and embedding degree $k = 22$. Compared to other well-known pairing-friendly curves at the same security level, the curve GG22D7-457 has smaller prime field size and ρ-value, which benefits from the fast operations on $\mathbb{G}_1$. However, the pairing computation on GG22D7-457 is not efficient. In this paper, we investigate to derive a higher performance for the pairing computation on GG22D7-457. We first propose novel formulas of the super-optimal pairing on this curve by utilizing a 2-isogeny as GLV-endomorphism. Besides, this tool can be generalized to more generic families of pairing-friendly curves with n-isogenies as endomorphisms. In our paper, we provide the explicit formulas for the super-optimal pairings exploiting $2, 3$-isogenies. Finally, we make a concrete computational cost analysis and implement the pairing computations on curve GG22D7-457 using our approaches. In terms of Miller function evaluation, employing the techniques in this paper obtain a saving of 24.44% in $\mathbb{F}_p$-multiplications compared to the optimal ate pairing. As for the running time, the experimental results illustrate that the Miller loop on GG22D7-457 by utilizing our methods is 26.0% faster than the state-of-the-art. Additionally, the performance of the super-optimal pairing on GG22D7-457 is competitive compared to the well-known pairing-friendly curves at the 192-bit security level. These results show that GG22D7-457 becomes an attractive candidate for the pairing-based protocols. Furthermore, our techniques have the potential to enhance the applications of super-optimal pairings on more pairing-friendly curves.

Keywords: Pairing-friendly curves optimal pairing super-optimal pairing isogeny DAA schemes

1 Introduction

In recent years, pairings become an important component of public-key cryptography due to their applications in various protocols such as identity-based encryption [5], short signature [6], key agreements [8,34,23] and SNARKs (Succinct Non-interactive ARguments of Knowledge) [12,11,1]. A pairing on an elliptic curve over a finite field $\mathbb{F}_p$ is an efficient non-degenerate bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, wherein the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ consist of the points on the curve E with prime order r. Furthermore, $\mathbb{G}_T$ is also an order-r subgroup of $\mathbb{F}_{p^k}^*$, where k denotes the embedding degree.

For practical purpose, pairing-friendly curves should be designed to offer both adequate security and high computational efficiency. The security of pairing-based protocols relies on the computational hardness of the Discrete Logarithm Problem (DLP). Pollard's rho algorithm [29] is regarded as the best-known method for solving ECDLP (Elliptic Curve Discrete Logarithm Problem), with a complexity of $\mathcal{O}(\sqrt{r})$. As for the finite field aspect, the best algorithm for DLP is NFS (Number Field Sieve) algorithm [31] and its variants. In 2016, Kim and Barbulescu [25] proposed the Extended Tower NFS algorithm (exTNFS), which can crucially reduce the complexity of DLP if the base field characteristic p can be represented as a polynomial and the embedding degree k is a composite number. Consequently, the corresponding size of parameter p associated with a composite number k should be enlarged to achieve the sufficient security level, resulting in a slower implementation of pairing computation. Several researches aim to update the parameters or construct new pairing-friendly curves [35,21] to make them reach the desired security levels under the exTNFS attack. Guillevic [21] gave an updated list of families of pairing-friendly curves at the 128-bit security level. As for the 192-bit security level, Aranha, Fotiadis and Guillevic investigated the pairing friendly curves resistant to the special TNFS algorithm in [2]. Gasnier and Guillevic [19] provided the updated parameters for the existing families, and generalized the KSS method [24] (named subfield method) to construct new complete families of embedding degrees of interest. For embedding degree $k = 22$, the authors introduced a new family named GG22D7 with CM discriminant $D = 7$ and $\rho = 1.2$ [19,2]. This family has several cryptographically-interesting properties. Compared to family FST 6.3 [16] with $D = 1$ and $\rho = 1.3$, GG22D7 possesses a smaller ρ-value, which is the best of all the families of pairing-friendly curves with $k = 22$ [19, Table 4]. Hence, it exhibits an efficient performance for hashing to the first pairing subgroup $\mathbb{G}_1$.

Several protocols are constructed to reduce the workload of one resource-constrained party. For example, the Enhanced Privacy ID (EPID) scheme [7] and the Trusted Platform Module (TPM) in DAA scheme [40] require to execute a few exponentiations in $\mathbb{G}_1$. Under the circumstances, pairing-friendly curves with fast operations in $\mathbb{G}_1$ are preferred. A curve of the family GG22D7, named GG22D7-457, is associated with the minimum prime field characteristic p of only 8 digits (457 bits) among the pairing-friendly curves at the 192-bit security level. Therefore, GG22D7-457 benefits from an efficient execution for the operations in $\mathbb{G}_1$ and is relevant for the DAA schemes. Besides, it is more competitive for the

full extension field arithmetic. Nevertheless, the performances of such schemes also depend on the pairing computations. Until now, GG22D7-457 does not match a comparable performance for pairing computations as some well-known 192-bit security level families such as AFG16, KSS18, FM18 or BLS24. Inspired by this, we aim to optimize the pairing computation on GG22D7-457 and fill the gap of performances between itself and the well-known curves, making it more benefit to be selected as a choice for the aforementioned pairing-based cryptographic schemes.

In [19], Gasnier and Guillevic utilized the techniques of optimal pairing [38] to obtain the formulas for pairing computation on GG22D7-457. It can be computed in $\log_2(r)/\varphi(k)$ Miller iterations [26]. Since there does not exist non-trivial efficiently-computable automorphism on GG22D7-457, the previous techniques in [30,15,10,9] can not be directly extended to this curve for shortening the length of Miller loop.

In this paper, we investigate that GG22D7-457 has a 2-isogeny as the GLV-endomorphism [18], which can be used to construct the super-optimal pairing. Our new formulas for the pairing computation with $\log_2(r)/2\varphi(k)$ Miller iterations is more efficient than the optimal ate pairing previously computed on GG22D7-457. Moreover, the techniques can not only speed up the pairing computation on curves equipped with 2-isogenies, but also be generalized to construct the formulas for the super-optimal pairing on more generic families of GLV-curves with n-isogenies as their endomorphisms.

1.1 Contributions

The contributions of this paper are summarized as follows:

1. We utilize $2, 3$-isogenies to shorten the length of the Miller loop of the optimal ate pairing. Especially, we present new formulas for the super-optimal pairing on family GG22D7. Furthermore, we provide concrete implementation details and cost analysis. For the computation of Miller loop, our techniques demonstrate savings of 24.44% in terms of $\mathbb{F}_p$-multiplications compared to the optimal pairing on the same 192-bit security level curve GG22D7-457. Our experimental results show that in terms of Miller loop, applying our super-optimal pairing formulas is 26.0% faster than exploiting the traditional optimal ate pairing. Therefore, our methods make GG22D7-457 become a competitive choice for the pairing-based cryptographic protocols.
2. We determine the curves which are compatible with $2, 3$-isogenies as GLV-endomorphisms, and provide an explicit analysis and formulas for the corresponding Miller loop computations. Besides, we generalize the above method to more generic GLV-curves with n-isogenies as their endomorphisms. Hence, our techniques can be potentially applied to extend the applications of super-optimal pairings on more pairing-friendly curves.

1.2 Organizations of this paper

The notations and definitions are stated in Section 2. The Miller algorithm and the optimal ate pairing are recalled. Our formulas for super-optimal pairings, along with a explicit theoretical analysis are presented in Section 3. Section 4 illustrates the concrete implementation details, computational cost analysis and experimental results. Finally, our conclusion and future work are drawn in Section 5.

2 Preliminaries

In this section, we introduce the corresponding mathematical preliminaries used in our results.

Let E be an ordinary elliptic curve defined over a finite field $\mathbb{F}_p$, where p ($p > 5$) is a prime. The additive group $E(\mathbb{F}_p)$ consists of points (x, y) satisfying the short Weierstrass equation:

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

with $x, y \in \mathbb{F}_p$, and a point at infinity $\mathcal{O}_E$. The j-invariant of E is defined as $j(E) = 1728 \cdot \frac{4a^3}{4a^3+27b^2}$. Denote by $\#E(\mathbb{F}_p)$ the cardinality of $E(\mathbb{F}_p)$. It is well-known that $\#E(\mathbb{F}_p)$ satisfies $\#E(\mathbb{F}_p) = p + 1 - t$, where t is the trace of the p-power Frobenius endomorphism $\pi : (x, y) \mapsto (x^p, y^p)$ [39, Theorem 4.12].

Let r be a large prime satisfying $r \mid \#E(\mathbb{F}_p)$. The embedding degree k with respect to r is the smallest positive integer such that $r \mid p^k - 1$. We denote the eigenspaces of π acting on the r- torsion group $E[r] = \{P \in E \mid [r]P = \mathcal{O}_E\}$ with the eigenvalues 1 and p by $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. In other words, $\mathbb{G}_1$ and $\mathbb{G}_2$ can be represented as $\mathbb{G}_1 = E(\mathbb{F}_p)[r]$ and $\mathbb{G}_2 = E(\mathbb{F}_{p^k})[r] \cap \{P \in E \mid \pi(P) = [p]P\}$, respectively. In the following, we propose the definitions of the isogenies, the families of pairing-friendly elliptic curves and the optimal ate pairing.

2.1 Isogenies

Let E and E' be two elliptic curves defined over $\mathbb{F}_p$. An isogeny $\varphi : E \to E'$ over $\mathbb{F}_p$ can be regarded as a non-constant group homomorphism from $E(\mathbb{F}_p)$ to $E'(\mathbb{F}_p)$ such that $\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$. The degree of φ is defined to be its degree as a group homomorphism. The kernel of φ is a finite subgroup $G \subseteq E(\mathbb{F}_p)$, denoted by $\ker(\varphi)$. We call the isogeny $\hat{\varphi} : E' \to E$ such that $\hat{\varphi}(\varphi(P)) = [\deg(\varphi)]P$ for every $P \in E$ as the dual of φ, where $\deg(\varphi)$ is the degree of φ. A separable isogeny that satisfies $\ker(\varphi) = \deg(\varphi) = n$ is called n-isogeny. We only consider separable isogenies in this paper. Explicit formulas for φ were first given by Vélu [37,17].

2.2 Families of pairing-friendly elliptic curve

In this subsection, we present the definitions of the CM discriminant D and the families of pairing-friendly curves.

By Hasse's theorem [39, Theorem 4.2], we have $-2\sqrt{p} \leq t \leq 2\sqrt{p}$. Let D be a positive square-free integer such that $4p - t^2 = Dy^2,\ y \in \mathbb{Z}$. From [39, Theorem 10.6], we know that the endomorphism ring of an ordinary curve E over $\mathbb{F}_p$ denoted by $\mathrm{End}_p(E)$ is isomorphic to an order in an imaginary quadratic field. In fact, the field is exactly $K = \mathbb{Q}(\sqrt{-D})$ and $\mathrm{End}_p(E)$ contains the p-power Frobenius map $\pi_p = t \pm y\sqrt{-D}$.

An elliptic curve E over $\mathbb{F}_p$ is pairing-friendly if the following two conditions hold:

1. the order of the additive group $\#E(\mathbb{F}_p)$ has a large prime factor r satisfying $\frac{\log_2(p)}{\log_2(r)} \leq 2$,
2. the embedding degree k with respect to r is less than $\log_2(r)/8$.

The tuple (p, t, r) of a pairing-friendly curve can be parametrized by polynomials. We state the following definition for illustration.

Definition 1. *Let $p(x), t(x), r(x) \in \mathbb{Q}[x]$ be non-zero polynomials. A polynomial tuple $(p(x), t(x), r(x))$ parametrizes a family of pairing-friendly elliptic curves with embedding degree k and CM discriminant D, if the following conditions are satisfied:*

1. *$p(x)$ represents primes and it is non-constant, irreducible, with a positive leading coefficient.*
2. *$r(x)$ is a non-constant, irreducible, integer-valued polynomial with a positive leading coefficient.*
3. *$r(x)$ divides both $p(x) + 1 - t(x)$ and $\Phi_k(t(x) - 1)$, where $\Phi_k(x)$ denotes the k-th cyclotomic polynomial.*
4. *There are infinitely many integer solutions (x, Y) for the parametrized CM equation $DY^2 = 4p(x) - t(x)^2$.*

2.3 Optimal ate pairing

We first present the definitions of the Miller function $f_{n,P}$ and Miller's algorithm. For any point $P \in E$ and $n \in \mathbb{Z}$, denote by $f_{n,P}$ the normalized rational function associated with the divisor:

$$(f_{n,P}) = n(P) - ([n]P) - (n-1)(\mathcal{O}_E).$$

Especially for $P \in E[r]$, the corresponding divisor becomes:

$$(f_{r,P}) = r(P) - r(\mathcal{O}_E).$$

For any $i, j \in \mathbb{Z}$, there exists a relationship between $f_{i,P}, f_{j,P}$ and $f_{i+j,P}$:

$$(f_{i+j,P}) = \left(f_{i,P} \cdot f_{j,P} \cdot \frac{\ell_{[i]P,[j]P}}{v_{[i+j]P}} \right), \tag{1}$$

where $\ell_{[i]P,[j]P}$ represents a line passing through the points $[i]P$ and $[j]P$, and $v_{[i+j]P}$ represents a vertical line passing through $[i+j]P$ and $[-i-j]P$. A well-known efficient algorithm to compute the evaluation of $f_{n,P}(Q)$ where $n \in \mathbb{Z}, P \in \mathbb{G}_1, Q \in \mathbb{G}_2$ was proposed by Miller [26], which is described in Algorithm 1.

Algorithm 1 Miller's algorithm

Input: Two points $P \in \mathbb{G}_1,\ Q \in \mathbb{G}_2, n = \sum_{i=0}^{N} n_i 2^i$ with $n_i \in \{-1, 0, 1\}$.
Output: The value $f_{n,P}(Q)$
1: $T \leftarrow Q,\ f \leftarrow 1$
2: **for** $i = N-1$ **to** 0 **do**
3: $\quad f \leftarrow f^2 \cdot \frac{\ell_{T,T}(P)}{v_{[2]T}(P)},\ T \leftarrow [2]T$
4: $\quad$ **if** $n_i = 1$ **then**
5: $\quad\quad f \leftarrow f \cdot \frac{\ell_{T,Q}(P)}{v_{T+Q}(P)},\ T \leftarrow T + Q$
6: $\quad$ **end if**
7: $\quad$ **if** $n_i = -1$ **then**
8: $\quad\quad f \leftarrow f \cdot \frac{\ell_{T,-Q}(P)}{v_{T-Q}(P)},\ T \leftarrow T - Q$
9: $\quad$ **end if**
10: **end for**
11: **return** f

Let $\lambda = mr$ with $r \nmid m$. And write the p-adic representation of λ as $\lambda = \sum_{i=0}^{l} c_i p^i$. By Minkowski's theorem [27], there exists one of the shortest vectors $V = (c_0, \cdots, c_{\varphi(k)-1})$ with $|c_i| \leq r^{1/\varphi(k)}$, where $\varphi(k)$ is the Euler function. Define μ_r to be the group of primitive r-th roots of unity. An optimal ate pairing [38] $opt : \mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$ on E is defined as follows:

$$(Q, P) \mapsto \left(\prod_{i=0}^{l} f_{c_i, Q}^{p^i}(P) \cdot \prod_{i=0}^{l-1} \frac{\ell_{[s_{i+1}]Q, [c_i p^i]Q}(P)}{v_{[s_i]Q}(P)} \right)^{(p^k-1)/r} \tag{2}$$

with $s_i = \sum_{j=i}^{l} c_j p^j$. The bilinearity of opt can be established by leveraging the bilinearity of ate pairing [22] and Eq. (1).

3 Main Results

In this section we propose the optimized formulas for pairing computations. We first explore how to determine a curve equipped with an n-isogeny as a GLV-endomorphism. Subsequently, we present novel formulas for the super-optimal ate pairing on $\mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r$ and the Tate pairing on $\mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r$ by utilizing n-isogeny. Since the formulas are relatively more efficient when n is small, 2, 3-isogenies will be commonly exploited in practice. Consequently, we detailedly discuss the formulas for the super-optimal pairing on two cryptographically interesting families GG22D7 and GG28D11 [19] employing 2 and 3-isogenies, respectively.

As mentioned in Section 2.2, the endomorphism ring $\mathrm{End}_p(E)$ of an ordinary curve E is isomorphic to an order of an imaginary field

$$\mathbb{Q}(\sqrt{-D}) = \{a_1 + b_1\sqrt{-D} \mid a_1, b_1 \in \mathbb{Q}\}.$$

The largest subring of $\mathbb{Q}(\sqrt{-D})$ is a finitely generated abelian group [39]:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{-D}}{2}\right] & D \equiv 3 \mod 4, \\ \mathbb{Z}\left[\sqrt{-D}\right] & D \equiv 1, 2 \mod 4. \end{cases}$$

An **order** in $\mathbb{Q}[\sqrt{-D}]$ is a ring R satisfying $\mathbb{Z} \subsetneq R \subseteq \mathcal{O}_K$ [39]. Such an order has the form:

$$R = \mathbb{Z} + \mathbb{Z}f\delta,$$

where $f > 0$ and $\delta = (1 + \sqrt{-D})/2$ or $\sqrt{-D}$. We call the integer f as the **conductor** of R. Let $\varphi \in \mathrm{End}_p(E)$ be an endomorphism of E over $\mathbb{F}_p$. Then φ can be represented as $\varphi = a_1 + b_1 f\sqrt{-D}$ or $\varphi = a_1 + b_1 f((1 + \sqrt{-D})/2)$, where $a_1, b_1 \in \mathbb{Z}$. If φ is simultaneously an n-isogeny, it satisfies the following equation:

$$Nrd(\varphi) = \varphi\hat{\varphi} = n, \tag{3}$$

where $Nrd(\varphi)$ and $\hat{\varphi}$ are the norm and conjugate element of φ, respectively.

If φ has the form: $\varphi = a_1 + b_1\sqrt{-D}$, then Eq. (3) transforms into:

$$\varphi\hat{\varphi} = \left(a_1 + b_1\sqrt{-D}\right)\left(a_1 - b_1\sqrt{-D}\right) = a_1^2 + b_1^2 D = n.$$

If φ can be expressed as $\varphi = (2a_1 + b_1)/2 + \frac{b_1\sqrt{-D}}{2}$, then Eq. (3) is:

$$\varphi\hat{\varphi} = \left(\frac{2a_1 + b_1}{2} + \frac{b_1\sqrt{-D}}{2}\right)\left(\frac{2a_1 + b_1}{2} - \frac{b_1\sqrt{-D}}{2}\right) = \frac{(2a_1 + b_1)^2}{4} + \frac{b_1^2 D}{4} = n.$$

A curve with such D is associated with an n-isogeny φ as the GLV endomorphism. We aim to determine the integer solution (a_1, b_1) of this equation. For simplicity, we represent the n-isogeny as $\varphi = a + b\sqrt{-D}$, where $a, b \in \mathbb{Q}$ and $2a, 2b \in \mathbb{Z}$.

3.1 Speed up the optimal pairing computation on $\mathbb{G}_2 \times \mathbb{G}_1$

In this subsection, we present the formulas for the super-optimal pairings on GLV-curves with n-isogenies φ as their endomorphisms, and exploit the small cases $n = 2$ and 3 to our target families GG22D7 and GG28D11, respectively.

Using the same notations as Section 2, let the GLV-endomorphism $\varphi = a + b\sqrt{-D}$ represent an n-isogeny with the characteristic equation $\varphi^2 - 2a\varphi + n = 0$. In other words, D satisfies $Nrd(\varphi) = a^2 + Db^2 = n$. One can prove that φ is an endomorphism of the r-th cyclic group $\mathbb{G}_2$. Therefore, for every $Q \in \mathbb{G}_2$ there exists an integer λ such that $\varphi(Q) = [\lambda]Q$. Consider the composite map $\tau = \varphi \circ \pi$, we have $\tau(Q) = [\lambda \cdot p \mod r]Q$.

We fix the number field $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$ which contains the primitive k-th root ζ_k and $\sqrt{-D}$. According to the KSS construction [24,19], the polynomial $r(x) \in \mathbb{Q}[x]$ is the minimal polynomial of an element $\alpha = (a + b\sqrt{-D}) \cdot \zeta_k$ in K. Let $t(x),\ y(x)$ and $p(x)$ be the polynomials such that $t(\alpha) = \zeta_k + 1 \mod r(\alpha)$, $y(\alpha) = \frac{\zeta_k - 1}{\sqrt{-D}} \mod r(\alpha)$ and $p(x) = \frac{t^2(x) + Dy^2(x)}{4}$. Define k' to be the minimum integer such that $\varphi^{k'} = A + B\sqrt{-D} \in \mathbb{Q}(\sqrt{-D})$. From [41], the polynomials $r(x),\ t(x),\ y(x)$ and $p(x)$ are given as follows:

$$
\begin{aligned}
&r(x) : \text{the maximum factor of } x^{2k'} - 2Ax^{k'} + A^2 + DB^2,\\
&t(x) = \frac{-bx^{k'+1} + (aB + Ab)x}{B(a^2 + Db^2)} + 1,\\
&y(x) = -\frac{ax^{k'+1} + (bDB - aA)x}{DB(a^2 + Db^2)} + \frac{x^{k'} - A}{DB},\\
&p(x) = \frac{t^2(x) + Dy^2(x)}{4}.
\end{aligned}
\tag{Const.1}
$$

If there exists a seed x such that $t(x), r(x)$ are integers and $p(x)$ is prime, then the tuple $t(x),\ r(x),\ p(x)$ parametrizes a family of pairing-friendly curves. We denote the above family (Const.1) by $F(n, D, k, a, b)$. By the above construction, a curve E in $F(n, D, k, a, b)$ is associated with the embedding degree k, CM-discriminant D, and an n-isogeny $\varphi = a + b\sqrt{-D}$ as GLV-endomorphism. It can be deduced that $\varphi \circ \pi(Q) = [x]Q,\ Q \in \mathbb{G}_2$. In other words, the element $\varphi \circ \pi$ corresponds to $\alpha = (a + b\sqrt{-D}) \cdot \zeta_k$ in $\mathrm{End}_p(E)$. Furthermore, we can derive the following relation:

$$
\begin{aligned}
x^2 - 2axp + np^2 &\equiv x^2 - 2ax\zeta_k + n\zeta_k^2 \mod r(x)\\
&\equiv \zeta_k^2(\varphi^2 - 2a\varphi + n) \mod r(x)\\
&\equiv 0 \mod r(x).
\end{aligned}
$$

Since $2a \in \mathbb{Z}$, one of the shortest vectors $(c_0, \cdots, c_l)$ for the optimal pairing in this family is given by $(x^2, -2ax, n, 0, \cdots, 0)$. Plugging this vector into Eq. (2), we obtain the formula for the optimal pairing:

$$
opt(Q, P) = f_{x^2,Q}(P) \cdot f^p_{-2ax,Q}(P) \cdot f^{p^2}_{n,Q}(P) \cdot \ell_{\pi^2([n]Q),\pi([-2ax]Q)}(P). \tag{4}
$$

Now we explore how to simplify the computation for the optimal pairing on such GLV-curves in $F(n, D, k, a, b)$. The following theorem gives a framework of constructing optimized pairings formulas on certain pairing-friendly curves with n-isogenies as endomorphisms.

Theorem 1. *Let the notations be denoted as above. Let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. Then the formula of the bilinear pairing $\mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r : (Q, P) \mapsto opt(Q, P)^n$ for the GLV-curves in $F(n, D, k, a, b)$, with an n-isogeny as endomorphism is presented as follows:*

$$
sopt(Q, P) = \left(f^x_{x,Q}([n]P) \cdot f^{np}_{x,Q}(\hat{\varphi}(P)) \cdot f^p_{-2ax,Q}([n]P) \cdot \hat{L} \right)^{\frac{p^k - 1}{r}},
$$

the rational function $\hat{L}$ is given by:

$$\hat{L} = f_{n,Q}^{p^2}([n]P) \cdot \ell_{\pi^2([n]Q),\pi([-2ax]Q)}([n]P) \cdot L^p(\hat{\varphi}(P)) \cdot \prod_{i=1}^{n} L_i^p(\hat{\varphi}(P))$$

where L and L_i $(i = 1, \cdots, n)$ are rational functions associated with the divisors

$$(L) = \sum_{i=1}^{n}([x](Q+T_i)) - \sum_{i=1}^{n}([x]Q+T_i) + \sum_{i=1}^{n}(x-1)(\mathcal{O}_E) - \sum_{i=1}^{n}(x-1)(T_i)$$

and

$$(L_i) = x(Q+T_i) - x(Q) + ([x]Q) - ([x]Q+T_i),$$

respectively.

Proof. By [22, Lemma 2] and $\varphi \circ \pi(Q) = [x]Q$, the pairng $opt(Q,P)$ can be represented as:

$$\begin{aligned} opt(Q,P) &= f_{x,Q}^{x}(P) \cdot f_{x,[x]Q}(P) \cdot f_{-2ax,Q}^{p}(P) \cdot f_{n,Q}^{p^2}(P) \cdot \ell_{\pi^2([n]Q),\pi([-2ax]Q)}(P) \\ &= f_{x,Q}^{x}(P) \cdot f_{x,\varphi(Q)}^{p}(P) \cdot f_{-2ax,Q}^{p}(P) \cdot f_{n,Q}^{p^2}(P) \cdot \ell_{\pi^2([n]Q),\pi([-2ax]Q)}(P). \end{aligned}$$

By the definition of $f_{x,P}$, the divisor of $f_{x,\varphi(Q)}$ can be written as follows:

$$(f_{x,\varphi(Q)}) = x(\varphi(Q)) - ([x]\varphi(Q)) - (x-1)(\mathcal{O}_E).$$

By the properties of the pullback φ^* we obtain (see also [36, Chapter III]):

$$\varphi^*(f_{x,\varphi(Q)}) = \sum_{i=1}^{n} x(Q+T_i) - \sum_{i=1}^{n}([x]Q+T_i) - \sum_{i=1}^{n}(x-1)(T_i), \tag{5}$$

where the set $\{T_1, \cdots, T_n\}$ is the kernel of φ. Substituting $(f_{x,Q+T_i})$ into the above equation, it yields that:

$$\begin{aligned} \varphi^*(f_{x,\varphi(Q)}) = &\sum_{i=1}^{n}(f_{x,Q+T_i}) + \sum_{i=1}^{n}([x](Q+T_i)) - \sum_{i=1}^{n}([x]Q+T_i) \\ &+ \sum_{i=1}^{n}(x-1)(\mathcal{O}_E) - \sum_{i=1}^{n}(x-1)(T_i). \end{aligned}$$

Since the degree of the divisor $\varphi^*(f_{x,\varphi(Q)}) - \sum_{i=1}^{n}(f_{x,Q+T_i})$ satisfies

$$\deg\left(\sum_{i=1}^{n}([x](Q+T_i)) - \sum_{i=1}^{n}([x]Q+T_i) + \sum_{i=1}^{n}(x-1)(\mathcal{O}_E) - \sum_{i=1}^{n}(x-1)(T_i)\right) = 0,$$

there exists a rational function L corresponding to it. Consequently, we have:

$$\varphi^*(f_{x,\varphi(Q)}) = \sum_{i=1}^{n}(f_{x,Q+T_i}) + (L).$$

Additionally, according to [36, Chapter III], it is known that $\varphi^*(f_{x,\varphi(Q)}) = (f_{x,\varphi(Q)} \circ \varphi)$. Therefore, it can be derived that:

$$f_{x,\varphi(Q)}(\varphi(P)) = L(P) \cdot \prod_{i=1}^{n} f_{x,Q+T_i}(P). \tag{6}$$

Since $\varphi \circ \hat{\varphi} = [n]$, acting $\hat{\varphi}$ on the above equality yields:

$$f_{x,\varphi(Q)}([n]P) = L(\hat{\varphi}(P)) \cdot \prod_{i=1}^{n} f_{x,Q+T_i}(\hat{\varphi}(P)).$$

Finally, substracting $(f_{x,Q})$ from $(f_{x,Q+T_i})$, we can deduce that:

$$(f_{x,Q+T_i}) - (f_{x,Q}) = x(Q+T_i) - x(Q) + ([x]Q) - ([x]Q+T_i). \tag{7}$$

Similarly, the degree of divisor $(f_{x,Q+T_i}) - (f_{x,Q})$ is zero. Consequently, for each i there exists a rational function L_i such that:

$$f_{x,Q+T_i} = f_{x,Q} \cdot L_i, \ i = 1, 2, \cdots, n.$$

Substituting these equalities into Eq. (4), it can be deduced that:

$$f_{x,\varphi(Q)}([n]P) = f_{x,Q}^n(\hat{\varphi}(P)) \cdot L(\hat{\varphi}(P)) \cdot \prod_{i=1}^{n} L_i(\hat{\varphi}(P)).$$

Based on the bilinearity of $opt(Q,P)$ and the aforementioned analysis, $opt(Q,P)^n$ is also bilinear, thus it can be represented as:

$$\begin{aligned}
&opt(Q,[n]P)\\
=&f_{x,Q}^x([n]P) \cdot f_{x,[x]Q}([n]P) \cdot f_{-2ax,Q}^p([n]P) \cdot f_{n,Q}^{p^2}(P) \cdot \ell_{\pi^2([n]Q),\pi([-2ax]Q)}([n]P)\\
=&f_{x,Q}^x([n]P) \cdot f_{x,\varphi(Q)}^p([n]P) \cdot f_{-2ax,Q}^p([n]P) \cdot f_{n,Q}^{p^2}(P) \cdot \ell_{\pi^2([n]Q),\pi([-2ax]Q)}([n]P)\\
=&f_{x,Q}^x([n]P) \cdot f_{x,Q}^{np}(\hat{\varphi}(P)) \cdot f_{-2ax,Q}^p([n]P) \cdot \hat{L}
\end{aligned}$$

where $\hat{L} = f_{n,Q}^{p^2}([n]P) \cdot \ell_{\pi^2([n]Q),\pi([-2ax]Q)}([n]P) \cdot L^p(\hat{\varphi}(P)) \cdot \prod_{i=1}^{n} L_i^p(\hat{\varphi}(P))$.

From [41] we know that if it satisfies that $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$ or $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, with $a = 0$ and $k \equiv 0 \mod 4$ [41], we have $\deg(r(x)) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\zeta_k) : \mathbb{Q}] = \varphi(k)$. Thus the length of the Miller loop satisfies $\log_2 |x| \approx \log_2(r)/\varphi(k)$. Consequently, there exist no super-optimal pairings on such GLV-curves. For instance, several well-known families of pairing friendly curves such as BLS12, BLS24, KSS16 and KSS18 do not possess super-optimal pairings.

On the contrary, if $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, an element $\alpha = (a + b\sqrt{-D}) \cdot \zeta_k$ with $a \neq 0$ or $k \neq 0 \mod 4$ is a primitive root of $K = \mathbb{Q}(\sqrt{-D}, \zeta_k)$. In this situation, $\deg(r(x)) = [K : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2\varphi(k)$. After exploiting the above techniques, the length of the Miller loop of $sopt(Q,P)$ is approximately

$\log_2(r)/2\varphi(k)$. Hence $sopt(Q,P)$ is a super-optimal pairing utilizing n-isogenies as GLV-endomorphisms. Besides, we can accomplish the evaluations of both $f_{x,Q}([n]P)$ and $f_{x,Q}(\hat{\varphi}(P))$ in the same Miller loop.

If $n = 1$, φ naturally represents an efficiently-computable automorphism, which has been used to construct super-optimal pairings on curves with $D = 1$ or 3 [15,9]. Nevertheless, there is no such non-trivial automorphism on some GLV-curves with $D \neq 1, 3$, such as the curve GG22-457.

In the case of $n \geq 2$, we consider to make use of n-isogenies as endomorphisms. When n is small, the remaining rational function $\hat{L}$ is easy to compute. In particular, we primarily focus on detailing the cases $n = 2, 3$, and consider $n = 2$ for implementation to enhance the efficiency of the pairing computations on GG22-457 with $D = 7$. Note that the curve GG22-457 is defined over relatively small base field at the 192-bit security level, which is preferred in certain pairing-based cryptographic protocols, for example DAA schemes.

It is worth noting that as the degree n increases, the form of $\hat{L}$ may be more complicated, potentially leading to a higher computational cost. Additionally, one can explore the utilization for the large-degree isogenies by simplifying the function $\hat{L}$ to further extend the application of our techniques.

Using 2-isogeny to speed up the pairing computation Let φ denote a 2-isogeny. Based on the preceding analysis, there are two situations of $\varphi = a + b\sqrt{-D},\ a, b \in \mathbb{Q}$. If φ can be expressed as $\varphi = a_1 + b_1\sqrt{-D},\ a_1, b_1 \in \mathbb{Z}$, it follows that:

$$a_1^2 + b_1^2 D = 2.$$

Since D is also a positive integer, there are two possible choices for the pair $(a_1^2, b_1^2 D)$:

$$\begin{cases} a_1^2 = 0, & b_1^2 D = 2 \\ a_1^2 = 1, & b_1^2 D = 1 \end{cases}$$

which implies that:

$$a_1^2 = b_1^2 = 1,\ D = 1 \text{ or } a_1^2 = 0,\ b_1^2 = 1,\ D = 2.$$

However, when $D = 1$, it corresponds to the Weierstrass equation $E : y^2 = x^3 + cx$ with $j(E) = 1728$ [13]. This type of curves possesses efficiently-computable automorphisms which can effectively expedite the computations of the scalar multiplications [18] and the Tate pairing [32]. For instance, take $p \equiv 1 \mod 4$ then the map:

$$\tau : (x, y) \mapsto (-x, iy)$$

where $i \in \mathbb{F}_p,\ i^2 = -1$ is an automorphism of E over $\mathbb{F}_p$. The difference between the actions of two maps $\tau = \sqrt{-1}$ and $\varphi = \pm 1 \pm \sqrt{-1}$ on a point $P \in E$ is only adding or subtracting itself, up to a sign. Therefore, we do not need to use 2-isogeny to speed up the pairing computations on such GLV-curves. If $D = 2$, then the endomorphism φ can be represented as $\varphi = \pm\sqrt{-2}$.

If $\varphi = (2a_1 + b_1)/2 + \frac{b_1\sqrt{-D}}{2},\ a_1, b_1 \in \mathbb{Z}$, this implies that D must satisfy $D \equiv 3 \mod 4$. It can be derived that:

$$\begin{aligned}\varphi\hat{\varphi} &= \left(\frac{2a_1 + b_1}{2} + \frac{b_1\sqrt{-D}}{2}\right)\left(\frac{2a_1 + b_1}{2} - \frac{b_1\sqrt{-D}}{2}\right) \\ &= \frac{4a_1^2 + 4a_1b_1 + b_1^2}{4} + \frac{b_1^2 D}{4} \\ &= 2\end{aligned}$$

which is equivalent to $(2a_1 + b_1)^2 + b_1^2 D = 8$. Similarly, due to the fact that D is an integer and $D \equiv 3 \mod 4$, there is only one possible situation:

$$(2a_1 + b_1)^2 = 1,\ b_1^2 D = 7,$$

which corresponds to $b_1 = \pm 1,\ 2a_1 + b_1 = \pm 1,$ and $D = 7$. Therefore, φ can be written as $\varphi = \pm\frac{1}{2} \pm \frac{\sqrt{-7}}{2}$. In conclusion, only the pairing-friendly curves corresponding to $D = 2$ and $D = 7$ are equipped with the 2-isogenies as the GLV-endomorphisms (See Examples 5 and 6 in [18]). Similarly, there are no non-trivial automorphisms on such curves.

Assume that the embedding degree k satisfies $\sqrt{-2},\ \sqrt{-7} \notin \mathbb{Q}(\zeta_k)$. Based on the above analysis, the families $F(2, 7, k, \pm\frac{1}{2}, \pm\frac{1}{2})$ or $F(2, 2, k, 0, \pm 1)$, which are constructed by making $r(x)$ be the minimal polynomial of $\alpha = (\frac{\pm 1 \pm \sqrt{-7}}{2}) \cdot \zeta_k$ or $\alpha = (\pm\sqrt{-2}) \cdot \zeta_k$ is compatible with the techniques in Theorem 1. Since the derivation is similar, we omit the process of constructing the super-optimal pairings on $F(2, 2, k, 0, \pm 1)$ for simplicity.

Let $p(x), t(x), r(x)$ be the polynomials parametrizing the family $F(2, 7, k, -\frac{1}{2}, \frac{1}{2})$ with a 2-isogeny $\varphi = (-1 + \sqrt{-7})/2$ as endomorphism. By the conditions $-\frac{1}{2} \neq 0$ and the above analysis we know that there is a super-optimal pairing on $F(2, 7, k, -\frac{1}{2}, \frac{1}{2})$. For any $Q \in \mathbb{G}_2$ we have:

$$\varphi \circ \pi(Q) = \varphi([t(x) - 1]Q) = [x]Q.$$

Furthermore, it can be deduced that

$$\alpha^2 - \alpha \cdot \zeta_k + 2\zeta_k^2 = \zeta_k^2 \cdot \left(\left(\frac{-1 + \sqrt{-7}}{2}\right)^2 - \frac{-1 + \sqrt{-7}}{2} + 2\right) = 0,$$

which implies that

$$x^2 + xp(x) + 2p(x)^2 \equiv 0 \mod r(x).$$

Thus, one of the shortest vectors $c_0, \cdots, c_l$ for the optimal pairing on family $F(2, 7, k, -\frac{1}{2}, \frac{1}{2})$ is given by $(x^2, x, 2, 0, \cdots, 0)$. By Theorem 1, we can derive the formulas for the super-optimal pairing on $F(2, 7, k, -\frac{1}{2}, \frac{1}{2})$. Let $T_2 \in E(\mathbb{F}_p)$ be a generator of $\ker(\varphi)$. This also means that T_2 is a rational point of order *two*. Our main result of this subsection is summarized in the following theorem:

Theorem 2. *Let the notations be denoted as above. Let $P \in \mathbb{G}_1,\ Q \in \mathbb{G}_2$. Then the formula of the bilinear pairing $\mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r : (Q, P) \mapsto opt(Q, P)^2$ for the GLV-curves in $F(2, 7, k, -\frac{1}{2}, \frac{1}{2})$ is given as follows:*

$$sopt(Q, P) = \left(f_{x,Q}^{p+x}([2]P) \cdot f_{x,Q}^{2p}(\hat{\varphi}(P)) \cdot \hat{L} \right)^{\frac{p^k-1}{r}},$$

the function $\hat{L}$ is given by:

$$\hat{L} = \begin{cases} \frac{f_{2,Q}^{p^2}([2]P) \cdot \ell_{\pi^2([2]Q),\varphi(\pi^2(Q))}([2]P) \cdot \ell^p_{\varphi(\pi(Q)),Q+T_2}(\hat{\varphi}(P)) \cdot \ell^{\frac{xp-p}{2}}_{Q+T_2,Q+T_2}(\hat{\varphi}(P))}{\ell^p_{\varphi(\pi(Q))+T_2,Q}(\hat{\varphi}(P)) \cdot \ell^{\frac{xp-p}{2}}_{Q,Q}(\hat{\varphi}(P))}, & x \text{ is odd}, \\ \frac{f_{2,Q}^{p^2}([2]P) \cdot \ell_{\pi^2([2]Q),\varphi(\pi^2(Q))}([2]P) \cdot \ell^p_{\varphi(\pi(Q)),T_2}(\hat{\varphi}(P)) \cdot \ell^{\frac{xp}{2}}_{Q+T_2,Q+T_2}(\hat{\varphi}(P))}{v^p_{\varphi(\pi(Q))+T_2}(\hat{\varphi}(P)) \cdot \ell^{\frac{xp}{2}}_{Q,Q}(\hat{\varphi}(P))}, & x \text{ is even}. \end{cases}$$

To prove Theorem 2, we first propose the following two lemmas, which provides explicit descriptions of the functions L and L_i $(i = 1, 2)$ in Theorem 1, respectively.

Lemma 1. *For $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, we have*

$$f_{x,\varphi(Q)}([2]P) = \begin{cases} \frac{f_{x,Q}(\hat{\varphi}(P)) \cdot f_{x,Q+T_2}(\hat{\varphi}(P))}{v_{T_2}^{\frac{x-1}{2}}(\hat{\varphi}(P))}, & x \text{ is odd}, \\ \frac{f_{x,Q}(\hat{\varphi}(P)) \cdot f_{x,Q+T_2}(\hat{\varphi}(P)) \cdot \ell_{[x]Q,T_2}(\hat{\varphi}(P))}{v_{[x]Q+T_2}(\hat{\varphi}(P)) \cdot v_{T_2}^{\frac{x}{2}}(\hat{\varphi}(P))}, & x \text{ is even}. \end{cases}$$

Proof. By the definition of $f_{x,\varphi(Q)}$ we have:

$$(f_{x,\varphi(Q)}) = x(\varphi(Q)) - ([x]\varphi(Q)) - (x-1)(\mathcal{O}_E).$$

From Eq. (5), it can be deduced that:

$$\varphi^*(f_{x,\varphi(Q)}) = x((Q) + (Q + T_2)) - ([x]Q) - ([x]Q + T_2) - (x-1)((\mathcal{O}_E) + (T_2)).$$

If x is odd, then

$$\begin{aligned} \varphi^*(f_{x,\varphi(Q)}) &= (f_{x,Q}) + (f_{x,Q+T_2}) + (x-1)(\mathcal{O}_E) - (x-1)(T_2) \\ &= (f_{x,Q}) + (f_{x,Q+T_2}) - (v_{T_2}^{\frac{x-1}{2}}). \end{aligned}$$

Additionally, it follows from Eq. (6) that:

$$f_{x,\varphi(Q)} \circ \varphi = \frac{f_{x,Q} \cdot f_{x,Q+T_2}}{v_{T_2}^{\frac{x-1}{2}}}.$$

Since $\varphi \circ \hat{\varphi} = [2]$, acting the dual $\hat{\varphi}$ on the above equality yields:

$$f_{x,\varphi(Q)} \circ [2] = \frac{(f_{x,Q} \circ \hat{\varphi}) \cdot (f_{x,Q+T_2} \circ \hat{\varphi})}{(v_{T_2} \circ \hat{\varphi})^{\frac{x-1}{2}}}$$

which implies that:

$$f_{x,\varphi(Q)}([2]P) = \frac{f_{x,Q}(\hat{\varphi}(P)) \cdot f_{x,P+T_2}(\hat{\varphi}(Q))}{v_{T_2}^{\frac{x-1}{2}}(\hat{\varphi}(Q))}.$$

If x is even, we have:

$$\begin{aligned}\varphi^*(f_{x,\varphi(Q)}) &= (f_{x,Q}) + (f_{x,Q+T_2}) + ([x]Q) + (x-1)((\mathcal{O}_E) - (T_2)) - ([x]Q + T_2) \\ &= (f_{x,Q}) + (f_{x,Q+T_2}) + (\ell_{[x]Q,T_2}) - (v_{[x]Q+T_2}) - (v_{T_2}^{\frac{x}{2}}).\end{aligned}$$

Similar to the above deduction, we have:

$$f_{x,\varphi(Q)}([2]P) = \frac{f_{x,Q}(\hat{\varphi}(P)) \cdot f_{x,Q+T_2}(\hat{\varphi}(P)) \cdot \ell_{[x]Q,T_2}(\hat{\varphi}(P))}{v_{[x]Q+T_2}(\hat{\varphi}(P)) \cdot v_{T_2}^{\frac{x}{2}}(\hat{\varphi}(P))},$$

which completes the proof.

The following lemma establishes the relationship between $f_{x,Q}$ and $f_{x,Q+T_2}$:

Lemma 2. *Using the notations introduced in Lemma 1, we have:*

$$f_{x,Q+T_2}(P) = \begin{cases} f_{x,Q}(P) \cdot \left(\frac{\ell_{Q+T_2,Q+T_2}(P)}{\ell_{Q,Q}(P)}\right)^{\frac{x-1}{2}} \cdot \frac{\ell_{[x]Q,Q+T_2}(P)}{\ell_{[x]Q+T_2,Q}(P)}, & x \text{ is odd}, \\ f_{x,Q}(P) \cdot \left(\frac{\ell_{Q+T_2,Q+T_2}(P)}{\ell_{Q,Q}(P)}\right)^{\frac{x}{2}}, & x \text{ is even}. \end{cases}$$

Proof. From Eq. (7) we obtain:

$$(f_{x,Q+T_2}) - (f_{x,Q}) = \begin{cases} x(Q+T_2) - x(Q) - ([x]Q + T_2) + ([x]Q), & x \text{ is odd}, \\ x(Q+T_2) - x(Q), & x \text{ is even}. \end{cases}$$

If x is even, then

$$\begin{aligned}(f_{x,Q+T_2}) - (f_{x,Q}) &= x(Q+T_2) - x(Q) \\ &= \frac{x}{2}(2(Q+T_2) - 2(Q)) \\ &= \frac{x}{2}(2(Q+T_2) + ([-2]Q) - 3(\mathcal{O}_E) - 2(Q) - ([-2]Q) + 3(\mathcal{O}_E)) \\ &= \frac{x}{2}((\ell_{Q+T_2,Q+T_2}) - (\ell_{Q,Q}))\end{aligned}$$

which implies that

$$f_{x,Q+T_2}(P) = f_{x,Q}(P) \cdot \left(\frac{\ell_{Q+T_2,Q+T_2}(Q)}{\ell_{Q,Q}(P)}\right)^{\frac{x}{2}}.$$

Similarly, if x is odd, we have:

$$\begin{aligned}(f_{x,Q+T_2}) - (f_{x,Q}) &= x(Q+T_2) - x(Q) - ([x]Q + T_2) + ([x]Q) \\ &= \frac{x-1}{2}((\ell_{Q+T_2,Q+T_2}) - (\ell_{Q,Q})) + (\ell_{[x]Q,Q+T_2}) - (\ell_{[x]Q+T_2,Q}),\end{aligned}$$

which completes the proof.

It is now in a position to give the whole proof for Theorem 2.

Proof of Theorem 2: According to Theorem 1, by Eq. (4) we can derive the corresponding formula for the optimal pairing as detailed in [19]:

$$\begin{aligned} opt(Q,P) &= \left(f_{x^2,Q}(P)\cdot f_{x,Q}^{p}(P)\cdot f_{2,Q}^{p^2}(P)\cdot \ell_{\pi^2([2]Q),\pi([x]Q)}(P)\right)^{\frac{p^k-1}{r}} \\ &= \left(f_{x,Q}^{p+x}(P)\cdot f_{x,[x]Q}(P)\cdot f_{2,Q}^{p^2}(Q)\cdot \ell_{\pi^2([2]Q),\pi([x]Q)}(P)\right)^{\frac{p^k-1}{r}}. \end{aligned}$$

By the bilinearity of $opt(Q,P)$ we have

$$\begin{aligned} sopt(Q,P) &= opt(Q,[2]P) \\ &= \left(f_{x^2,Q}([2]P)\cdot f_{x,Q}^{p}([2]P)\cdot f_{2,Q}^{p^2}([2]P)\cdot \ell_{\pi^2([2]Q),\pi([x]Q)}([2]P)\right)^{\frac{p^k-1}{r}}. \end{aligned} \tag{8}$$

From the previous analysis, it is evident that

$$f_{x^2,Q}([2]P) = f_{x,Q}^{x}([2]P)\cdot f_{x,[x]Q}([2]P).$$

Substituting the above equality into Eq. (8) we obtain:

$$sopt(Q,P)=\left(f_{x,Q}^{p+x}([2]P)\cdot f_{x,[x]Q}([2]P)\cdot f_{2,Q}^{p^2}([2]P)\cdot \ell_{\pi^2([2]Q),\pi([x]Q)}([2]P)\right)^{\frac{p^k-1}{r}}. \tag{9}$$

Due to the fact that $\varphi\circ\pi(Q)=[x]Q$, it can be deduced that

$$f_{x,[x]Q}([2]P)=f_{x,\varphi\circ\pi(Q)}([2]P) = f_{x,\varphi(Q)}^{p}([2]P).$$

Substituting it into Eq. (9) we derive:

$$sopt(Q,P)=\left(f_{x,Q}^{p+x}([2]P)\cdot f_{x,\varphi(Q)}^{p}([2]P)\cdot f_{2,Q}^{p^2}([2]P)\cdot \ell_{\pi^2([2]Q),\pi([x]Q)}([2]P)\right)^{\frac{p^k-1}{r}}. \tag{10}$$

By applying Lemmas 1 and 2, we can represent $f_{x,\varphi(Q)}([2]P)$ as follows:

$$f_{x,\varphi(Q)}([2]P) = \begin{cases} \dfrac{f_{x,Q}^2(\hat{\varphi}(P))\cdot \ell_{\varphi(\pi(Q)),Q+T_2}(\hat{\varphi}(P))\cdot \ell_{Q+T_2,Q+T_2}^{\frac{x-1}{2}}(\hat{\varphi}(P))}{\ell_{\varphi(\pi(Q))+T_2,Q}(\hat{\varphi}(P))\cdot \ell_{Q,Q}^{2^{\frac{x-1}{2}}}(\hat{\varphi}(P))\cdot v_{T_2}^{2^{\frac{x-1}{2}}}(\hat{\varphi}(P))}, & x \text{ is odd}, \\ \dfrac{f_{x,Q}^2(\hat{\varphi}(P))\cdot \ell_{\varphi(\pi(Q)),T_2}(\hat{\varphi}(P))\cdot \ell_{Q+T_2,Q+T_2}^{\frac{x}{2}}(\hat{\varphi}(P))}{v_{\varphi(\pi(Q))+T_2}(\hat{\varphi}(P))\cdot \ell_{Q,Q}^{\frac{x}{2}}(\hat{\varphi}(P))\cdot v_{T_2}^{\frac{x}{2}}(\hat{\varphi}(P))}, & x \text{ is even}. \end{cases}$$

Note that $v_{T_2}(\hat{\varphi}(P)) = x_{\hat{\varphi}(P)} - x_{T_2} \in \mathbb{F}_p$ since $\hat{\varphi}(P), T_2 \in E(\mathbb{F}_p)$. Therefore, we can conclude that:

$$\begin{aligned} v_{T_2}(\hat{\varphi}(P))^{\frac{p^k-1}{r}} &= \left((x_{\hat{\varphi}(P)} - x_{T_2})^{\frac{p^k-1}{\Phi_k(p)}}\right)^{\frac{\Phi_k(p)}{r}} \\ &= 1. \end{aligned}$$

Consequently, $v_{T_2}(\hat{\varphi}(P))$ vanishes in the final exponentiation, and there is no need to evaluate $v_{T_2}^{\frac{x}{2}}$ or $v_{T_2}^{\frac{x-1}{2}}$ at $\hat{\varphi}(P)$. Finally, we substitute the above results into Eq. (10) and obtain the new formula. □

Note that $opt(P,Q)^2$ also defines a bilinear pairing, as $opt(P,Q)$ is bilinear. Hence, we obtain a new bilinear pairing on $\mathbb{G}_2 \times \mathbb{G}_1$, that is equivalent to the traditional optimal ate pairing up to a square. Compared to the traditional optimal pairing, the length of the Miller loop in our new pairing is reduced to around $\lfloor \log_2(x) \rfloor \approx \log_2(r(x))/(2\varphi(k))$. Moreover, we can evaluate $f_{x,Q}([2]P)$ and $f_{x,Q}(\hat{\varphi}(P))$ in a shared Miller loop, which significantly speeds up the pairing computation since the function $\hat{L}$ can be efficiently computed. Indeed, the exponentiation in $\hat{L}$ can be simultaneously done as executing the Miller loop. In the next section, we explore how to perform the pairing computation using our new formulas in detail.

Remark 1. Note that our approach is not limited to be applicable for family $\in F(2,7,k,-\frac{1}{2},\frac{1}{2})$. Any family of the pairing-friendly curves constructed by making $r(x)$ be the minimal polynomial of $\alpha = (\frac{\pm 1 \pm \sqrt{-7}}{2}) \cdot \zeta_k$ with $\sqrt{-7} \notin \mathbb{Q}(\zeta_k)$, or $\alpha = (\pm\sqrt{-2}) \cdot \zeta_k$ with $\sqrt{-2} \notin \mathbb{Q}(\zeta_k)$ is compatible with the techniques in Theorem 2.

Application on the family GG22D7. As mentioned in Section 1, Gasnier and Guillevic proposed an excellent family of pairing-friendly curves named GG22D7 with $D = 7$ [19]. This family has several specific features such as small ρ-value. A curve named GG22D7-457 in this family benefits from the efficient $\mathbb{G}_1$ arithmetic.

Example 1. (GG22D7, [19]) Let $k = 22,\ D = 7,\ \varphi = (-1+\sqrt{-7})/2,\ \alpha = \varphi \cdot \zeta_k$.

$$\begin{aligned}
t(x) =& (x^{12} + 45x + 46)/46,\\
p(x) =& (x^{24} - x^{23} + 2x^{22} + 67x^{13} + 94x^{12} + 134x^{11} + 2048x^2 + 4096)/7406,\\
r(x) =& (x^{20} - x^{19} - x^{18} + 3x^{17} - x^{16} - 5x^{15} + 7x^{14} + 3x^{13} - 17x^{12} + 11x^{11}\\
&+ 23x^{10} + 22x^9 - 68x^8 + 24x^7 + 112x^6 - 160x^5 - 64x^4 + 384x^3\\
&- 256x^2 - 512x + 1024)/23.
\end{aligned}$$

Hence, we deduce that GG22D7 $\in F(2,7,22,-\frac{1}{2},\frac{1}{2})$, which is compatible with our techniques. Thus the pairing computation on this family can be optimized by utilizing 2-isogeny φ.

Using 3-isogeny to speed up the pairing computation Similar to the analysis of applying 2-isogeny, let φ be a 3-isogeny. If φ has the form $\varphi = a_1 + b_1\sqrt{-D},\ a_1, b_1 \in \mathbb{Z}$, it holds that:

$$a_1^2 + b_1^2 D = 3.$$

The two possible integer solutions are:

$$\begin{cases} a_1^2 = 0, & b_1^2 D = 3, \\ a_1^2 = 1, & b_1^2 D = 2. \end{cases}$$

However, the first situation is $D = 3$, in relation to the Weierstrass equation: $E : y^2 = x^3 + c$ with $j(E) = 0$ [13]. Like the case $D = 1$, this kind of curves also have efficiently-computable automorphisms. And the second solution corresponds to $D = 2$, whose pairing computation can be optimized by using 2-isogeny. Therefore, integrating 3-isogeny into the aforementioned two cases is not feasible.

If $\varphi = (2a_1 + b_1)/2 + \frac{b_1\sqrt{-D}}{2},\ a_1, b_1 \in \mathbb{Z}$, this means that $D \equiv 3 \mod 4$ in this case. It can be deduced that

$$\begin{aligned} \varphi\hat{\varphi} &= \left(\frac{2a_1 + b_1}{2} + \frac{b_1\sqrt{-D}}{2}\right)\left(\frac{2a_1 + b_1}{2} - \frac{b_1\sqrt{-D}}{2}\right) \\ &= 3 \end{aligned}$$

which implies that: $(2a + b)^2 + b^2 D = 12$. Similarly, by the condition $D \equiv 3 \mod 4$ there are the following three possible situations:

$$\begin{cases} (2a + b)^2 = 0, & b^2 D = 12, \\ (2a + b)^2 = 1, & b^2 D = 11, \\ (2a + b)^2 = 9, & b^2 D = 3. \end{cases}$$

Except for the second situation, the corresponding CM-discriminants are $D = 3$. Therefore, we only focus on the situation with respect to $D = 11$, which implies that $b = \pm 1,\ 2a + b = \pm 1$. Therefore, φ can be expressed as: $\varphi = \pm\frac{1}{2} \pm \frac{\sqrt{-11}}{2}$.

Assume that the embedding degree k satisfies $\sqrt{-11} \notin \mathbb{Q}(\zeta_k)$. Similarly, we apply the techniques in Theorem 1 to the families $F(3, 11, k, \pm\frac{1}{2}, \pm\frac{1}{2})$, which are constructed by making $r(x)$ be the minimal polynomial of $\alpha = (\frac{\pm 1 \pm \sqrt{-11}}{2}) \cdot \zeta_k$. By setting $\varphi = \frac{-1+\sqrt{-11}}{2}$, now we show how to exploit the GLV endomorphism φ to enhance the efficiency of the pairing computations on family $F(3, 11, k, -\frac{1}{2}, \frac{1}{2})$.

From the above conditions we have:

$$x^2 + xp(x) + 3p(x)^2 \equiv 0 \mod r(x).$$

The deduction process is the same as 2-isogeny. Consequently, one of the shortest vectors $c_0, \cdots, c_l$ for the optimal pairing on $F(3, 11, k, -\frac{1}{2}, \frac{1}{2})$ is given by $(x^2, x, 3, 0, \cdots, 0)$. We can construct the formulas for the super-optimal pairing on $F(3, 11, k, -\frac{1}{2}, \frac{1}{2})$ by Theorem 1. Let $T_3 \in E(\mathbb{F}_p)$ be a generator of $\ker(\varphi)$. Our novel formula for the pairing computation that leverages 3-isogeny φ is stated in the following theorem:

Theorem 3. *Let the notation as above. Let $P \in \mathbb{G}_1,\ Q \in \mathbb{G}_2$. Then the formula of the bilinear pairing $\mathbb{G}_2 \times \mathbb{G}_1 \to \mu_r : (Q, P) \mapsto opt(Q, P)^3$ for the family constructed in family $F(3, 11, k, -\frac{1}{2}, \frac{1}{2})$ is given as follows:*

$$sopt(Q, P) = \left(f_{x,Q}^{p+x}([3]P) \cdot f_{x,Q}^{3p}(\hat{\varphi}(P)) \cdot \hat{L}\right)^{\frac{p^k-1}{r}},$$

the function $\hat{L}$ is given by:

$$\hat{L}=\begin{cases}\dfrac{f_{3,Q}^{p^2}([3]P)\cdot\ell^p_{\pi([3]Q),[x]Q}([3]P)\cdot\left(\prod_{i=1}^{2}f_{3,Q+[i]T_3}^{\frac{xp}{3}}(\hat{\varphi}(P))\right)\cdot\ell^p_{[x]Q,[x]Q}(\hat{\varphi}(P))}{\left(\prod_{i=1}^{2}f_{3,Q}^{\frac{xp}{3}}(\hat{\varphi}(P))\right)\cdot\ell^p_{[x]Q+T_3,[x]Q-T_3}(\hat{\varphi}(P))}, & x\equiv 0(3),\\ \dfrac{f_{3,Q}^{p^2}([3]P)\cdot\ell^p_{\pi([3]Q),[x]Q}([3]P)\cdot\prod_{i=1}^{2}\left(f_{3,Q+[i]T_3}^{\frac{(x-1)p}{3}}(\hat{\varphi}(P))\cdot\ell^p_{[x]Q,Q+[i]T_3}(\hat{\varphi}(P))\right)}{\prod_{i=1}^{2}\left(f_{3,Q}^{\frac{(x-1)p}{3}}(\hat{\varphi}(P))\cdot\ell^p_{[x]Q+[i]T_3,Q}(\hat{\varphi}(P))\right)}, & x\equiv 1(3),\\ \dfrac{f_{3,Q}^{p^2}([3]P)\cdot\ell^p_{\pi([3]Q),[x]Q}([3]P)\cdot\prod_{i=1}^{2}\left(f_{3,Q+[i]T_3}^{\frac{(x+1)p}{3}}(\hat{\varphi}(P))\cdot\ell^p_{[x]Q,Q}(\hat{\varphi}(P))\right)}{\prod_{i=1}^{2}\left(f_{3,Q}^{\frac{(x+1)p}{3}}(\hat{\varphi}(P))\cdot\ell^p_{[x]Q+[i]T_3,[x]Q-[i]T_3}(\hat{\varphi}(P))\right)}, & x\equiv 2(3)\end{cases}$$

where $\hat{\varphi}$ is the dual of φ.

The proof of Theorem 3 requires the following two lemmas to obtain the functions L and $L_i(i=1,2,3)$ in Theorem 1, respectively.

Lemma 3. *For $P\in\mathbb{G}_1$ and $Q\in\mathbb{G}_2$, we have*

$$f_{x,\varphi(Q)}([3]P)=\begin{cases}\dfrac{\prod_{i=0}^{2}f_{x,Q+[i]T_3}(\hat{\varphi}(P))\cdot\ell_{[x]Q,[x]Q}(\hat{\varphi}(P))}{v_{T_3}^{x-1}(\hat{\varphi}(P))\cdot\ell_{[x]Q+T_3,[x]Q-T_3}(\hat{\varphi}(P))}, & x\equiv 0(3),\\ \dfrac{\prod_{i=0}^{2}f_{x,Q+[i]T_3}(\hat{\varphi}(P))}{v_{T_3}^{x-1}(\hat{\varphi}(P))}, & x\equiv 1,2(3).\end{cases}$$

Proof. From Eq. (5) we obtain:

$$\varphi^*(f_{x,\varphi(Q)})=\sum_{i=0}^{2}x(Q+[i]T_3)-\sum_{i=0}^{2}([x]Q+[i]T_3)-\sum_{i=0}^{2}(x-1)([i]T_3).$$

If $x\equiv 0 \mod 3$, it holds that:

$$\sum_{i=0}^{2}([x]Q+[ix]T_3)=3([x]Q).$$

Hence it can be derived that:

$$\begin{aligned}\varphi^*(f_{x,\varphi(Q)})=&\sum_{i=0}^{2}(f_{x,Q+[i]T_3})+3([x]Q)-\sum_{i=0}^{2}([x]Q+[i]T_3)+(3x-3)(\mathcal{O}_E)\\&-\sum_{i=0}^{2}(x-1)([i]T_3)\\=&\sum_{i=0}^{2}(f_{x,Q+[i]T_3})+\left(\frac{\ell_{[x]Q,[x]Q}}{\ell_{[x]Q+T_3,[x]Q-T_3}}\right)-(v_{T_3}^{x-1}).\end{aligned}$$

Additionally, according to Eq. (6) we deduce:

$$f_{x,\varphi(Q)} \circ \varphi = \frac{\prod_{i=0}^{2} f_{x,Q+[i]T_3} \cdot \ell_{Q,Q}}{v_{T_3}^{x-1} \cdot \ell_{[x]Q+T_3,[x]Q-T_3}}.$$

From $\varphi \circ \hat{\varphi} = [3]$, acting the dual $\hat{\varphi}$ on the above equality yields:

$$f_{x,\varphi(Q)}([3]P) = \frac{\prod_{i=0}^{2} f_{x,Q+[i]T_3}(\hat{\varphi}(P)) \cdot \ell_{Q,Q}(\hat{\varphi}(P))}{v_{T_3}^{x-1}(\hat{\varphi}(P)) \cdot \ell_{[x]Q+T_3,[x]Q-T_3}(\hat{\varphi}(P))}.$$

If $x \equiv 1, 2 \mod 3$, it can be deduced that

$$\sum_{i=0}^{2}([x]Q + [ix]T_3) = \sum_{i=0}^{2}([x]Q + [i]T_3).$$

Consequently, we can derive that

$$\begin{aligned}\varphi^*(f_{x,\varphi(Q)}) &= \sum_{i=0}^{2}(f_{x,Q+[i]T_3}) + (3x-3)(\mathcal{O}_E) - \sum_{i=0}^{2}(x-1)([i]T_3) \\ &= \sum_{i=0}^{2}(f_{x,Q+[i]T_3}) - (v_{T_3}^{x-1}).\end{aligned}$$

Similar to the deduction in Lemma 1 , we obtain

$$f_{x,\varphi(Q)}([3]P) = \frac{\prod_{i=0}^{2} f_{x,Q+[i]T_3}(\hat{\varphi}(P))}{v_{T_3}^{x-1}(\hat{\varphi}(P))}.$$

which completes the proof.

Lemma 4 provides a representation of $\prod_{i=1}^{2} f_{x,Q+[i]T_3}$ in terms of $f_{x,Q}$:

Lemma 4. *Using the notations of Lemma 3, we have:*

$$\prod_{i=1}^{2} f_{x,Q+[i]T_3}(P) = \begin{cases} f_{x,Q}^2(P) \cdot \prod_{i=1}^{2} \left(\frac{f_{3,Q+[i]T_3}(P)}{f_{3,Q}(P)}\right)^{\frac{x}{3}}, & x \equiv 0(3), \\ f_{x,Q}^2(P) \cdot \prod_{i=1}^{2} \left(\left(\frac{f_{3,Q+[i]T_3}(P)}{f_{3,Q}(P)}\right)^{\frac{x-1}{3}} \cdot L_1\right), & x \equiv 1(3), \\ f_{x,Q}^2(P) \cdot \prod_{i=1}^{2} \left(\left(\frac{f_{3,Q+[i]T_3}(P)}{f_{3,Q}(P)}\right)^{\frac{x+1}{3}} \cdot L_2\right), & x \equiv 2(3). \end{cases}$$

where $L_1 = \frac{\ell_{[x]Q,Q+[i]T_3}(P)}{\ell_{[x]Q+[i]T_3,Q}(P)}$ *and* $L_2 = \frac{\ell_{[x]Q,Q}(P)}{\ell_{[x]Q+[i]T_3,[x]Q-[i]T_3}(P)}$.

Proof. From Eq. (7) we obtain:

$$(f_{x,Q+T_3}) - (f_{x,Q}) = \begin{cases} x(Q+T_3) - x(Q) & x \equiv 0(3) \\ x(Q+T_3) - x(Q) - ([x]Q+T_3) + ([x]Q), & x \equiv 1,2(3). \end{cases}$$

If $x \equiv 0 \mod 3$, it yields that:

$$\begin{aligned}\sum_{i=1}^{2}(f_{x,Q+[i]T_3}) - 2(f_{x,Q}) &= \sum_{i=1}^{2}\frac{x}{3}(3(Q+[i]T_3) - 3(Q)) \\ &= \frac{x}{3}((f_{3,Q+[i]T_3}) - (f_{3,Q})) \\ &= \left(\prod_{i=1}^{2}\left(\frac{f_{3,Q+[i]T_3}}{f_{3,Q}}\right)^{\frac{x}{3}}\right)\end{aligned}$$

Similarly, if $x \equiv 1 \mod 3$, we derive:

$$\begin{aligned}\sum_{i=1}^{2}(f_{x,Q+[i]T_3}) - 2(f_{x,Q}) &= \sum_{i=1}^{2}\left((x-1)((P+[i]T_3) - (P)) + \left(\frac{\ell_{[x]Q,Q+[i]T_3}}{\ell_{[x]Q+[i]T_3,Q}}\right)\right) \\ &= \left(\prod_{i=1}^{2}\left(\left(\frac{f_{3,Q+[i]T_3}}{f_{3,Q}}\right)^{\frac{x-1}{3}} \cdot \frac{\ell_{[x]Q,Q+[i]T_3}}{\ell_{[x]Q+[i]T_3,Q}}\right)\right).\end{aligned}$$

And if $x \equiv 2 \mod 3$, it can be deduced that:

$$\sum_{i=1}^{2}(f_{x,Q+[i]T_3}) - 2(f_{x,Q}) = \left(\prod_{i=1}^{2}\left(\left(\frac{f_{3,Q+[i]T_3}}{f_{3,Q}}\right)^{\frac{x+1}{3}} \cdot \frac{\ell_{[x]Q,Q}}{\ell_{[x]Q+[i]T_3,[x]Q-[i]T_3}}\right)\right).$$

which completes the proof.

On the basis of Lemmas 3 and 4 we can prove Theorem 3 now.

Proof of Theorem 3: Utilizing Eq. (4) we can derive the formula for the optimal pairing:

$$\begin{aligned}opt(Q,P) &= \left(f_{x^2,Q}(P) \cdot f_{x,Q}^{p}(P) \cdot f_{3,Q}^{p^2}(P) \cdot \ell_{\pi^2([3]Q),\pi([x]Q)}(P)\right)^{\frac{p^k-1}{r}} \\ &= \left(f_{x,Q}^{p+x}(P) \cdot f_{x,[x]Q}(P) \cdot f_{3,Q}^{p^2}(P) \cdot \ell_{\pi^2([3]Q),\pi([x]Q)}(P)\right)^{\frac{p^k-1}{r}}.\end{aligned}$$

By the bilinearity of $opt(Q,P)$ we have:

$$\begin{aligned}sopt(Q,P) &= opt(Q,[3]P) \\ &= \left(f_{x^2,Q}([3]P) \cdot f_{x,Q}^{p}([3]P) \cdot f_{3,Q}^{p^2}([3]P) \cdot \ell_{\pi^2([3]Q),\pi([x]Q)}([3]P)\right)^{\frac{p^k-1}{r}}.\end{aligned} \tag{11}$$

Substituting $f_{x^2,Q}([3]P) = f_{x,Q}^{x}([3]P) \cdot f_{x,[x]Q}([3]P)$ in Eq. (11) we obtain:

$$sopt(Q,P) = \left(f_{x,Q}^{p+x}([3]P) \cdot f_{x,[x]Q}([3]P) \cdot f_{3,Q}^{p^2}([3]P) \cdot \ell_{\pi^2([3]Q),\pi([x]Q)}([3]P)\right)^{\frac{p^k-1}{r}}. \tag{12}$$

Since $\varphi \circ \pi(Q) = [x]Q$, plugging it into $f_{x,[x]Q}([3]P)$ yields that:

$$f_{x,[x]Q}([3]P) = f_{x,\varphi\circ\pi(Q)}([3]P) = f^p_{x,\varphi(Q)}([3]P).$$

Substituting it into Eq. (12) we derive:

$$sopt(Q,P) = \left(f^{p+x}_{x,Q}([3]P) \cdot f^p_{x,\varphi(Q)}([3]P) \cdot f^{p^2}_{3,Q}([3]P) \cdot \ell_{\pi^2([3]Q),\pi([x]Q)}([3]P)\right)^{\frac{p^k-1}{r}}. \tag{13}$$

By applying Lemmas 3 and 4, we can represent $f_{x,\varphi(Q)}([3]P)$ as follows:

$$f_{x,\varphi(Q)}([3]P) = \begin{cases} \dfrac{f^3_{x,Q}(\hat{\varphi}(P)) \cdot \left(\prod_{i=1}^2 f^{\frac{xp}{3}}_{3,Q+[i]T_3}(\hat{\varphi}(P))\right) \cdot \ell^p_{[x]Q,[x]Q}(\hat{\varphi}(P))}{\left(\prod_{i=1}^2 f^{\frac{xp}{3}}_{3,Q}(\hat{\varphi}(P))\right) \cdot \ell^p_{[x]Q+T_3,[x]Q-T_3}(\hat{\varphi}(P)) \cdot v^{x-1}_{T_3}(\hat{\varphi}(P))}, & x \equiv 0(3), \\ \dfrac{f^3_{x,Q}(\hat{\varphi}(P)) \cdot \prod_{i=1}^2 \left(f^{\frac{(x-1)p}{3}}_{3,Q+[i]T_3}(\hat{\varphi}(P)) \cdot \ell^p_{[x]Q,Q+[i]T_3}(\hat{\varphi}(P))\right)}{\prod_{i=1}^2 \left(f^{\frac{(x-1)p}{3}}_{3,Q}(\hat{\varphi}(P)) \cdot \ell^p_{[x]Q+[i]T_3,Q}(\hat{\varphi}(P))\right) \cdot v^{x-1}_{T_3}(\hat{\varphi}(P))}, & x \equiv 1(3), \\ \dfrac{f^3_{x,Q}(\hat{\varphi}(P)) \cdot \prod_{i=1}^2 \left(f^{\frac{(x+1)p}{3}}_{3,Q+[i]T_3}(\hat{\varphi}(P)) \cdot \ell^p_{[x]Q,Q}(\hat{\varphi}(P))\right)}{\prod_{i=1}^2 \left(f^{\frac{(x+1)p}{3}}_{3,Q}(\hat{\varphi}(P)) \cdot \ell^p_{[x]Q+[i]T_3,[x]Q-[i]T_3}(\hat{\varphi}(P))\right) \cdot v^{x-1}_{T_3}(\hat{\varphi}(P))}, & x \equiv 2(3) \end{cases}$$

Note that $v_{T_3}(\hat{\varphi}(P)) = x_{\hat{\varphi}(P)} - x_{T_3} \in \mathbb{F}_p$ since $\hat{\varphi}(P), T_3 \in E(\mathbb{F}_p)$. Therefore, we can conclude that:

$$\begin{aligned} v_{T_3}(\hat{\varphi}(P))^{\frac{p^k-1}{r}} &= \left((x_{\hat{\varphi}(P)} - x_{T_3})^{\frac{p^k-1}{\Phi_k(p)}}\right)^{\frac{\Phi_k(p)}{r}} \\ &= 1. \end{aligned}$$

Therefore, the vertical line functions $v^{\frac{x}{3}}_{T_3}(\hat{\varphi}(P))$ or $v^{\frac{x-1}{3}}_{T_3}(\hat{\varphi}(P))$ do not need to be evaluated. Finally we substitute the above results into Eq. (13), which completes the proof. □

Note that $sopt(Q,P) = opt(P,Q)^3$ gives a bilinear pairing since $opt(P,Q)$ is bilinear. Compared with the traditional optimal pairing, the length of the Miller loop achieves $\lfloor \log_2(x) \rfloor \approx \log_2(r(x))/(2\varphi(k))$ and we can simultaneously evaluate $f_{x,Q}([3]P)$ and $f_{x,Q}(\hat{\varphi}(P))$ in a shared Miller loop. Besides, the computation of function $\hat{L}$ is inexpensive since we can concurrently accomplish the exponentiation in $\hat{L}$ when performing the Miller loop. Therefore, exploiting 3-isogeny can crucially enhance the performance of the pairing computation.

Application on the family GG28D11 As an illustrative example for $D = 11$, we present the following family proposed by Gasnier and Guillevic named GG28D11 [19] with the embedding degree $k = 28$.

Example 2. (GG28 [19]) $k = 28,\ D = 11,\ \varphi = (-1+\sqrt{-11})/2,\ \alpha = \varphi \cdot \zeta_k$.

$$\begin{aligned} t(x) =& (x^{15} + 718x + 3237)/3237, \\ p(x) =& (x^{30} + x^{29} + 3x^{28} + 2515x^{16} + 14384x^{15} + 7545x^{14} + 4782969x^2 \\ & + 13304911x + 14348907)/38419953, \\ r(x) =& x^{24} + 5x^{22} + 16x^{20} + 35x^{18} + 31x^{16} - 160x^{14} - 1079x^{12} - 1440x^{10} \\ & + 2511x^8 + 25515x^6 + 104976x^4 + 295245x^2 + 531441. \end{aligned}$$

It yields that GG28D11 $\in F(3, 11, 28, -\frac{1}{2}, \frac{1}{2})$, which is compatible with our method. Thus the corresponding pairing computation can be sped up by utilizing 3-isogeny φ.

3.2 Speed up the pairing computation on $\mathbb{G}_1 \times \mathbb{G}_2$

In this subsection, we state that our method can also be extended to the (reduced) Tate pairing on type $\mathbb{G}_1 \times \mathbb{G}_2 \to \mu_r$: $e(P, Q) = f_{r,P}(Q)^{\frac{p^k-1}{r}}$ where $P \in \mathbb{G}_1,\ Q \in \mathbb{G}_2$. Similarly, we mainly focus on optimizing the pairing computation on the curves corresponding to $D = 7$ using 2-isogeny. The generalization to the GLV-curves with n-isogenies ($n > 1$) is direct.

Using the same notation as before, we first prove the following lemma:

Lemma 5. *When $D = 7$, there exists a 2-isogeny φ over $\mathbb{F}_p$ that acts on the elements of $\mathbb{G}_1$ as a scalar multiplication $[\lambda]$.*

Proof. Based on the previous analysis, an endomorphism over $\mathbb{F}_p$ of the form: $\varphi = \pm\frac{1}{2} \pm \frac{\sqrt{-7}}{2} \in \mathrm{End}_p(E)$ is a 2-isogeny. For $P \in \mathbb{G}_1 = E(\mathbb{F}_p)[r] \setminus \{\mathcal{O}_E\}$, we have: $[r]\varphi(P) = \varphi([r]P) = \mathcal{O}_E$. Due to the fact that r is a prime, the image $\varphi(P) \in \mathbb{G}_1$ and φ is an endomorphism of $\mathbb{G}_1$. Since $\mathbb{G}_1$ is a cyclic group, we obtain $\varphi(P) = [\lambda]P$ which completes the proof.

We can obtain the scalar $\lambda \in \mathbb{F}_p$ by solving the following characteristic equation:

$$\lambda^2 + tr(\varphi)\lambda + Nrd(\varphi) = 0$$

where $tr(\varphi) = \varphi + \hat{\varphi}$ is the trace of φ. By the choices of φ, λ and $\bar{\lambda}$ are the two roots of the equation $\lambda^2 + 2\lambda + 2 = 0$ or $\lambda^2 - 2\lambda + 2 = 0$. For simplicity, we consider λ with respect to $\lambda^2 + 2\lambda + 2 = 0$. Our main result of the subsection is summarized in the following theorem.

Theorem 4. *Let E be an ordinary curve over $\mathbb{F}_p$ corresponding to $D = 7$ with a 2-isogeny φ defined as above. Let $P \in \mathbb{G}_1$ and $[\lambda]$ the scalar multiplication map of the subgroup $\langle P \rangle$ such that $\varphi(P) = [\lambda]P$. Let a be an integer such that $ar = \lambda^2+\lambda+2$. Then for $Q \in \mathbb{G}_2$, the bilinear pairing $e(P, Q)^{2a}$ can be computed as:*

$$e(P, Q)^{2a} = \left(f_{\lambda,P}^{\lambda+1}([2]Q) \cdot f_{\lambda,P}^2(\hat{\varphi}(Q)) \cdot f_{2,P}([2]Q) \cdot L \right)^{\frac{p^k-1}{r}}.$$

The rational function L is given by:

$$L = \begin{cases} \frac{\ell_{\varphi^2(P),\varphi(P)}([2]Q)\cdot \ell_{\varphi(P),P+T_2}(\hat{\varphi}(Q))\cdot \ell_{P+T_2,P+T_2}^{\frac{\lambda-1}{2}}(\hat{\varphi}(Q))}{\ell_{\varphi(P)+T_2,P}(\hat{\varphi}(Q))\cdot \ell_{P,P}^{\frac{\lambda-1}{2}}(\hat{\varphi}(Q))\cdot v_T^{\frac{\lambda-1}{2}}(\hat{\varphi}(Q))}, & \lambda \text{ is odd}, \\ \frac{\ell_{\varphi^2(P),\varphi(P)}([2]Q)\cdot \ell_{\varphi(P),T_2}(\hat{\varphi}(Q))\cdot \ell_{P+T_2,P+T_2}^{\frac{\lambda}{2}}(\hat{\varphi}(Q))}{v_{\varphi(P)+T_2}(\hat{\varphi}(Q))\cdot \ell_{P,P}^{\frac{\lambda}{2}}(\hat{\varphi}(Q))\cdot v_{T_2}^{\frac{\lambda}{2}}(\hat{\varphi}(Q))}, & \lambda \text{ is even}. \end{cases}$$

We have known that there is a 2-isogeny φ with respect to λ such that $\lambda^2+\lambda+2 = 0 \mod r$. Therefore, the integer a mentioned in the above theorem exists. The proof of Theorem 2 relies on the following lemma.

Lemma 6. *Using the same notation of Theorem 3, we have:*

$$e(P,Q)^a = (f_{\lambda,P}^{\lambda+1}(Q) f_{\lambda,[\lambda]P}(Q) f_{2,P}(Q) \ell_{\varphi^2(P),\varphi(P)}(Q))^{\frac{p^k-1}{r}}.$$

Proof. By the definition of reduced Tate pairing, we have:

$$e(P,Q)^a = f_{r,P}(Q)^{a\cdot\frac{p^k-1}{r}} = f_{ar,P}(Q)^{\frac{p^k-1}{r}}.$$

Since $ar = \lambda^2+\lambda+2$, it yields that:

$$e(P,Q)^a = f_{\lambda^2+\lambda+2,P}(Q)^{\frac{p^k-1}{r}}.$$

By Eq. (1), we obtain:

$$(f_{\lambda^2+\lambda+2,P}) = (f_{\lambda^2+\lambda,P}\cdot f_{2,P}\cdot \ell_{[\lambda^2+\lambda]P,[-2]P}),$$

since $[\lambda^2+\lambda]P = [-2]P$, it can be derived that:

$$\begin{aligned}(f_{\lambda^2+\lambda+2,P}) &= (f_{\lambda^2+\lambda,P}\cdot f_{2,P}\cdot v_{[2]P}) \\ &= (f_{\lambda^2,P}\cdot f_{\lambda,P}\cdot f_{2,P}\cdot \frac{\ell_{[\lambda^2]P,[\lambda]P}}{v_{[2]P}}\cdot v_{[2]P}) \\ &= (f_{\lambda^2,P}\cdot f_{\lambda,P}\cdot f_{2,P}\cdot \ell_{\varphi^2(P),\varphi(P)}).\end{aligned}$$

Following Lemma 2 in [22], we know that

$$(f_{\lambda^2,P}) = (f_{\lambda,P}^{\lambda}\cdot f_{\lambda,[\lambda]P}).$$

Therefore,

$$\begin{aligned}(f_{\lambda^2+\lambda+2,P}) &= (f_{\lambda^2,P}\cdot f_{\lambda,P}\cdot f_{2,P}\cdot \ell_{\varphi^2(P),\varphi(P)}) \\ &= (f_{\lambda,P}^{\lambda+1}\cdot f_{\lambda,[\lambda]P}\cdot f_{2,P}\cdot \ell_{\varphi^2(P),\varphi(P)}),\end{aligned}$$

which completes the proof.

Proof of Theorem 3: By the definition of $f_{\lambda,[\lambda]P}$ we have: $(f_{\lambda,[\lambda]P}) = \lambda([\lambda]P) - ([\lambda^2]P) - (\lambda-1)(\mathcal{O}_E)$. We also have: $\varphi(P) = [\lambda]P$ and $\#\ker(\varphi) = \deg(\varphi) = 2$. Using Eq. (5) we obtain:

$$\varphi^*(f_{\lambda,[\lambda]P}) = \lambda((P) + (P+T_2)) - ([\lambda]P) - ([\lambda]P + T_2) - (\lambda-1)((\mathcal{O}_E) + (T_2)).$$

Additionally, by Lemmas 1 and 2 we can represent $f_{\lambda,[\lambda]P}([2]Q)$ as:

$$f_{\lambda,[\lambda]P}([2]Q) = \begin{cases} \dfrac{f_{\lambda,P}^2(\hat{\varphi}(Q))\cdot \ell_{[\lambda]P,P+T_2}(\hat{\varphi}(Q))\cdot \ell_{P+T_2,P+T_2}^{\frac{\lambda-1}{2}}(\hat{\varphi}(Q))}{\ell_{[\lambda]P+T_2,P}(\hat{\varphi}(Q))\cdot \ell_{P,P}^{\frac{\lambda-1}{2}}(\hat{\varphi}(Q))\cdot v_{T_2}^{\frac{\lambda-1}{2}}(\hat{\varphi}(Q))}, & \lambda \textit{ is odd}, \\ \dfrac{f_{\lambda,P}^2(\hat{\varphi}(Q))\cdot \ell_{[\lambda]P,T_2}(\hat{\varphi}(Q))\cdot \ell_{P+T_2,P+T_2}^{\frac{\lambda}{2}}(\hat{\varphi}(Q))}{v_{[\lambda]P+T_2}(\hat{\varphi}(Q))\cdot \ell_{P,P}^{\frac{\lambda}{2}}(\hat{\varphi}(Q))\cdot v_{T_2}^{\frac{\lambda}{2}}(\hat{\varphi}(Q))}, & \lambda \textit{ is even}. \end{cases}$$

Since $e(P,[2]Q)^a = e(P,Q)^{2a}$ and $\varphi(P) = [\lambda]P$, we substitute the above equations into Lemma 6 to derive the following new formulas for $e(P,Q)^{2a}$:

$$e(P,Q)^{2a} = \left(f_{\lambda,P}^{\lambda+1}([2]Q)\cdot f_{\lambda,P}^2(\hat{\varphi}(Q))\cdot f_{2,P}([2]Q)\cdot L\right)^{\frac{p^k-1}{r}},$$

where the function L is:

$$L = \begin{cases} \dfrac{\ell_{\varphi^2(P),\varphi(P)}([2]Q)\cdot \ell_{\varphi(P),P+T_2}(\hat{\varphi}(Q))\cdot \ell_{P+T_2,P+T_2}^{\frac{\lambda-1}{2}}(\hat{\varphi}(Q))}{\ell_{\varphi(P)+T_2,P}(\hat{\varphi}(Q))\cdot \ell_{P,P}^{\frac{\lambda-1}{2}}(\hat{\varphi}(Q))\cdot v_{T_2}^{\frac{\lambda-1}{2}}(\hat{\varphi}(Q))}, & \lambda \textit{ is odd}, \\ \dfrac{\ell_{\varphi^2(P),\varphi(P)}([2]Q)\cdot \ell_{\varphi(P),T_2}(\hat{\varphi}(Q))\cdot \ell_{P+T_2,P+T_2}^{\frac{\lambda}{2}}(\hat{\varphi}(Q))}{v_{\varphi(P)+T_2}(\hat{\varphi}(Q))\cdot \ell_{P,P}^{\frac{\lambda}{2}}(\hat{\varphi}(Q))\cdot v_{T_2}^{\frac{\lambda}{2}}(\hat{\varphi}(Q))}, & \lambda \textit{ is even}. \end{cases}$$

This completes the proof. □

Note that $e(P,Q)^{2a}$ induces a bilinear pairing since $e(P,Q)$ is bilinear. Furthermore, it is non-degenerate when $r \nmid a$. In practice, a is much smaller than r. Hence we obtain a new non-degenerate, bilinear pairing on $\mathbb{G}_1 \times \mathbb{G}_2$ which is equal to the traditional (reduced) Tate pairing up to a fixed power. Compared to the traditional Tate pairing on $\mathbb{G}_1 \times \mathbb{G}_2$, the length of Miller loop L of our new pairing is reduced to about $\lfloor \log_2(\lambda) \rfloor \approx \log_2(r)/2$, which can optimize the pairing computation since the evaluations of the extra line functions are inexpensive. Especially on the family GG22D7, the twist Ate pairing is actually the Tate pairing itself. Consequently, employing our method can effectively speed up the $\mathbb{G}_1 \times \mathbb{G}_2$-type pairing on this family.

4 Efficient implementation on the pairing computation

In this section we present the details of the shared iterative steps involved in Miller function evaluations and the computational cost analysis of $\mathbb{G}_2 \times \mathbb{G}_1$-type pairing (super-optimal pairing). Additionally, the experimental results of $\mathbb{G}_2 \times \mathbb{G}_1$-type pairing computations are also illustrated. We take the family GG22D7 at the 192-bit security level for implementation, and employ our techniques to speed up the pairing computation.

4.1 Choice of parameters at the 192-bit security level

As mentioned in [19], $p(x)$ represents a prime of size 457 bits and the maximal factor r of $r(x)$ is a 383-bit prime when $x = -779523$ in Example 1, with respect to a 192-bit security level. Besides, the extension field $\mathbb{F}_{p^{22}}$ can be constructed as follows:

$$\mathbb{F}_p \Rightarrow \mathbb{F}_{p^{11}} = \mathbb{F}_p[\xi]/(\xi^{11} - 2\xi - 2) \Rightarrow \mathbb{F}_{p^{22}} = \mathbb{F}_{p^{11}}[v]/(v^2 - \xi).$$

The curve defined over $\mathbb{F}_p$ with coefficient $a = -3$ has Frobenius trace $t(x)$ and j-invariant $j(E) = -3375$ [19]. Gasnier and Guillevic name this curve as GG22D7-457 [19] to distinguish it by the embedding degree k, the CM-discriminant and the characteristic p.

Based on the above, for any $Q \in \mathbb{G}_2$, we take $\varphi = \frac{1-\sqrt{-7}}{2}$ and obtain:

$$\tau(Q) = \varphi \circ \pi(Q) = [-x]Q.$$

Furthermore, one of the shortest vectors $(c_0, \cdots, c_l)$ for the optimal pairing in the above family is given by $(x^2, -x, 2, 0, \cdots, 0)$. In other words, it satisfies that:

$$x^2 - xp(x) + 2p(x)^2 \equiv 0 \mod r(x).$$

By Theorem 2, our formula of pairing on GG22D7-457 is defined by:

$$sopt(Q, P) = \left(f_{-x,Q}^{p-x}([2]P) \cdot f_{-x,Q}^{2p}(\hat{\varphi}(P)) \cdot \hat{L}\right)^{\frac{p^{22}-1}{r}}, \tag{14}$$

where

$$\hat{L} = \frac{\ell_{Q,Q}^{p^2}([2]P) \cdot \ell_{\pi([2]Q),[-x]Q}^{p}([2]P) \cdot \ell_{[-x]Q,Q+T_2}^{p}(\hat{\varphi}(P)) \cdot \ell_{Q+T_2,Q+T_2}^{\frac{(-x-1)p}{2}}(\hat{\varphi}(P))}{\ell_{[-x]Q+T_2,Q}^{p}(\hat{\varphi}(P)) \cdot \ell_{Q,Q}^{\frac{(-x-1)p}{2}}(\hat{\varphi}(P))}.$$

Therefore, the length of Miller loop is about:

$$\log_2(x) \approx \frac{1}{22}\log_2(r(x)),$$

which achieves $\frac{1}{2\varphi(k)}\log_2(r(x))$ and is smaller than the traditional optimal pairing. Additionally, we can compute $f_{-x,Q}([2]P)$ and $f_{-x,Q}(\hat{\varphi}(P))$ simultaneously in a shared Miller loop.

4.2 Pairing computation

In this subsection, we first present explicit formulas for shared Miller doubling and addition steps. Then we illustrate how to execute the final exponentiation efficiently. Finally we give the comparison of the computational cost of pairing computation on GG22D7-457 between utilizing our methods and the previous optimal pairing.

Notations. Let $\mathbf{m}$, $\mathbf{s}$, and $\mathbf{i}$ be the costs of multiplication, squaring and inversion in $\mathbb{F}_p$, respectively. Let $\mathbf{m}_{11}, \mathbf{s}_{11}, \mathbf{i}_{11}$ and $\mathbf{f}_{11}$ represent the costs of addition, multiplication, squaring, inversion and Frobenius endomorphism in $\mathbb{F}_{p^{11}}$, respectively. And let $\mathbf{m}_{22}$, $\mathbf{s}_{22}$, $\mathbf{i}_{22}$, $\mathbf{f}_{22}$ and $\mathbf{e}_x$ represent the costs of addition, multiplication, squaring, inversion, Frobenius endomorphism and the exponentiation by $|x|$ in $\mathbb{F}_{p^{22}}$. We omit the calculation of the additions over finite fields for simplicity. Now we focus on the computation process of Miller function evaluations.

Recall from Eq. (14), in the computational phase of pairing on GG22D7-457 we need to evaluate two Miller functions $f_{x,Q}(\hat{\varphi}(P))$ and $f_{x,Q}([2]P)$. Computing a pairing by multiple Miller function evaluations were studied in [42,3,10]. Inspired by these works, we execute these two evaluations simultaneously in a shared Miller loop.

Since the curve has the form $E : y^2 = x^3 + ax + b$ with embedding degree $k = 22$ and CM-discriminant $D = 7$, it possesses a quadratic twist $E' : y^2 = x^3 + a/\xi^2 + b/\xi^3$ [22] over $\mathbb{F}_{p^{11}}$. The corresponding isomorphism from $E' \to E$ is given by:

$$\phi : (x, y) \mapsto (x\xi, y\xi v).$$

Thanks to the twist map, the subgroup $\mathbb{G}_2$ can be represented as:

$$\mathbb{G}_2 = E(\mathbb{F}_{p^{22}})[r] \cap \ker(\pi - [p]) \cong E'(\mathbb{F}_{p^{11}})[r].$$

We work with Jacobian coordinates for any point $P = (x_P, y_P) \in E$ to avoid inversion, which means that we represent P by (X_P, Y_P, Z_P) in projective space, where $x_P = X_P/Z_P^2,\ y_P = X_P/Z_P^3$. The denominator elimination can be exploited since the embedding degree k is even. Therefore, we only need to update the numerator. The function $f_{1,Q}$ can be initialized as:

$$f_{1,Q}([2]P) = f_{1,Q}(\hat{\varphi}(P)) = 1.$$

The Jacobian coordinates of $[2]P$ and $\hat{\varphi}(P)$ can be obtained using the mixed double formulas in [4] and Vélu's formulas [37], respectively. We omit the computational procedures for simplicity. The costs of evaluating $[2]$ and $\hat{\varphi}$ at P are $1\mathbf{m}+5\mathbf{s}$ and $5\mathbf{m}+1\mathbf{s}$, respectively. Subsequently, we compute the corresponding affine coordinates $x_{[2]P},\ y_{[2]P},\ x_{\hat{\varphi}(P)}$ and $y_{\hat{\varphi}(P)}$ using the techniques of batch multiplication and inversion at a cost of $9\mathbf{m}+2\mathbf{s}+1\mathbf{i}$. Therefore, the cost of initialization is $15\mathbf{m}+8\mathbf{s}+1\mathbf{i}$. In the following, we explore how to update the two intermediate values $f_{m,Q}([2]P)$ and $f_{m,Q}(\hat{\varphi}(P))$ in the shared Miller loop.

Shared addition step. Let $Q' = (x_{Q'}, y_{Q'})$ be a point in $E'(\mathbb{F}_{p^{11}})[r]$. Denote by (X_T, Y_T, Z_T) the Jacobian coordinates of $[m]Q'$. We adopt the mixed addition formula in [4] to compute the point $[m+1]Q'$, which can be done by the following sequences:

$$\begin{aligned}
&ZZ \leftarrow Z_T^2,\ U \leftarrow x'_Q \cdot ZZ,\ S \leftarrow y'_Q \cdot Z_T \cdot ZZ,\ H \leftarrow U - X_T,\\
&I \leftarrow (2H)^2,\ J \leftarrow H \cdot I,\ \alpha_{T+Q'} \leftarrow S - Y_T,\ W \leftarrow 2\alpha_{T+Q'},\ V \leftarrow X_T \cdot I,\\
&X_{T+Q'} \leftarrow W^2 - J - 2V,\ Y_{T+Q'} = W \cdot (V - X_{T+Q'}) - 2Y_T \cdot J,\\
&Z_{TQ'} \leftarrow Z_T \cdot H,\ Z_{T+Q'} \leftarrow 2Z_{TQ'}.
\end{aligned}$$

The above operations achieve a computational cost of $8\mathbf{m}_{11}+3\mathbf{s}_{11}$. Acting the twist map on T and Q', we obtain

$$\phi(T) = (X_T\xi, Y_T\xi v, Z_T),\ Q = \phi(Q') = (x_{Q'}\xi, y_{Q'}\xi v) \in \mathbb{G}_2.$$

It can be deduced from the iteration formulas of $f_{m,Q}$ that:

$$f_{m+1,Q}(x,y) \leftarrow f_{m,Q}(x,y) \cdot L_{\phi(T),\phi(Q')}(x,y)$$

where the function $L_{\phi(T),\phi(Q')}(x,y)$ is defined as follows:

$$L_{\phi(T),\phi(Q')}(x,y) = Z_{TQ'} \cdot y - (Z_{TQ'} \cdot y_{Q'}\xi + \alpha_{T+Q'}(x - x_{Q'}\xi))v.$$

Note that α_{T+Q} and Z_{TQ} have been obtained when computing $T+Q$. Furthermore, the computation of multipling an element of $\mathbb{F}_{p^{11}}$ by ξ only requires several additions. Therefore, we perform the following sequence to compute $L_{\phi(T),\phi(Q')}([2]P)$ and $L_{\phi(T),\phi(Q')}(\hat{\varphi}(P))$:

$$\begin{aligned}
&B \leftarrow Z_{TQ'} \cdot y_{Q'}\xi,\ C \leftarrow \alpha_{T+Q'} \cdot x_{Q'}\xi,\ D \leftarrow B - C + \alpha_{T+Q'}x_{[2]P},\\
&E \leftarrow B - C + \alpha_{T+Q'}x_{\hat{\varphi}(P)},\ L_{\phi(T),\phi(Q')}([2]P) \leftarrow Z_{TQ'} \cdot y_{[2]P} - Dv,\\
&L_{\phi(T),\phi(Q')}(\hat{\varphi}(P)) \leftarrow Z_{TQ'} \cdot y_{\hat{\varphi}(P)} - Ev
\end{aligned}$$

at a cost of $2\mathbf{m}_{11}+44\mathbf{m}$. Finally, we execute $2\mathbf{m}_{22}$ to obtain:

$$\begin{aligned}
&f_{m+1,Q}([2]P) \leftarrow f_{m,Q}([2]P) \cdot L_{\phi(T),\phi(Q')}([2]P),\\
&f_{m+1,Q}(\hat{\varphi}(P)) \leftarrow f_{m,Q}(\hat{\varphi}(P)) \cdot L_{\phi(T),\phi(Q')}(\hat{\varphi}(P)).
\end{aligned}$$

Therefore, the total computational cost of a shared addition step is

$$\begin{aligned}
\mathrm{Cost}_{\mathrm{SADD}} &= 8\mathbf{m_{11}} + 3\mathbf{s_{11}} + 2\mathbf{m_{11}} + 44\mathbf{m} + 2\mathbf{m_{22}}\\
&= 2\mathbf{m_{22}} + 10\mathbf{m_{11}} + 3\mathbf{s_{11}} + 44\mathbf{m}.
\end{aligned}$$

Shared doubling step. We first adopt the doubling formula for $a=-3$ in [4] to obtain $[2]T$ from T, which can be expressed as the following sequence of operations:

$$\begin{aligned}
&YY = Y_T^2,\ ZZ \leftarrow Z_T^2,\ S = X_T \cdot YY,\ \beta_{[2]T} \leftarrow 3(X_T - ZZ/\xi) \cdot (X_T + ZZ/\xi),\\
&N \leftarrow \beta_{[2]T}^2 - 8S,\ X_{[2]T} \leftarrow N,\ Y_{[2]T} \leftarrow \beta_{[2]T} \cdot (4S - X_{[2]T}) - 8YY^2,\\
&Z_{[2]T} \leftarrow (Y_T + Z_T)^2 - YY - ZZ.
\end{aligned}$$

From the above sequence, the cost of performing a doubling is $3\mathbf{m}_{11}+5\mathbf{s}_{11}$. By the formulas of $f_{m,Q}$, we can update it by:

$$f_{2m,Q}(x,y) \leftarrow f_{m,Q}^2(x,y) \cdot L_{\phi(T),\phi(T)}(x,y)$$

where the function $L_{\phi(T),\phi(T)}(x,y)$ is given by:

$$L_{\phi(T),\phi(T)}(x,y) = Z_{[2]T}Z_T^2 y - (2Y_T^2\xi + (xZ_T^2 - X_T\xi) \cdot \beta_{[2]T})v.$$

The values $Z_{[2]T}, \beta_{[2]T}$, Y_T^2 and Z_T^2 have been obtained in the calculations of $[2]T$. Consequently, we execute the following sequence to compute $L_{\phi(T),\phi(T)}([2]P)$ and $L_{\phi(T),\phi(T)}(\hat{\varphi}(P))$ as:

$$
\begin{aligned}
&B \leftarrow 2Y_T^2\xi,\ C \leftarrow \beta_{[2]T}Z_T^2,\ D \leftarrow \beta_{[2]T}X_T,\ E \leftarrow Z_{[2]T}Z_T^2,\\
&F \leftarrow E \cdot y_{[2]P},\ G \leftarrow E \cdot y_{\hat{\varphi}(P)},\ L_{\phi(T),\phi(T)}([2]P) \leftarrow F - (B + Cx_{[2]P} - D\xi)v,\\
&L_{\phi(T),\phi(T)}(\hat{\varphi}(P)) \leftarrow G - (B + Cx_{\hat{\varphi}(P)} - D\xi)v,
\end{aligned}
$$

which requires $3\mathbf{m}_{11}$+$44\mathbf{m}$.

The two values we need to update: $L_{\phi(T),\phi(T)}([2]P)$ and $L_{\phi(T),\phi(T)}(\hat{\varphi}(P))$ can be done by performing $2\mathbf{m}_{22}$+$2\mathbf{s}_{22}$ at last. Hence the total cost of the shared doubling step is:

$$
\begin{aligned}
\mathrm{Cost}_{\mathrm{SDBL}} &= 3\mathbf{m_{11}} + 5\mathbf{s_{11}} + 3\mathbf{m_{11}} + 44\mathbf{m} + 2\mathbf{m_{22}} + 2\mathbf{s_{22}}\\
&= 2\mathbf{m_{22}} + 2\mathbf{s_{22}} + 6\mathbf{m_{11}} + 5\mathbf{s_{11}} + 44\mathbf{m}.
\end{aligned}
$$

In the first doubling step, we can set $T = Q' = (x_{Q'}, y_{Q'})$ and employ the mixed doubling formula in [4] to compute $[2]T$. The corresponding cost is:

$$
\mathrm{Cost}_{\mathrm{SDBL}_1} = 3\mathbf{m_{11}} + 5\mathbf{s_{11}} + 22\mathbf{m}.
$$

4.3 Cost analysis of pairing computation

In this subsection we first compare the computational cost of the optimal pairing on GG22D7-457 applying the formulas in [19] and ours. We also present the cost comparison with the curve KSS16-766. Finally, we implement our methods on RELIC and provide a performance comparison.

Note that $sopt(Q,P)^{p^{21}}$ is also bilinear. Recall from Eq. (12) in Section 4.1, it can be rewritten as:

$$
\left(\left(f_{-x,Q}^{2p^{21}}([2]P) \cdot \frac{M_1}{M_2}\right)^{\frac{-x+1}{4}} \cdot f_{-x,Q}(\hat{\varphi}(P))\right)^2 \cdot \frac{M_3}{M_4} \cdot \frac{M_2}{M_1}
$$

where the four functions $M_i,\ i = 1, \cdots, 4$ are given by:

$$
\begin{aligned}
M_1 =& \ell_{Q+T_2,Q+T_2}(\hat{\varphi}(P)),\ M_2 = \ell_{Q,Q}(\hat{\varphi}(P)),\\
M_3 =& f_{-x,Q}([2]P) \cdot \ell_{Q,Q}^{p}([2]P) \cdot \ell_{\pi([2]Q),[-x]Q}([2]P) \cdot \ell_{[-x]Q,Q+T_2}(\hat{\varphi}(P)),\\
M_4 =& f_{-x,Q}^{p^{21}}([2]P) \cdot \ell_{[-x]Q+T_2,Q}(\hat{\varphi}(P)).
\end{aligned}
$$

Since the embedding degree $k = 22$ is even, the inversion of an element in $\mathbb{F}_{p^{22}}$ can be replaced by multiplying its conjugate element. We apply the technique of 2-NAF to reduce the Hamming weight of the length of Miller loop. Thus the length of Miller loop $-x = 779523$ and the exponent $\frac{-x+1}{4} = 194881$ can be represented as:

$$
-x = [1\ 0\ -1\ 0\ 0\ 0\ 0\ -1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ -1]_2
$$

and

$$\frac{-x+1}{4} = [1\ 0\ -1\ 0\ 0\ 0\ 0\ -1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1]_2,$$

respectively. Since the 2-NAF representation of $-x$ has exactly two more bits than that of $\frac{-x+1}{4}$, we can share the computations of the exponentiation

$$\left(f_{-x,Q}^{2p^{21}}([2]P) \cdot \frac{M_1}{M_2}\right)^{\frac{-x+1}{4}}$$

and the Miller evaluation $f_{-x,Q}(\hat{\varphi}(P))$ by using the techniques in [20,33,9]. The computational process of

$$\left(f_{-x,Q}^{2p^{21}}([2]P) \cdot \frac{M_1}{M_2}\right)^{\frac{-x+1}{4}} \cdot f_{-x,Q}(\hat{\varphi}(P))$$

is illustrated in Algorithm 2.

Algorithm 2 Computing the value $\left(f_{-x,Q}^{2p^{21}}([2]P) \cdot \frac{M_1}{M_2}\right)^{\frac{-x+1}{4}} \cdot f_{-x,Q}(\hat{\varphi}(P))$.

Input: Three points $Q,\ [2]P,\ \hat{\varphi}(P)$, line function M_1 and the 2-NAF representation $-x = \sum_{i=0}^{N} n_i 2^i$ with $n_i \in \{-1, 0, 1\}$.

Output: The value $\left(f_{-x,Q}^{2p^{21}}([2]P) \cdot \frac{M_1}{M_2}\right)^{\frac{-x+1}{4}} \cdot f_{-x,Q}(\hat{\varphi}(P))$.

1: $T \leftarrow Q,\ f \leftarrow 1,\ g \leftarrow 1,\ tab \leftarrow [\ ],\ j \leftarrow 0$
2: **for** $i = N-1$ **to** 0 **do**
3: $\quad f \leftarrow f^2 \cdot \ell_{T,T}([2]P),\ tab[j] \leftarrow \ell_{T,T}(\hat{\varphi}(P)),\ T \leftarrow [2]T,\ j \leftarrow j+1$
4: $\quad$ **if** $i = N-1$ **then**
5: $\quad\quad M_2 \leftarrow \ell_{T,T}([2]P)$
6: $\quad$ **end if**
7: $\quad$ **if** $n_i = 1$ **then**
8: $\quad\quad f \leftarrow f \cdot \ell_{T,Q}([2]P),\ tab[j] \leftarrow \ell_{T,Q}(\hat{\varphi}(P)),\ T \leftarrow T+Q,\ j \leftarrow j+1$
9: $\quad$ **else if** $n_i = -1$ **then**
10: $\quad\quad f \leftarrow f \cdot \ell_{T,-Q}([2]P),\ tab[j] \leftarrow \ell_{T,-Q}(\hat{\varphi}(P)),\ T \leftarrow T-Q,\ j \leftarrow j+1$
11: $\quad$ **end if**
12: **end for** // $f = f_{-x,Q}([2]P)$
13: $j \leftarrow 0$
14: **for** $i = N-1$ **to** $N-2$ **do**
15: $\quad g \leftarrow g^2 \cdot tab[j],\ j \leftarrow j+1$
16: $\quad$ **if** $n_i = 1$ or $n_i = -1$ **then**
17: $\quad\quad g \leftarrow g \cdot tab[j],\ j \leftarrow j+1$
18: $\quad$ **end if**
19: **end for** // $g = f_{3,Q}(\hat{\varphi}(P))$
20: $h \leftarrow f^{2p^{21}} \cdot M_1 \cdot \overline{M_2} \cdot g,\ h_1 \leftarrow f^{2p^{21}} \cdot M_1 \cdot \overline{M_2}$
21: **for** $i = N-3$ **to** 0 **do**
22: $\quad h \leftarrow h^2 \cdot tab[j],\ j \leftarrow j+1$
23: $\quad$ **if** $n_i = 1$ or $n_i = -1$ **then**

$h \leftarrow h \cdot tab[j],\ j \leftarrow j+1$
end if
if $n_{i+2} = 1$ **then**
$h \leftarrow h \cdot h_1,\ j \leftarrow j+1$
else if $n_{i+2} = -1$ **then**
$h \leftarrow h \cdot \overline{h_1},\ j \leftarrow j+1$
end if
end for
return h

Thanks to the expansions of $-x$ and $\frac{-x+1}{4}$, it requires 6 shared addition steps, 20 shared doubling steps and the extra cost of $8\mathbf{m}_{22}+1\mathbf{s}_{22}+1\mathbf{f}_{22}$ to obtain

$$\left(f_{-x,Q}^{2p^{21}}([2]P) \cdot \frac{M_1}{M_2}\right)^{\frac{-x+1}{4}} \cdot f_{-x,Q}(\hat{\varphi}(P))$$

by Algorithm 2. The corresponding cost of Miller loop is:

$$\begin{aligned}\mathrm{Cost}_{\mathrm{Miller}} &= \mathrm{Cost}_{\mathrm{SDBL}_1} + 19\mathrm{Cost}_{\mathrm{SDBL}} + 6\mathrm{Cost}_{\mathrm{SADD}} + 8\mathbf{m_{22}} + 1\mathbf{s_{22}} + 1\mathbf{f_{22}} \\ &= 58\mathbf{m_{22}} + 39\mathbf{s_{22}} + 177\mathbf{m_{11}} + 118\mathbf{s_{11}} + 1122\mathbf{m} + 1\mathbf{f_{22}}.\end{aligned}$$

Note that the two values $\ell_{Q,Q}(\hat{\varphi}(P))$ and $\ell_{Q,Q}([2]P)$ have been obtained after executing the first shared doubling steps of $f_{-x,Q}(\hat{\varphi}(P))$ and $f_{-x,Q}([2]P)$, respectively. The point $[-x]Q$ is obtained after evaluating $f_{-x,Q}$. We apply the mixed addition formulas in [4] to compute $Q+T_2$ and $[-x]Q+T_2$ at a cost of $6\mathbf{m}_{11}+6\mathbf{s}_{11}+11\mathbf{m}$. Additionally, we perform $1\mathbf{m}_{11}+2\mathbf{f}_{11}$ to obtain the point $\pi([2]Q)$.

Computing the remaining four line functions requires $27\mathbf{m}_{11}+7\mathbf{s}_{11}+88\mathbf{m}$. We omit the specific cost calculation process of the above point additions and line function evaluations for simplicity. The details can be found in the accompanying code.

It remains to compute

$$\left(\left(f_{-x,Q}^{2p^{21}}([2]P) \cdot \frac{M_1}{M_2}\right)^{\frac{-x+1}{4}} \cdot f_{-x,Q}(\hat{\varphi}(P))\right)^2 \cdot \frac{M_3}{M_4} \cdot \frac{M_2}{M_1}.$$

The corresponding cost of the remaining accumulation is $8\mathbf{m}_{22}+1\mathbf{s}_{22}+2\mathbf{f}_{22}$. Consequently, the total cost of the Miller function evaluation is:

$$\begin{aligned}\mathrm{Cost}_{\mathrm{ML}} &= \mathrm{Cost}_{\mathrm{Init}} + \mathrm{Cost}_{\mathrm{Miller}} + \mathrm{Cost}_{\mathrm{Remain}} \\ &= 66\mathbf{m_{22}} + 40\mathbf{s_{22}} + 211\mathbf{m_{11}} + 131\mathbf{s_{11}} + 1236\mathbf{m} + 8\mathbf{s} + 3\mathbf{f_{22}} + 2\mathbf{f_{11}} + 1\mathbf{i}.\end{aligned}$$

The relative cost of multiplication, squaring, Frobenius endomorphism, inversion and exponentiation in $\mathbb{F}_p$, $\mathbb{F}_{p^{11}}$ or $\mathbb{F}_{p^{22}}$ are presented in Table 1 [19]. As for the exponentiation, we utilize addition chain to estimate $\mathbf{e}_x$ in $\mathbb{F}_{p^k}$, which requires

$6\mathbf{m}_k+18\mathbf{s}_k$.

Table 1. Cost of multiplication, squaring, Frobenius endomorphism, inversion and exponentiation in $\mathbb{F}_{p^k}$ [19] . The inversion in base field $\mathbb{F}_p$ is estimated with $\mathbf{i} = 25\mathbf{m}$.

k	$\mathbf{m}_k$	$\mathbf{s}_k$	$\mathbf{f}_k$	$\mathbf{i}_k$	$\mathbf{e}_x$
1	$\mathbf{m}$	$\mathbf{s}$	0	$25\mathbf{m}$	$6\mathbf{m} + 18\mathbf{s}$
11	$48\mathbf{m}$ [28]	$48\mathbf{s}$	$110\mathbf{m}$	$789\mathbf{m}$	$288\mathbf{m} + 864\mathbf{s}$
22	$3\mathbf{m}_{11} = 144\mathbf{m}$	$2\mathbf{m}_{11} = 96\mathbf{m}$	$231\mathbf{m}$	$981\mathbf{m}$	$864\mathbf{m} + 1728\mathbf{s}$

By setting $\mathbf{s} = \mathbf{m}$, we can estimate the cost of the Miller loop and the final exponentiation. Table 2 shows the computational cost comparison between the traditional optimal pairing and our new pairing formula on GG22D7-457. For the final exponentiation part, we refer to the SageMath code in [19] to obtain the corresponding cost.

Table 2. The cost of pairing computation exploiting optimal pairing and super-optimal pairing with 2-isogeny on curve GG22D7-457, including Miller function evaluation and the final exponentiation.

	This work	Optimal pairing [19]	Ratio
Miller loop	$31942\mathbf{m}$	$42276\mathbf{m}$	75.6%
Final exp	$73848\mathbf{m}$	$73848\mathbf{m}$	-
Pairing total	$105380\mathbf{m}$	$116124\mathbf{m}$	90.7%

From Table 2 we know that our new pairing formula using 2-isogeny outperforms the traditional optimal pairing in terms of the Miller loop on GG22D7-457, obtaining a saving of 24.4% of $\mathbb{F}_p$-multiplications. As for the whole pairing computation, we also achieve a reduction of 9.3% in terms of $\mathbb{F}_p$-multiplications.

4.4 Implementation results

Our implementation is based on RELIC, a cryptographic library for pairing-based protocols on popular pairing friendly curves. We integrate our code into RELIC and obtain performance comparisons of pairing computations between GG22D7-457 and other popular curves at 192-bit security level. The code is compiled and benchmarked on Intel(R) Core(TM) i9-12900K 3.20 GHz with TurboBoost and hyperthreading features disabled. Table 3 illustrates the detail of comparisons for pairing computations among different pairing-friendly curves.

According to Table 3, the Miller loop of super-optimal pairing utilizing 2-isogeny is 26.0% faster than using optimal pairing on GG22D7-457. Compared to the other curves, the optimized Miller loop on GG22D7-457 is about 23.3%, 4.7% and 8.3% faster than that on curves KSS16-766, KSS18-638 and FM18-768, while 22.9%, 8.9% and 41.5% slower than on curves AFG16-766, FM16-765 and BLS24-509. In terms of the whole pairing computation, after applying 2-isogeny, GG22D7-457 is 24.6%, 10.4%, 27.0% and 22.5% faster than curves KSS16-766, AFG16-766, FM16-765 and FM18-768, while 13.1% and 49.7% slower than curves KSS18-638 and BLS24-509. The results show that the curve GG22D7-457 can be

Table 3. Benchmarking results of pairing computations among different pairing-friendly curves at 192-bit security level, reported in 10^3 clock cycles in a 64-bit processor. The results are averaged over 10^4 executions.

Curve	Miller loop	Final exp	pairing total
GG22D7-457, $D = 7$ (This work)	7168	15764	22933
GG22D7-457, $D = 7$ (opt)	9691	15647	25539
KSS16-766 [19], $D = 1$ (opt)	9349	21077	30427
AFG16-766 [35], $D = 1$ (opt)	5525	20082	25607
FM16-765 [14], $D = 1$ (opt)	6526	24826	31413
KSS18-638 [19], $D = 3$ (opt)	7518	12405	19922
FM18-768 [14], $D = 3$ (opt)	7813	21782	29595
BLS24-509 [19], $D = 3$ (opt)	4190	7348	11538

regarded as an alternative choice, which depends on the protocols requirements and performance trade-off. This curve may benefit from efficient performance for operations in $\mathbb{G}_1$ since the characteristic p of the prime field is relatively small compared to other curves at the same security level. Thus it may be an appropriate choice if a protocol requires fast operations such as group exponentiations in $\mathbb{G}_1$. Therefore, our techniques can be used to enhance the performance of pairing computations on more pairing-friendly curves with n-isogenies as their GLV-endomorphisms, making them be more competitive in pairing-based cryptography.

5 Conclusion and Future Work

In this work, we gave a research for the pairing friendly-curves equipped with n-isogenies ($n > 1$) as endomorphisms, especially curve GG22D7-457 at the 192-bit security level with several cryptographically great properties. To improve the performance of pairing computation on GG22D7-457, we first proposed new formulas for the super-optimal pairings on the curves with n-isogenies as GLV-endomorphisms and targeted the case $n = 2$ to this curve. Building upon this, we made a specific theoretical analysis of super-optimal pairing formulas on families of curves with $D = 7$ (GG22D7) and $D = 11$ (GG28D11), constructed by using 2-isogeny and 3-isogeny, respectively.

Additionally, we presented efficient implementation details of pairing computation on GG22D7-457 utilizing our methods, and made a concrete computational cost analysis. Our results illustrated that using our new super-optimal pairing formula can reduce about 24.4% $\mathbb{F}_p$-multiplications compared to the optimal ate pairing for the Miller loop on GG22D7-457. Furthermore, our methods made GG22D7-457 a little bit win out in the performance of Miller loop compared to the well-known curves KSS16-766, KSS18-638 and FM18-768, even though it is still slower than the curves AFG16-766, FM16-765 and BLS24-509.

In conclusion, the techniques in this work extend the application of super-optimal pairings, and can be used to make more pairing-friendly curves become candidates for constructing pairing-based protocols.

Acknowledgement

References

1. Aranha, D.F., El Housni, Y., Guillevic, A.: A survey of elliptic curves for proof systems. Designs, Codes and Cryptography **91**(11), 3333–3378 (2023)
2. Aranha, D.F., Fotiadis, G., Guillevic, A.: A short-list of pairing-friendly curves resistant to the special TNFS algorithm at the 192-bit security level. Cryptology ePrint Archive, Paper 2024/1223 (2024), https://eprint.iacr.org/2024/1223, https://eprint.iacr.org/2024/1223
3. Aranha, D.F., Fuentes-Castañeda, L., Knapp, E., Menezes, A., Rodríguez-Henríquez, F.: "Implementing Pairings at the 192-Bit Security Level". In: Abdalla, M., Lange, T. (eds.) Pairing-Based Cryptography – Pairing 2012. pp. 177–195. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
4. Bernstein, D.J.: Explicit-formulas database. http://www. hyperelliptic. org/EFD (2007)
5. Boneh, D., Franklin, M.: "Identity-Based Encryption from the Weil Pairing". In: Kilian, J. (ed.) Advances in Cryptology — CRYPTO 2001. pp. 213–229. Springer Berlin Heidelberg, Berlin, Heidelberg (2001)
6. Boneh, D., Lynn, B., Shacham, H.: "Short Signatures from the Weil Pairing". In: Boyd, C. (ed.) Advances in Cryptology — ASIACRYPT 2001. pp. 514–532. Springer Berlin Heidelberg, Berlin, Heidelberg (2001)
7. Brickell, E., Li, J.: Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities. IEEE Transactions on Dependable and Secure Computing **9**(3), 345–360 (2012). https://doi.org/10.1109/TDSC.2011.63
8. Chen, L., Kudla, C.: Identity based authenticated key agreement protocols from pairings. In: 16th IEEE Computer Security Foundations Workshop, 2003. Proceedings. pp. 219–233 (2003)
9. Dai, Y., He, D., Peng, C., Yang, Z., an Zhao, C.: Revisiting Pairing-friendly Curves with Embedding Degrees 10 and 14. Cryptology ePrint Archive, Paper 2023/1958 (2023), https://eprint.iacr.org/2023/1958, https://eprint.iacr.org/2023/1958
10. Dai, Y., Zhang, F., Zhao, C.a.: Don't Forget Pairing-Friendly Curves with Odd Prime Embedding Degrees. IACR Transactions on Cryptographic Hardware and Embedded Systems **2023**(4), 393–419 (Aug 2023)
11. El Housni, Y., Guillevic, A.: "Optimized and Secure Pairing-Friendly Elliptic Curves Suitable for One Layer Proof Composition". In: Krenn, S., Shulman, H., Vaudenay, S. (eds.) Cryptology and Network Security. pp. 259–279. Springer International Publishing, Cham (2020)
12. El Housni, Y., Guillevic, A.: Families of SNARK-Friendly 2-Chains of Elliptic Curves. In: Dunkelman, O., Dziembowski, S. (eds.) Advances in Cryptology – EUROCRYPT 2022. pp. 367–396. Springer International Publishing, Cham (2022)
13. El Mrabet, N., Joye, M.: Guide to pairing-based cryptography. CRC Press (2017)

14. Fotiadis, G., Konstantinou, E.: TNFS resistant families of pairing-friendly elliptic curves. Theoretical Computer Science **800**, 73–89 (2019), special issue on Refereed papers from the CAI 2017 conference
15. Fouotsa, E., Guimagang, L.A., Ayissi, R.: x-superoptimal pairings on elliptic curves with odd prime embedding degrees: BW 13-P 310 and BW 19-P 286. Applicable Algebra in Engineering, Communication and Computing pp. 1–19 (2023)
16. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Journal of cryptology **23**, 224–280 (2010)
17. Galbraith, S.D.: Mathematics of Public Key Cryptography. Cambridge University Press, USA, 1st edn. (2012)
18. Gallant, R.P., Lambert, R.J., Vanstone, S.A.: "Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms". In: Kilian, J. (ed.) Advances in Cryptology — CRYPTO 2001. pp. 190–200. Springer Berlin Heidelberg, Berlin, Heidelberg (2001)
19. Gasnier, J., Guillevic, A.: An Algebraic Point of View on the Generation of Pairing-Friendly Curves (Sep 2023), https://hal.science/hal-04205681, working paper or preprint
20. Granger, R., Smart, N.P.: On computing products of pairings. Cryptology ePrint Archive, Paper 2006/172 (2006), https://eprint.iacr.org/2006/172, https://eprint.iacr.org/2006/172
21. Guillevic, A.: "A Short-List of Pairing-Friendly Curves Resistant to Special TNFS at the 128-Bit Security Level". In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) Public-Key Cryptography – PKC 2020. pp. 535–564. Springer International Publishing, Cham (2020)
22. Hess, F., Smart, N., Vercauteren, F.: The Eta Pairing Revisited. IEEE Transactions on Information Theory **52**(10), 4595–4602 (2006)
23. Joux, A.: A one round protocol for tripartite Diffie–Hellman. Journal of cryptology **17**(4), 263–276 (2004)
24. Kachisa, E.J., Schaefer, E.F., Scott, M.: "Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field". In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing-Based Cryptography – Pairing 2008. pp. 126–135. Springer Berlin Heidelberg, Berlin, Heidelberg (2008)
25. Kim, T., Barbulescu, R.: "Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case". In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology – CRYPTO 2016. pp. 543–571. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
26. Miller, V.S.: The weil pairing, and its efficient calculation. Journal of cryptology **17**, 235–261 (2004)
27. Minkowski, H.: Geometrie der zahlen. BG Teubner (1910)
28. Montgomery, P.: Five, six, and seven-term Karatsuba-like formulae. IEEE Transactions on Computers **54**(3), 362–369 (2005)
29. Pollard, J.M.: Monte Carlo methods for index computation (mod p). Mathematics of computation **32**(143), 918–924 (1978)
30. Qi, Y.F., Tang, C.M., Guo, B., Xu, M.Z.: Super-optimal pairings. Applied Mechanics and Materials **281**, 127–133 (2013)
31. Schirokauer, O.: Discrete logarithms and local units. Philosophical Transactions of the Royal Society of London. Series A: Physical and Engineering Sciences **345**(1676), 409–423 (1993)
32. Scott, M.: "Faster Pairings Using an Elliptic Curve with an Efficient Endomorphism". In: Maitra, S., Veni Madhavan, C.E., Venkatesan, R. (eds.) Progress in

Cryptology - INDOCRYPT 2005. pp. 258–269. Springer Berlin Heidelberg, Berlin, Heidelberg (2005)
33. Scott, M.: On the efficient implementation of pairing-based protocols. In: Chen, L. (ed.) Cryptography and Coding. pp. 296–308. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
34. Scott, M.: Unbalancing pairing-based key exchange protocols. Cryptology ePrint Archive (2013)
35. Scott, M., Guillevic, A.: A new family of pairing-friendly elliptic curves. In: Budaghyan, L., Rodríguez-Henríquez, F. (eds.) "Arithmetic of Finite Fields". pp. 43–57. Springer International Publishing, Cham (2018)
36. Silverman, J.H.: The arithmetic of elliptic curves. In: Graduate texts in mathematics (1986)
37. Vélu, J.: Isogénies entre courbes elliptiques. CR Acad. Sci. Paris, Séries A **273**, 305–347 (1971)
38. Vercauteren, F.: Optimal Pairings. IEEE Transactions on Information Theory **56**(1), 455–461 (Jan 2010)
39. Washington, L.C.: Elliptic curves: number theory and cryptography. Chapman and Hall/CRC (2008)
40. Yang, K., Chen, L., Zhang, Z., Newton, C.J.P., Yang, B., Xi, L.: Direct Anonymous Attestation With Optimal TPM Signing Efficiency. IEEE Transactions on Information Forensics and Security **16**, 2260–2275 (2021). https://doi.org/10.1109/TIFS.2021.3051801
41. Yoon, K.: A new method of choosing primitive elements for Brezing–Weng families of pairing-friendly elliptic curves. Journal of Mathematical Cryptology **9**(1), 1–9 (2015)
42. Zhao, C.A., Xie, D., Zhang, F., Zhang, J., Chen, B.L.: Computing bilinear pairings on elliptic curves with automorphisms. Des. Codes Cryptography **58**(1), 35–44 (jan 2011)