Efficient Algorithms for $\mathbb{G}_2$ Subgroup Membership Testing on Pairing-Friendly Curves

Jianming Lin[1,2], Yu Dai[3], Chang-An Zhao[2,4*], Yuhao Zheng[2]

[1]School of Mathematics, Jiaying University, Meizhou, 514015, Guangdong, China.
[2]School of Mathematics, Sun Yat-sen University, Guangzhou, 510275, Guangdong, China.
[3]School of Mathematics and Statistics, Wuhan University of Technology, Wuhan, 430072, Hubei, China.
[4]Guangdong Provincial Key Laboratory of Information Security Technology, Guangzhou, 510006, Guangdong, China.

*Corresponding author(s). E-mail(s): zhaochan3@mail.sysu.edu.cn;
Contributing authors: linjm76@mail.sysu.edu.cn; eccdaiy39@gmail.com;
zhengyh57@mail2.sysu.edu.cn;

Abstract

Subgroup membership testing serves as a crucial countermeasure against small subgroup attacks, thereby ensuring the security of pairing-based cryptographic protocols. Despite its vital importance, the expensive computational requirements for membership testing on specific pairing-friendly curves pose a non-negligible challenge. In this paper, we revisit the $\mathbb{G}_2$ membership testing algorithms on KSS16 curves and propose a novel approach specifically designed for the families constructed by the KSS method (Kachisa-Schaefer-Scott method). Moreover, we generalize several previous methods for $\mathbb{G}_2$ membership testing, rendering them applicable to more generic pairing-friendly curves. Specifically, we implement an efficient $\mathbb{G}_2$ membership testing on three well-known curves KSS16-329, KSS16-330, and KSS16-766 for verification. The experimental results illustrate that our new method achieves improvements of **24.0%**, **33.3%**, and **29.2%** in terms of clock cycles compared to the state-of-the-art, respectively.

Keywords: Small subgroup attacks Subgroup membership Testing KSS curves Efficiently computable endomorphisms

1 Introduction

In the realm of public-key cryptography, bilinear pairings on elliptic curves have become a significant component of many cryptographic protocols, such as identity-based encryption [10], authentication scheme [43], short signatures [11], zero-knowledge proof [17, 18], and blockchain-based systems [37]. The subgroups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are three cyclic groups with large prime order r involved in a pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, which is a bilinear map on an elliptic curve E. Denote by k and $\mathbb{F}_{p^k}$ the embedding degree of E with respect to r and a finite field of p^k elements, respectively. Within this framework, the two input groups $\mathbb{G}_1$ and $\mathbb{G}_2$ emerge as the subgroups of $E(\mathbb{F}_{p^k})$, while the output group $\mathbb{G}_T \subseteq \mathbb{F}_{p^k}^*$. The security of pairing-based protocols relies on the difficulty of solving discrete logarithm problems (DLP) in these three subgroups mentioned above [16, 26, 41].

Nevertheless, if the communication channel is insecure, the attackers may force the running system to return a point with a small order. Thus, there is a potential probability that the cryptographic systems suffer from the small-subgroup attacks [6, 36]. Two feasible countermeasures, named cofactor clearing and subgroup membership testing, have been proposed to avert such vulnerabilities.

The cofactor clearing is to multiply the target points Q hashed on the corresponding curves [20] by the cofactor to make the candidate elements within the expected subgroups of order r. This approach is efficient when working on $\mathbb{G}_1$ since the corresponding cofactor h_1 is relatively small. In 2022, Housni, Guillevic, and Piellard investigated cofactor clearing and proposed an efficient algorithm on $\mathbb{G}_1$ [19]. In the situation of $\mathbb{G}_2$, the cofactor h_2 becomes crucially large. Even though the tools in [13, 22, 33, 40] can be exploited to reduce the sizes of scalar multiplications, this algorithm is still cumbersome. Furthermore, cofactor clearing may bring several extra problems since it necessitates alterations to the parameters of the protocols, often impeding the implementation [39].

Troubles arising from cofactor clearing can be circumvented by performing subgroup membership testing, which is designed to determine whether the candidate element belongs to the prime-order subgroup $\mathbb{G}_2$. A naive approach is to multiply the element by r (raise the element to the power of r in the case of $\mathbb{G}_T$) and verify its equivalence to the identity element $\mathcal{O}_E \in E(\mathbb{F}_{p^k})$ ($1 \in \mathbb{F}_{p^k}$ in the case of $\mathbb{G}_T$). However, this method leads to a huge computational cost and significantly weakens the performance of the whole protocol. In 2021, Scott [39] introduced efficient algorithms for the subgroup membership testing for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on the BLS family [7]. This approach was subsequently generalized by Housni, Guillevic and Piellard [19] to the BN family [8]. In 2023, Dai *et al.* [15] proposed new techniques of the membership testing (DLZZ criterion [3]) for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$, which are suitable for a broader class of pairing-friendly curves with j-invariants 0 or 1728, including BN, BLS and BW [21] families. Koshelev [34] leveraged the information of the cofactor h and proposed efficient techniques for testing the memberships of points in the prime-order subgroups of elliptic curves over finite fields by employing Tate pairings, under the condition that h is relatively small. More recently, based on Koshelev's method, Dai *et al.* [14] proposed a new approach to accelerate the $\mathbb{G}_1$ membership testing on BLS and BW curves.

In recent years, the demand for high-assurance pairing-based cryptographic systems has extended beyond the 128-bit security level offered by popular families of pairing-friendly curves such as BN and BLS12. As applications including identity-based encryption [10] and advanced zero-knowledge proof frameworks [17, 18] evolve toward stronger security guarantees and more complex multi-pairing computations, elliptic curves with higher embedding degrees have become increasingly relevant. Within this context, the Kachisa-Schaefer-Scott (KSS) [30] family, particularly family KSS16 offers a well-balanced trade-off between high security (approximately 192-bit) and practical efficiency in extension-field arithmetic. Aranha *et al.* [4] demonstrated that optimized pairing implementations at the 192-bit security level are practical, identifying implementation techniques and candidate curves, including KSS16, suitable for high-security deployment. Moreover, in light of advances in discrete logarithm algorithms, particularly the extended Number Field Sieve (exTNFS) [32], Barbulescu and Duquesne's [5] revised security estimates under the exTNFS attack framework and provided updated parameter recommendations for several major families, including KSS16. Their results show that KSS16 remains a viable candidate at the 192- and even 256-bit security levels when appropriate parameter sizes are selected, thereby reinforcing its relevance for applications that require long-term or high-assurance security guarantees.

The KSS16 curves have been identified as a promising candidate for cryptographic protocols that require multiple or chained bilinear operations, such as proof aggregation and recursive verification in modern proof systems [46]. Recent literature underscores this relevance. Zhang and Lin [46] concluded that KSS16 is among the most efficient choices for computing products/quotients of pairings at the 192-bit level. Aranha, Housni, and Guillevic [2] highlighted the emerging importance of family KSS16 for succinct non-interactive arguments of knowledge (SNARKs) and other proof frameworks. They emphasize that, beyond raw pairing efficiency, such pairing-friendly curves must support composability, high 2-adicity, and favorable extension-field structures, which demonstrates strong potential. Besides, KSS16 curves have been incorporated in several well-known high-performance cryptographic libraries, such as RELIC [1] and ELiPS [31] for the research at high security levels. In conclusion, KSS16 represents an effective alternative ext-generation cryptographic protocols that integrate proof composition, privacy-preserving computation, and long-term cryptographic soundness within a unified, pairing-friendly framework. Up to now, there has been a lack of research that systematically focuses on the $\mathbb{G}_2$ membership testing on the KSS family. Motivated by this gap, we explore deriving an efficient approach for the $\mathbb{G}_2$ membership testing tailored to the KSS family.

1.1 Our Contributions

In this paper, we revisit the previous methods for $\mathbb{G}_2$ membership testing, then propose some new and more extensive algorithms. We first provide an efficient algorithm for the $\mathbb{G}_2$ membership testing on the KSS family [30] admitting fast pairing computations. Moreover, we extend Scott's method and DLZZ criterion to more generic families of pairing-friendly curves. In more detail, our contributions are summarized as follows:

1. We first concentrate on the KSS family and develop an effective algorithm for $\mathbb{G}_2$ membership testing that leverages some specific properties of this family. Our algorithm is tailored to family KSS16, which is one of the efficient choices for pairing computations on curves at 128-bit security level [5]. In particular, our new method demonstrates a substantial improvement in performance over DLZZ criterion on two popular pairing-friendly curves KSS16-330 [1] and KSS16-329 [2], that can be suitable for SNARKs [17, 18] (Succinct Non-interactive ARguments of Knowledge).
2. We generalize Scott's method for the $\mathbb{G}_2$ membership testing by relaxing the corresponding condition, making it applicable to a wider class of pairing-friendly curves. This generalization outperforms DLZZ criterion on curve BLS27-426 ensuring the 192-bit security level [3], which admits an efficient $\mathbb{G}_1$ arithmetic among 192-bit security curves and possesses potential to be utilized in DAA (Direct Anonymous Attestation) schemes [44].
3. Moreover, we extend the techniques proposed by Dai *et al.* to any families of GLV-curves [25] equipped with degree-n endomorphisms ($n \geq 2$) besides the curves with CM-discriminants 1 or 3, and give the condition that determines whether the computational cost can be reduced to $\log_2(r)/2\varphi(k)$ bit operations. This idea can also be employed to extend DLZZ criterion for $\mathbb{G}_1$ membership testing on more pairing-friendly curves.
4. Finally, we implement our methods on three KSS16 curves in RELIC. The experimental results illustrate that our new methods obtain an enhancement of about **24.0%**, **33.3%** and **29.2**% in terms of CPU clock cycles compared to DLZZ criterion for the $\mathbb{G}_2$ membership testing on KSS16-329, KSS16-330 and KSS16-766, respectively. Our source code is available at

   https://github.com/SMtestings/relic-G2MT-KSS16.

1.2 Organizations of This Paper.

The remainder of this paper is outlined as follows. Section 2 presents the definitions of the pairing subgroups, GLV-endomorphisms of ordinary elliptic curves, along with the KSS construction. The efficient methods for the $\mathbb{G}_2$ membership testing are described in Sections 3. In Section 4, we provide the concrete cost analysis and experimental results. The conclusion is presented in Section 5.

2 Mathematical Background

In this section, we first introduce the fundamental concepts of the three pairing subgroups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$. Subsequently, we provide a concise overview of the efficiently computable endomorphisms on ordinary curves. Moreover, we also briefly present the KSS method [30]. The notations throughout this paper are first introduced.

Notations. Let $\mathbf{m}$ represent the multiplication in the base field $\mathbb{F}_p$, with the characteristic p of 6 digits. Denote by $\mathbf{m}_k$, $\mathbf{s}_k$ and $\mathbf{f}_k$ the costs of a multiplication, a squaring and a Frobenius endomorphism in $\mathbb{F}_{p^k}$, respectively. For simplicity, we omit the calculations for the addition/subtraction and the operations in the subfields of $\mathbb{F}_{p^4}$.

2.1 Pairing Subgroups on Ordinary Elliptic Curves

Denote by E an ordinary elliptic curve over a finite field $\mathbb{F}_p$, where p and $\mathcal{O}_E$ are a large prime and the identity element in E, respectively. Let $\#E(\mathbb{F}_p)$ represent the group order of $E(\mathbb{F}_p)$. Then we have $\#E(\mathbb{F}_p) = p + 1 - t$ [42, Chapter 4.3], with t the trace of p-power Frobenius endomorphism $\pi : (x, y) \to (x^p, y^p)$ satisfying the characteristic equation

$$\pi^2 - t\pi + p = 0.$$

Let r be a large prime factor of $\#E(\mathbb{F}_p)$. Define the embedding degree k with respect to r to be the smallest positive integer satisfying $r \mid p^k - 1$. We denote the eigenspaces of π acting on the r-torsion group $E[r] = \{P \in E \mid [r]P = \mathcal{O}_E\}$ with eigenvalues 1 and p as $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. More precisely, these two pairing subgroups can be expressed as:

$$\mathbb{G}_1 = E(\mathbb{F}_p)[r], \quad \mathbb{G}_2 = E(\mathbb{F}_{p^k})[r] \cap \ker(\pi - [p]).$$

Suppose that E admits a degree-d twist E' defined over $\mathbb{F}_{p^e}$, where $e = k/d$. Define $\phi : E' \to E$ to be the twisting isomorphism. Then $\mathbb{G}_2$ can be concisely represented as $\mathbb{G}_2 = E'(\mathbb{F}_{p^e})[r]$. On this basis, the straightforward methods for $\mathbb{G}_2$ membership testing are presented as follows

1. For curves admitting a twist: $Q \in \mathbb{G}_2 = E'(\mathbb{F}_{p^e})[r] \Leftrightarrow Q \in E'(\mathbb{F}_{p^e})$ and $[r]Q = \mathcal{O}_{E'}$.
2. For curves without a twist: $Q \in \mathbb{G}_2 = E(\mathbb{F}_{p^k})[r] \cap \ker(\pi - [p]) \Leftrightarrow Q \in E(\mathbb{F}_{p^k}), [r]Q = \mathcal{O}_E$ and $\Phi_k(\pi)(Q) = \mathcal{O}_E$,

where Φ_k denotes the k-th cyclotomic polynomial.

2.2 Efficiently Computable Endomorphisms of Ordinary Curves

In this subsection, we introduce the efficiently computable endomorphisms of ordinary curves. Define D as a positive square-free integer such that $4p - t^2 = Dy^2$, $y \in \mathbb{Z}$. According to [42, Chapter 10.2], the endomorphism ring of an ordinary curve E over a finite field is isomorphic to an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$. The largest subring of $\mathbb{Q}(\sqrt{-D})$ is

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

An **order** $R = \mathbb{Z} + \mathbb{Z}f\delta$ in $\mathbb{Q}[\sqrt{-D}]$ is a subring of $\mathcal{O}_K$ such that $\mathbb{Z} \subsetneq R \subseteq \mathcal{O}_K$ [42, Chapter 10.2], where $f > 0$ and $\delta = \frac{1+\sqrt{-D}}{2}$ or $\sqrt{-D}$. Let $\sigma \in \mathrm{End}_p(E)$ be an endomorphism of E over $\mathbb{F}_p$. Thus σ can be represented as $\sigma = a + b\sqrt{-D}$, where $a, b \in \mathbb{Q}$ and $2a, 2b \in \mathbb{Z}$. Define $\mathrm{Nrd}(\sigma) = \sigma\bar{\sigma} = (a + b\sqrt{-D})(a - b\sqrt{-D})$ to be the norm of σ.

An endomorphism σ with norm n is named as a degree-n endomorphism, which satisfies the following characteristic equation

$$\sigma^2 - 2a\sigma + n = 0. \tag{1}$$

This morphism enables scalar multiplication by λ_1 (resp. λ_2) on points in $\mathbb{G}_1$ (resp. $\mathbb{G}_2$), where λ_1 and λ_2 are the two distinct roots of the above equation. A degree-1 endomorphism of E is exactly the automorphism.

In the following, we introduce some common endomorphisms of ordinary curves. First, consider an ordinary curve $E : y^2 = x^3 + b,\ b \in \mathbb{F}_p$ with $D = 3$ and $p \equiv 1 \pmod 3$. There is an endomorphism $\sigma : (x, y) \to (\alpha x, y)$ on E with $\sigma = \frac{1+\sqrt{-3}}{2}$, where α is a primitive cube root of unity in $\mathbb{F}_p^*$. According to Eq. (1), σ satisfies $\sigma^2+\sigma+1 = 0$.

Similarly, for an elliptic curve $E : y^2 = x^3 + ax,\ a \in \mathbb{F}_p$ with $D = 1$ and $p \equiv 1 \pmod 4$, there exists an endomorphism $\sigma : (x, y) \to (-x, \beta y)$ on E, where β is a fourth primitive root of unity in $\mathbb{F}_p^*$. This efficiently computable endomorphism satisfies the characteristic equation $\sigma^2 + 1 = 0$ since $\sigma = \sqrt{-1}$.

These two endomorphisms allow for efficient scalar multiplications by employing the GLV method [25]. We refer to such endomorphisms as GLV-endomorphisms. A curve equipped with such an endomorphism is called a GLV-curve.

Additionally, the twisting isomorphism ϕ induces an endomorphism $\psi = \phi^{-1} \circ \pi \circ \phi$ [24] on E', satisfying the corresponding characteristic equation $\psi^2 - t\psi + p = 0$. The action of ψ on $Q \in \mathbb{G}_2 = E'(\mathbb{F}_{p^e})[r]$ allows for a scalar multiplication $[t - 1]$. This endomorphism has been used for enhancing the efficiency of scalar multiplications in $\mathbb{G}_2$ [24].

2.3 The DLZZ Criterion

We briefly recall the method of Dai, Lin, Zhao, and Zhou [15]. Let $q = p^e$, write $\#E'(\mathbb{F}_q) = h_2 r$, and let

$$L_\psi = \left\{ (c_0, \ldots, c_{\varphi(k)-1}) \in \mathbb{Z}^{\varphi(k)} : \sum_{i=0}^{\varphi(k)-1} c_i p^i \equiv 0 \pmod r \right\}.$$

The lattice has the natural basis

$$(r, 0, \ldots, 0),\ (-p, 1, 0, \ldots, 0), \ldots, \big(-p^{\varphi(k)-1}, 0, \ldots, 0, 1\big).$$

LLL reduction is used off-line to find a short vector $C = (c_0, \ldots, c_{\varphi(k)-1}) \in L_\psi$. Define

$$h_C(T) = \sum_{i=0}^{\varphi(k)-1} c_i T^i, \qquad g_\psi(T) = T^2 - tT + p.$$

Reducing h_C modulo g_ψ gives $h_C(T) \equiv b_0 + b_1 T \pmod{g_\psi(T)}$. Consequently,

$$\mathrm{Res}(h_C, g_\psi) = b_0^2 + b_0 b_1 t + b_1^2 p.$$

If

$$\gcd\big(\mathrm{Res}(h_C, g_\psi), h_2 r\big) = r, \tag{2}$$

then, for a non-identity point $Q \in E'(\mathbb{F}_q)$,

$$Q \in \mathbb{G}_2 \quad \Longleftrightarrow \quad \sum_{i=0}^{\varphi(k)-1} [c_i]\psi^i(Q) = \mathcal{O}_{E'}.$$

Indeed, the displayed endomorphism relation implies that $\mathrm{ord}(Q)$ divides the resultant, while $Q \in E'(\mathbb{F}_q)$ implies that $\mathrm{ord}(Q) \mid h_2 r$; condition (2) leaves only the r-part. The vector $(r, 0, \ldots, 0)$ always recovers the naive test, whereas a short LLL vector reduces the scalar lengths to approximately $\log_2(r)/\varphi(k)$ bits. Sections 3.1–3.3 replace or enlarge the endomorphism and lattice choices used by this criterion.

2.4 Reduced Tate Pairings and Power-Residue Symbols

The pairing filters in Sections 3.1 and 3.2 use the reduced Tate pairing. Let c be coprime to p, $c \mid q-1$, and let $P \in E'(\mathbb{F}_q)[c]$. For a divisor representative $D_Q = (Q+R) - (R)$ whose support is disjoint from that of the Miller function,

$$t_c(P, Q) = f_{c,P}(D_Q)^{(q-1)/c} \in \mu_c, \ \mathrm{div}(f_{c,P}) = c(P) - c(\mathcal{O}_{E'}).$$

The auxiliary point R avoids zeros and poles, and it can be omitted whenever the usual affine formula is known to be well defined. Algorithm 1 gives an implementation-oriented description, which is called Miller's algorithm [38]. The notation $\ell_{A,B}$ denotes the line passing through A and B (the tangent when $A = B$), and v_A is the vertical line passing through A and $-A$.

When c is small, the final pairing value often reduces to a c-th power-residue symbol. For $a \in \mathbb{F}_{p^e}^*$ and $c \mid p-1$,

$$\left(\frac{a}{p^e}\right)_c = a^{(p^e-1)/c} = N_{\mathbb{F}_{p^e}/\mathbb{F}_p}(a)^{(p-1)/c}.$$

Algorithm 2 computes the norm with Frobenius maps and then evaluates the symbol in the base field. For $c = 2$, the last step is the Legendre symbol and can be computed by the binary Jacobi algorithm using quadratic reciprocity. For small odd c, a degree-specific reciprocity algorithm may be used [29, 34].

The norm stage costs $(e-1)$ Frobenius actions and $(e-1)$ multiplications in $\mathbb{F}_{p^e}$. In particular, for $e = 4$ and $c = 2$, the cost is $3\mathbf{f}_4 + 3\mathbf{m}_4$, apart from the inexpensive binary Jacobi computation in $\mathbb{F}_p$.

2.5 The KSS Construction

Kachisa, Schaefer and Scott [30] proposed a method (KSS method) for constructing pairing-friendly curves based on the Brezing-Weng method (BW method) [12]. Using the BW method with a non-cyclotomic polynomial, the authors in [30] constructed a list of pairing-friendly curves with embedding degrees 16 and 18. In the following, we briefly describe this method.

Algorithm 1 Reduced Tate pairing $t_c(P, Q)$

Input: $P \in E'(\mathbb{F}_q)[c]$, $Q \in E'(\mathbb{F}_q)$, and $R \in E'(\mathbb{F}_q)$ avoiding all zeros and poles of the Miller functions.

Output: $t_c(P, Q) \in \mu_c$.

1. Write $c = (1 b_{\ell-1} \cdots b_0)_2$.
2. Set $T \leftarrow P$, $u \leftarrow 1$, and $v \leftarrow 1$.
3. **for** $i = \ell - 1, \ldots, 0$ **do**
4. $\quad u \leftarrow u^2 \dfrac{\ell_{T,T}(Q+R)}{v_{[2]T}(Q+R)}$.
5. $\quad v \leftarrow v^2 \dfrac{\ell_{T,T}(R)}{v_{[2]T}(R)}$.
6. $\quad T \leftarrow [2]T$.
7. $\quad$ **if** $b_i = 1$ **then**
8. $\quad\quad u \leftarrow u \dfrac{\ell_{T,P}(Q+R)}{v_{T+P}(Q+R)}$.
9. $\quad\quad v \leftarrow v \dfrac{\ell_{T,P}(R)}{v_{T+P}(R)}$.
10. $\quad\quad T \leftarrow T + P$.
11. $\quad$ **end if**
12. **end for**
13. **return** $\left(\dfrac{u}{v}\right)^{(q-1)/c}$.

Algorithm 2 c-th power-residue symbol in $\mathbb{F}_{p^e}$

Input: $a \in \mathbb{F}_{p^e}$ and a small integer $c \mid p - 1$.

Output: $\left(\dfrac{a}{p^e}\right)_c \in \mu_c \cup \{0\}$.

1. **if** $a = 0$ **then return** 0.
2. Set $z \leftarrow a$ and $N \leftarrow a$.
3. **for** $i = 1, \ldots, e - 1$ **do**
4. $\quad z \leftarrow z^p$.
5. $\quad N \leftarrow N \cdot z$.
6. **end for**
7. Regard N as an element of $\mathbb{F}_p$.
8. **if** $c = 2$ **then return** Jacobi$(\widetilde{N}, p)$, where $\widetilde{N}$ represents N.
9. **return** $N^{(p-1)/c}$, using an addition chain or a c-th reciprocity law.

Let $r(x)$, $t(x)$ and $p(x)$ respectively denote the parameterized polynomials of the prime factor r, the Frobenius trace t and the characteristic p. We set the number field $K = \mathbb{Q}(\zeta_k, \sqrt{-D})$, which contains the primitive k-th root ζ_k and $\sqrt{-D}$.

The polynomial $r(x)$ is defined to be the minimal polynomial of $\alpha = (a + b\sqrt{-D}) \cdot \zeta_k \in K$. Let $t(x)$, $y(x) \in \mathbb{Q}[x]/(r(x))$ be polynomials corresponding to $\zeta_k + 1$ and $\frac{\zeta_k - 1}{\sqrt{-D}}$

in K, respectively. Then $p(x) = \frac{t^2(x)+Dy^2(x)}{4}$ represents the parameterized polynomial of p such that

$$r(x) \mid p(x) + 1 - t(x) \text{ and } r(x) \mid\mid p^k(x) - 1.$$

Therefore, these three polynomials define a family of pairing-friendly curves. We present a well-known family called KSS16 for illustration.

Example 1 (KSS16)**.** *A family constructed from* $\alpha = \left(2\sqrt{-1} - 1\right) \cdot \zeta_{16}$ *with* $D = 1$ *and* $k = 16$*.*

$$\begin{aligned}
t(x) &= \frac{1}{35}(2x^5 + 41x + 35),\\
r(x) &= x^8 + 48x^4 + 625,\\
p(x) &= \frac{1}{980}(x^{10} + 2x^9 + 5x^8 + 48x^6 + 152x^5 + 240x^4 + 625x^2 + 2398x + 3125).
\end{aligned}$$

According to [5], KSS16 is one of the popular choices for the optimal ate pairing computation on curves achieving the 128-bit security level.

3 Main Results

In this section, we present our methods of subgroup membership testing for $\mathbb{G}_2$ on pairing-friendly curves. We first provide a fast testing method on KSS curves. Besides, we extend the methods proposed in [39] and [15] to more pairing-friendly curves. In the remainder of this paper, we only consider the curve E admitting a degree-d twist E' defined over $\mathbb{F}_{p^{k/d}} = \mathbb{F}_{p^e}$. Denote by h_1 and h_2 the cofactors $\#E(\mathbb{F}_p)/r$ and $\#E'(\mathbb{F}_{p^e})/r$, respectively.

3.1 An Efficient $\mathbb{G}_2$ Membership Testing on KSS Curves

In this subsection, we focus on the pairing-friendly curves constructed by the KSS method and give an efficiently tailored approach for the $\mathbb{G}_2$-membership testing on such curves. Moreover, we present the corresponding computation analysis and comparison on a specific family of curves called KSS16.

Recalled from Section 2.2, a degree-n endomorphism $\sigma \in \mathrm{End}_p(E)$ can be represented as $\sigma = a + b\sqrt{-D}$, where $a, b \in \mathbb{Q}$ and $a^2 + b^2D = n$. The KSS family is constructed by making $r(x)$ the minimal polynomial of the element

$$\alpha = (a + b\sqrt{-D}) \cdot \zeta_k.$$

Consequently, assume that E is a KSS curve admitting a degree-d twist, then for every $Q \in \mathbb{G}_2 = E'(\mathbb{F}_{p^e})[r]$ it yields that

$$\tau(Q) = [x]Q, \tag{3}$$

where the map $\tau = \phi^{-1} \circ \sigma \circ \pi \circ \phi$ and x are the composition of Φ, ψ, and the parametrized seed of E, respectively. Thus τ corresponds to the element $\alpha = (a + b\sqrt{-D}) \cdot \zeta_k \in \mathbb{Q}(\zeta_k, \sqrt{-D})$. Using the above notations, we present our approach for

the $\mathbb{G}_2$ membership testing on KSS curves. Lemma 1 illustrates the characteristic polynomial of the composite map τ.

Lemma 1 (Characteristic polynomial of τ)**.** *Let ψ correspond to*

$$\frac{t+\varepsilon f\sqrt{-D}}{2}, \qquad \varepsilon \in \{1,-1\}, \qquad Df^2 = 4p - t^2.$$

If $\sigma = a + b\sqrt{-D}$ has degree n, then

$$\chi_\tau(T) = T^2 - c_\tau T + np, \qquad c_\tau = at - \varepsilon bfD.$$

Proof. The norm of τ is

$$\tau\widehat{\tau} = \deg(\Phi)\deg(\psi) = np.$$

Moreover,

$$(a + b\sqrt{-D})\frac{t+\varepsilon f\sqrt{-D}}{2} = \frac{at - \varepsilon bfD + (\varepsilon af + bt)\sqrt{-D}}{2}.$$

Thus $\tau + \widehat{\tau} = at - \varepsilon bfD = c_\tau$, and the claimed characteristic polynomial follows. Notice in particular the minus sign in $T^2 - c_\tau T + np$. □

The following elementary group-structure observation is needed to handle a composite common cofactor correctly.

Lemma 2 (Rational torsion of a rank-two elliptic-curve group)**.** *Write*

$$E'(\mathbb{F}_q) \simeq \mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/(m_1 n_1 r)\mathbb{Z}, \qquad h_2 = m_1^2 n_1.$$

For every positive integer $u \mid h_2$,

$$E'(\mathbb{F}_q)[u] \simeq \mathbb{Z}/\gcd(u, m_1)\mathbb{Z} \oplus \mathbb{Z}/\gcd(u, m_1 n_1)\mathbb{Z}.$$

Consequently, $E'(\mathbb{F}_q)[u]$ is cyclic if and only if $\gcd(u, m_1) = 1$.

Proof. For a cyclic group $\mathbb{Z}/N\mathbb{Z}$, the kernel of multiplication by u has order $\gcd(u, N)$ and is isomorphic to $\mathbb{Z}/\gcd(u, N)\mathbb{Z}$. Applying this fact to the two invariant factors gives the result. □

Lemma 2 shows that the implication

$$u \parallel h_2 \quad \Longrightarrow \quad E'(\mathbb{F}_q)[u] \simeq \mathbb{Z}/u\mathbb{Z}$$

cannot be used when u is composite. For example, $u = 4$, $m_1 = 2$, and $n_1 = 2$ give $h_2 = 8$ and $E'(\mathbb{F}_q)[4] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, although $4 \mid h_2$ and $16 \nmid h_2$. The next theorem therefore neither assumes that the common factor is prime nor that it is square-free.

Theorem 1 (KSS membership criterion)**.** *Let E be a KSS curve admitting a degree-d twist E', and retain the notation above. Put*

$$A = x^2 - c_\tau x + np, \qquad B = A/r, \qquad s = \gcd(B, h_2).$$

Define the h_2-saturation of s *by*

$$\eta = \prod_{\ell \mid s} \ell^{v_\ell(h_2)}, \tag{4}$$

where $v_\ell(h_2)$ *is the largest positive integer such that* $\ell^{v_\ell(h_2)} \mid h_2$*, and the empty product is* 1*. Let* $P_1, \ldots, P_\rho$*,* $\rho \in \{0, 1, 2\}$*, be a minimal generating set of* $E'(\mathbb{F}_q)[\eta]$*; when* $\eta = 1$*, take* $\rho = 0$*. Assume that* $\eta \mid q - 1$*, so the reduced Tate pairing* t_η *is defined over* $\mathbb{F}_q$*.*

For every $Q \in E'(\mathbb{F}_q)$*,*

$$Q \in \mathbb{G}_2 \quad \Longleftrightarrow \quad \begin{cases} t_\eta(P_i, Q) = 1, & 1 \le i \le \rho, \\ \tau(Q) = [x]Q. \end{cases}$$

When $s = 1$*, this reduces to*

$$Q \in \mathbb{G}_2 \quad \Longleftrightarrow \quad \tau(Q) = [x]Q.$$

Proof. Since τ satisfies $\tau^2 - [c_\tau]\tau + [np] = 0$, condition (3) implies

$$[A]Q = [x^2 - c_\tau x + np]Q = \mathcal{O}_{E'} \qquad \text{for all } Q \in \mathbb{G}_2.$$

This also proves that $r \mid A$ and hence $B \in \mathbb{Z}$.

Let $G = E'(\mathbb{F}_q)$. The nondegeneracy of the reduced Tate pairing gives

$$t_\eta(P_i, Q) = 1 \text{ for all } i \quad \Longleftrightarrow \quad Q \in [\eta]G \tag{5}$$

[23, Theorem 26.3.3]. If $Q \in \mathbb{G}_2$, then $Q \in [\eta]\mathbb{G}_2 \subseteq [\eta]G$, because $\gcd(\eta, r) = 1$. Thus every point of $\mathbb{G}_2$ passes the pairing filters and satisfies $\tau(Q) = [x]Q$.

Conversely, suppose that all pairing filters equal 1 and $\tau(Q) = [x]Q$. Equation (5) gives $Q \in [\eta]G$. By Lemma 2, $|G[\eta]|$ is divisible by η, and therefore

$$\#[\eta]G = \frac{h_2 r}{|G[\eta]|} \quad \text{divides} \quad \frac{h_2 r}{\eta}.$$

By the definition of η, every prime dividing both B and h_2 is removed from h_2/η, so

$$\gcd(B, h_2/\eta) = 1.$$

The characteristic equation and $\tau(Q) = [x]Q$ yield $[A]Q = \mathcal{O}_{E'}$. Consequently,

$$\operatorname{ord}(Q) \mid \gcd\big(rB, \#[\eta]G\big) = r,$$

and hence $Q \in E'(\mathbb{F}_q)[r] = \mathbb{G}_2$. □

Remark 1. *If $\eta \nmid q-1$, the first line of Theorem 1 may be implemented as an exact test that $Q \in [\eta]E'(\mathbb{F}_q)$, or by a Tate pairing over an appropriate extension. The efficient instances considered here have small η and $\eta \mid q-1$. In particular, no assertion that s is always square-free is needed.*

Algorithm 3 $\mathbb{G}_2$ membership testing for a KSS family

Input: A point $Q \in E'(\mathbb{F}_q)$, an integer x, the composite map τ, and precomputed generators $P_1, \ldots, P_\rho$ of $E'(\mathbb{F}_q)[\eta]$.
Output: Whether $Q \in \mathbb{G}_2$.

```
for i = 1, ..., ρ do
    if t_η(P_i, Q) ≠ 1 then
        return false.
    end if
end for
if τ(Q) = [x]Q then
    return true.
end if
return false.
```

The torsion generators are precomputed. Online work consists of at most two reduced Tate pairings, one action of τ, and one scalar multiplication by x. If η is small, the pairings reduce to low-degree power-residue symbols as described in Algorithms 1 and 2.

Example 2 (The KSS16 family). For KSS16, E has CM discriminant $D = 1$ and admits a degree-4 twist E' over $\mathbb{F}_{p^4}$. From Example 1,

$$\alpha = (2\sqrt{-1} - 1)\zeta_{16}.$$

Let

$$\sigma : (X, Y) \longmapsto (-X, iY), \qquad i^2 = -1,$$

and set

$$\tau = \phi^{-1} \circ ([2]\sigma - [1]) \circ \pi \circ \phi.$$

Then

$$\tau(Q) = [x]Q, \qquad Q \in \mathbb{G}_2.$$

For comparison, the DLZZ method uses the Frobenius endomorphism and an LLL-reduced vector. When $x \equiv 25, 45 \pmod{70}$, a short vector is

$$(c_0, \ldots, c_7) = (11u + 4, -9u - 3, 3u + 1, 3u + 1, -13u - 5, 7u + 3, u, 11u + 4),$$
$$u = \frac{-x - 25}{70}.$$

Thus the DLZZ test evaluates

$$\sum_{i=0}^{6} \psi^i([c_i]Q) = -\psi^7([c_7]Q).$$

This requires one scalar multiplication by u, 13 point additions, one point doubling, and seven actions of ψ.

For our criterion, Lemma 1 gives

$$\tau^2 + (t - 2f)\tau + 5p = 0.$$

The twist order computed from [28, Proposition 2] satisfies

$$2 \parallel \#E'(\mathbb{F}_{p^4})$$

for $x \equiv 25, 45 \pmod{70}$. Moreover,

$$\gcd\big((x^2 + (t - 2f)x + 5p)/r, h_2\big) = 2.$$

Hence $s = \eta = 2$. There is a unique nonzero rational 2-torsion point, $P_2 = (0, 0)$, and the pairing filter becomes

$$t_2(P_2, Q) = (x_Q - x_{P_2})^{(p^4-1)/2} = x_Q^{(p^4-1)/2} = \left(\frac{x_Q}{p^4}\right)_2.$$

Algorithm 2 computes this quadratic character with $3\mathbf{f}_4 + 3\mathbf{m}_4$ (according to Section 2.4) and a base-field Jacobi-symbol computation.

If the character is 1, the remaining test is

$$\tau(Q) = ([2]\sigma - [1]) \circ \phi^{-1} \circ \pi \circ \phi(Q) = [x]Q.$$

It uses one scalar multiplication by x, one point addition, one point doubling, one action each of ψ and σ, and one quadratic-residue symbol. Table 1 compares this with DLZZ method. The algebraic criterion of Theorem 1 applies to any KSS family satisfying its hypotheses; the particularly inexpensive quadratic filter is a feature of these KSS16 instances.

Table 1 Operations for $\mathbb{G}_2$ membership testing on KSS16 curves. PDBL and PADD denote projective point doublings and additions.

Family	This work	DLZZ criterion [15]
KSS16	one scalar $[x]$ 1PDBL + 1PADD one action each of ψ and σ one quadratic symbol $\left(\frac{x_Q}{p^4}\right)_2$	one scalar $[(-x - 25)/70]$ 1PDBL + 13PADD seven actions of ψ —

For KSS16-330, the seed is $x = \texttt{0x3c4803fe1}$. A width-one NAF gives 29 doublings and 11 additions for $[u]$, and 35 doublings and 7 additions for $[x]$. The DLZZ and new tests therefore use, respectively,

$$30\mathsf{PDBL} + 24\mathsf{PADD} \quad \text{and} \quad 36\mathsf{PDBL} + 8\mathsf{PADD}.$$

With projective costs $12\mathbf{m}_4$ for addition and $8\mathbf{m}_4 + 3\mathbf{s}_4$ for doubling, the point-arithmetic portions cost

$$528\mathbf{m}_4 + 90\mathbf{s}_4 \quad \text{and} \quad 384\mathbf{m}_4 + 108\mathbf{s}_4.$$

Including one ψ action ($3\mathbf{f}_4$) and the quadratic symbol ($3\mathbf{f}_4 + 3\mathbf{m}_4$), the complete cost of our test is

$$387\mathbf{m}_4 + 108\mathbf{s}_4 + 6\mathbf{f}_4.$$

3.2 Generalizing Scott's Method for $\mathbb{G}_2$ Membership Testing on More Pairing-Friendly Curves

In this subsection, we aim to derive $\mathbb{G}_2$ membership testing methods that are applicable for more pairing-friendly curves. For the approach proposed by Scott [39], we weaken the corresponding condition and provide a generalized version which is different from the method in [15].

An efficient method for $\mathbb{G}_2$ membership testing on BN and BLS curves was first proposed by Scott in [39]. This testing method needs to satisfy the condition $\gcd(h_1, h_2) = 1$. The most expensive part of the computation of Scott's approach is the scalar multiplication by $t - 1$, where t is the Frobenius trace. However, in several situations $\gcd(h_1, h_2) = 1$ is not satisfied. Consequently, we aim to generalize Scott's method, making it still applicable if $\gcd(h_1, h_2) \neq 1$.

Let E denote a pairing-friendly curve admitting a twist E'. Using the above notations, we introduce the generalization of Scott's method, which is summarized as the following theorem.

Theorem 2 (Saturated-cofactor generalization of Scott's test)**.** *Let*

$$s_0 = \gcd(h_1, h_2), \qquad \eta_S = \prod_{\ell \mid s_0} \ell^{v_\ell(h_2)}.$$

Let $P_1, \ldots, P_\rho$ be a minimal generating set of $E'(\mathbb{F}_q)[\eta_S]$, and assume that $\eta_S \mid q - 1$, so the reduced Tate pairing t_{η_S} is defined over $\mathbb{F}_q$. Then, for $Q \in E'(\mathbb{F}_q)$,

$$Q \in \mathbb{G}_2 \quad \Longleftrightarrow \quad \begin{cases} t_{\eta_S}(P_i, Q) = 1, & 1 \leq i \leq \rho, \\ \psi(Q) = [t-1]Q. \end{cases}$$

If $s_0 = 1$, then $\eta_S = 1$ and this is exactly Scott's test.

Proof. The pairing conditions are equivalent to $Q \in [\eta_S]E'(\mathbb{F}_q)$. The order of the latter image is

$$\frac{h_2 r}{|E'(\mathbb{F}_q)[\eta_S]|},$$

and its cofactor divides h_2/η_S. By construction,

$$\gcd(h_1, h_2/\eta_S) = 1.$$

Scott's proof therefore applies on the image $[\eta_S]E'(\mathbb{F}_q)$ and shows that the Frobenius relation is equivalent to membership in its unique order-r subgroup. Conversely, multiplication by η_S is an automorphism of $\mathbb{G}_2$, so every point of $\mathbb{G}_2$ belongs to this image and passes all pairing filters. □

On the basis of Theorem 2, we propose Algorithm 4 for $\mathbb{G}_2$ subgroup membership testing. This formulation also resolves the prime-power issue for Scott's generalization: neither s_0 nor η_S is assumed to be prime or square-free, and Lemma 2 determines whether one or two torsion generators must be used. The method is most attractive when η_S is small; for large η_S, the Tate-pairing filter may dominate the computation.

Note that by performing the above adjustment, our method can be employed even though $\gcd(h_1, h_2) \neq 1$. We also point out that the DLZZ criterion is not limited by the condition $\gcd(h_1, h_2) = 1$. In the following, we show the difference between the DLZZ criterion and Theorem 2. Our method accomplishes the membership testing by determining whether the point is in $[\eta_S]E'(\mathbb{F}_q)$, while the DLZZ criterion makes use of LLL's algorithm to find a suitable short vector and requires satisfying an additional weaker condition. In certain cases, Algorithm 4 will be more efficient than the DLZZ criterion.

Algorithm 4 Generalized Scott's criterion

Input: A point $Q \in E'(\mathbb{F}_q)$, the trace t of the p-power Frobenius endomorphism π, the composite map ψ, and generators $P_1, \ldots, P_\rho$ of $E'(\mathbb{F}_q)[\eta_S]$.
Output: Whether $Q \in \mathbb{G}_2$.

1. **for** $i = 1, \ldots, \rho$ **do**
2. **if** $t_{\eta_S}(P_i, Q) \neq 1$ **then**
3. **return** false.
4. **end if**
5. **end for**
6. **if** $\psi(Q) = [t-1]Q$ **then**
7. **return** true.
8. **end if**
9. **return** false.

It is worth noting that the generator(s) P_i of $E'(\mathbb{F}_q)[\eta_S]$ can be precomputed. We now present Example 3 to illustrate the performance of our generalized Scott's criterion.

Example 3 (BLS27 familiy). We provide the following example (BLS27 family) for description, and verify that the above new method will be more efficient than the algorithm in [15] in some specific cases. (BLS27 family) The BLS27 family with embedding degree $k = 27$ and CM discriminant $D = 3$ is parametrized by the following three polynomials

$$\begin{aligned} r(x) &= \frac{1}{3}(x^{18} + x^9 + 1), \\ t(x) &= x + 1, \\ p(x) &= \frac{1}{3}(x-1)^2(x^{18} + x^9 + 1) + x. \end{aligned}$$

A BLS27 curve admits a degree-3 twist E' defined over $\mathbb{F}_{p^9}$. We first consider DLZZ criterion [15]. By calculation, the `gcd` of the resultant and h_2 in Theorem 1 in [15] is 3, which means that the condition is not satisfied. In [3], the authors make a modification and deduce that the corresponding $\mathbb{G}_2$ membership testing is to determine whether

$$[(1-x)/3](S - \psi^9(S)) + \psi^9(Q) = \mathcal{O}_{E'}$$

for the point $Q \in E'(\mathbb{F}_{p^9})$, where $S = R + \psi^3(R) + \psi^6(R),\ R = Q + \psi(Q) + \psi^2(Q)$. Consequently, it requires a scalar multiplication $[(1-x)/3]$, six point additions and six actions of the powers of ψ.

Now we consider the computational cost of our method. By calculation, we obtain

$$\gcd(h_1, h_2) = 3, \qquad v_3(h_2) = 1.$$

By Theorem 2, it holds that $\eta_S = 3$ and the 3-torsion subgroup $E'(\mathbb{F}_{p^9})[3]$ satisfies

$$E'(\mathbb{F}_{p^9})[3] \cong \mathbb{Z}_3.$$

Therefore, we can precompute a 3-torsion point $P_3 \in E'(\mathbb{F}_{p^9})$ such that $\langle P_3 \rangle = E'(\mathbb{F}_{p^9})[3]$, and determine whether

$$t_3(P_3, Q) = (\ell_{P_3,P_3}(Q))^{\frac{p^9-1}{3}} = \left(\frac{\ell_{P_3,P_3}(Q)}{p^9}\right)_3 = 1.$$

Since the slope $\lambda_\ell = \frac{3x_{P_3}^2}{2y_{P_3}}$ of the tangent line ℓ_{P_3,P_3} can also be precomputed, the computation of the above residue symbol can be accomplished by applying cubic reciprocity law and performing a multiplication over $\mathbb{F}_{p^9}$, which is extremely fast. If $\left(\frac{\ell_{P_3,P_3}(Q)}{p^9}\right)_3 = 1$, Scott's method can be utilized to finish the testing. Otherwise, it yields that $Q \notin \mathbb{G}_2$. Hence, our method needs to perform at most a scalar multiplication $[x-1]$, an action of ψ and a cubic residue symbol computation.

Table 2 shows the corresponding comparison of the operations between DLZZ criterion [15] and our algorithm on the BLS27 family. Note that our method reduces

about 6 point additions in $E'(\mathbb{F}_{p^9})$ compared to DLZZ criterion, as the lengths of the scalar multiplications are almost the same and the other executions are extremely fast. Consequently, our algorithm is more efficient than DLZZ criterion on BLS27 curves, especially for curve BLS27-426 associated with the seed $x = \texttt{-0x287beb}$, which possesses the smallest characteristic p among the pairing-friendly curves at the 192-bit security level [3]. In the following, we make a detailed cost comparison for $\mathbb{G}_2$ membership testing on BLS27-426.

By applying NAF, the scalar multiplication $[(1-x)/3]$ requires to execute 21 point doublings and 7 point additions, while $[x-1]$ needs to perform 22 point doublings and 7 point additions. Since the action of ψ and the 3-rd residue symbol computation are significantly efficient, the total costs of the testing approach in [15] and our generalized method are about 21 point doublings and 13 point additions, and 22 point doublings and 7 point additions, respectively. From [9], we know that the costs for executing a point addition and a point doubling on $E'(\mathbb{F}_{p^9})$ in Jacobian coordinates are 7 multiplications with 4 squarings, and 2 multiplications with 5 squarings over $\mathbb{F}_{p^9}$, respectively. Hence, it requires to execute 133 multiplications with 157 squarings, and 93 multiplications with 138 squarings over $\mathbb{F}_{p^9}$ by DLZZ criterion and our approach, respectively. This implies that our generalization requires less computation compared to DLZZ criterion.

Table 2 The operations involved in our method and the approach in [15] for the $\mathbb{G}_2$ membership testing on the curve BLS27-426. The notation PADD denotes the point additions.

Family	This work	[15]
BLS27	1 scalar $[x-1]$	1 scalar $[\frac{1-x}{3}]$
	1 action of ψ	6 actions of powers of ψ
	1 cubical residue symbol $\left(\frac{\ell_{P_3,P_3}(Q)}{p^9}\right)_3$	6 PADD

Although the above generalization is suitable for any pairing-friendly curves in theory, it is cumbersome in some situations. If η_S is large, the computation of the reduced Tate pairing is crucially expensive, making it less efficient than the previous method. In [34], the author recalled that today the η_S-th power residue symbol (the reduced Tate pairing $t_{\eta_S}(P,Q)$) can be computed in the (sub-)quadratic time only for $\eta_S \leq 11$. Besides, on some curves that are not constructed by the BLS method, the size of the scalar $[t(x)-1]$ is relatively large. Therefore, in the following, we investigate obtaining a method that requires a shorter scalar multiplication to perform for more generic pairing-friendly curves besides KSS/BLS curves.

3.3 Generalizing DLZZ Criterion by Utilizing Arbitrary Degree Endomorphisms

In this subsection, we extend DLZZ criterion to all GLV-curves admitting twists by utilizing the degree-n endomorphisms, which is summarized in the following theorem.

Theorem 3. *With the notations as above, let E denote an ordinary curve over $\mathbb{F}_p$ with embedding degree k and CM-discriminant D. Define E' to be a degree-d twist of E over*

$\mathbb{F}_{p^e}$ *such that* $r||E'(\mathbb{F}_{p^e})$. *Let* $\Phi = \phi^{-1}\circ\sigma\circ\phi \in End(E')$, *where* $\sigma = a+b\sqrt{-D},\ a,b \in \mathbb{Q}$ *is a degree-n endomorphism on* E. *Denote by* $Res(h,g)$ *the resultant of two polynomials* h *and* g.

1. *If* $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$, *it suffices to employ* $\psi = \phi^{-1}\circ\pi\circ\phi$ *to construct a dimension-*$\varphi(k)$ *modular lattice*

$$\mathcal{L}_\psi = \{(c_0,\cdots,c_{\varphi(k)-1}) \in \mathbb{Z}^{\varphi(k)} \mid \sum_{i=0}^{\varphi(k)-1} c_i \cdot p^i \equiv 0 \mod r\}.$$

Assume that $(c_0, c_1, \cdots, c_{\varphi(k)-1}) \in \mathcal{L}_\psi$ *satisfies* $\gcd(Res(h(\psi)\ and\ g(\psi)), h_2 \cdot r) = r$, *where* $h(\psi) = \sum_{i=0}^{\varphi(k)-1} c_i\psi^i$, $g(\psi) = \psi^2 - t\psi + p$. *Given* $Q \in E'(\mathbb{F}_{p^e})$, *then* $Q \in \mathbb{G}_2 = E'(\mathbb{F}_{p^e})[r]$ *if and only if*

$$\sum_{i=0}^{\varphi(k)-1} [c_i]\psi^i(Q) = \mathcal{O}_{E'}.$$

2. *If* $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, *along with* $a \neq 0$ *or* $k \neq 0 \mod 4$, *we employ the composited map* $\tau = \Phi\circ\psi = \phi^{-1}\circ\sigma\circ\pi\circ\phi$ *to construct a dimension-*$2\varphi(k)$ *modular lattice.*

$$\mathcal{L}_\tau = \{(c_0,\cdots,c_{2\varphi(k)-1}) \in \mathbb{Z}^{2\varphi(k)} \mid \sum_{i=0}^{2\varphi(k)-1} c_i \cdot \lambda^i \equiv 0 \mod r\},$$

where λ *is a integer such that* $\tau(Q') = [\lambda]Q'$ *for any* $Q' \in \mathbb{G}_2$. *Assume that the vector* $(c_0, c_1, \cdots, c_{2\varphi(k)-1})$ *satisfies* $\gcd(Res(h(\tau), g(\tau)), h_2 \cdot r) = r$, *where* $h(\tau) = \sum_{i=0}^{2\varphi(k)-1} c_i\tau^i$, $g(\tau) = \tau^2 - c_\tau\tau + np$, $c_\tau = at - \varepsilon bfD$. *Given* $Q \in E'(\mathbb{F}_{p^e})$, *then* $Q \in \mathbb{G}_2 = E'(\mathbb{F}_{p^e})[r]$ *if and only if*

$$\sum_{i=0}^{2\varphi(k)-1} [c_i]\tau^i(Q) = \mathcal{O}_{E'}.$$

Proof. If $\sqrt{-D} \in \mathbb{Q}(\zeta_k)$, the effect of $\Phi \sim a + b\sqrt{-D}$ in the composite map $\Phi\circ\psi \sim (a + b\sqrt{-D})\cdot\zeta_k$ will be killed by $\psi = \phi^{-1}\circ\pi\circ\phi \sim \zeta_k$. Therefore, we only need to utilize the map ψ to construct the modular lattice. The remaining proof is the same as [15, Theorem 1].

We now present the proof for the second situation. If $\sqrt{-D} \notin \mathbb{Q}(\zeta_k)$, define K to be the number field $\mathbb{Q}(\zeta_k \cdot (a + b\sqrt{-D}))$. It follows from [45, Theorem 2.4] that $K = \mathbb{Q}\left(\zeta_k, \sqrt{-D}\right)$ if $a \neq 0$ or $k \neq 0 \mod 4$. Thus the minimal polynomial of $\zeta_k\cdot(a+b\sqrt{-D})$ satisfies that

$$\deg(f(x)) = [\mathbb{Q}\left(\zeta_k, \sqrt{-D}\right) : \mathbb{Q}] = 2\varphi(k).$$

By $\tau(Q') = [\lambda]Q'$ for $Q' \in \mathbb{G}_2$ we deduce that $f(\lambda)(Q') = \mathcal{O}_{E'}$, which implies that $f(\lambda) \equiv 0 \mod r$. Consequently, there exists a modular lattice

$$\mathcal{L}_\tau = \{(c_0, c_1, \cdots, c_{2\varphi(k)-1}) \in \mathbb{Z}^{2\varphi(k)} \mid \sum_{i=0}^{2\varphi(k)-1} c_i \cdot \lambda^i \equiv 0 \mod r\}.$$

By LLL's algorithm [35] we can obtain a short vector $(c_0, \cdots, c_{2\varphi(k)-1}) \in \mathcal{L}_\tau$ such that $|c_i| \approx r^{1/2\varphi(k)}$.

If $Q \in \mathbb{G}_2$, it is clear that $\sum_{i=0}^{2\varphi(k)-1}[c_i]\tau^i(Q) = \mathcal{O}_{E'}$. On the contrary, let b_0 and b_1 be two integers such that

$$h(\tau) \equiv b_0 + b_1\tau \mod g(\tau).$$

By the properties of resultants, we have

$$\mathrm{Res}(h(\tau), g(\tau)) = \mathrm{Res}(b_0 + b_1\tau, g(\tau)) = b_0^2 + c_\tau b_0 b_1 + npb_1^2.$$

Denote by $\hat{\tau}$ the dual of τ. By Lemma 1, it can be deduced that

$$\begin{aligned}(b_0 + b_1\hat{\tau})(b_0 + b_1\tau) &= b_0^2 + b_0 \cdot b_1 \cdot \mathrm{Tr}(\tau) + b_1^2 \cdot \mathrm{Nrd}(\tau) \\ &= b_0^2 + c_\tau b_0 b_1 + npb_1^2,\end{aligned}$$

where $\mathrm{Tr}(\tau) = \tau + \hat{\tau}$ and $\mathrm{Nrd}(\tau) = \tau \cdot \hat{\tau}$ are the trace and the norm of τ, respectively. Since $h(\tau)(Q) = \mathcal{O}_{E'}$ and $g(\tau)(Q) = \mathcal{O}_{E'}$, it yields that

$$\begin{aligned}[\mathrm{Res}(h(\tau), g(\tau))](Q) &= [b_0^2 + c_\tau b_0 b_1 + npb_1^2]Q \\ &= (b_0 + b_1\hat{\tau})(b_0 + b_1\tau)(Q) \\ &= \mathcal{O}_{E'},\end{aligned}$$

which implies that $\mathrm{ord}(Q) | b_0^2 + c_\tau b_0 b_1 + npb_1^2$. By the condition

$$\gcd(\mathrm{Res}(h(\tau), g(\tau)), h_2 \cdot r) = r \text{ and } Q \in E'(\mathbb{F}_{p^e}),$$

we derive that $\mathrm{ord}(Q) \mid r$, which completes the proof. □

For finding a short vector on the GLV-curves admitting dimension-$2\varphi(k)$ decompositions as discussed in the second situation in Theorem 3, we can refer to Algorithm 1 in [15].

Remark 2. *Note that* $\gcd((b_0^2 - (at + bfD)b_0 b_1 + nb_1^2 p)/r, h_2) = 1$ *can be relaxed into* $\gcd((b_0^2 - (at + bfD)b_0 b_1 + nb_1^2 p)/r, h_2) = s$, *where* s *is a small integer if the desired short vector cannot be found. After deriving a short vector satisfying the relaxed condition, we can utilize [23, Theorem 26.3.3] to determine whether* s *is a factor of* $ord(Q)$, $Q \in E'(\mathbb{F}_{p^e})$. *Since* s *is small, this checking is crucially efficient. Once* $Q \in [s]E'(\mathbb{F}_{p^e})$, *the techniques in Theorem 3 can be exploited. Additionally, the idea in*

Theorem 3 can also be employed to generalize the DLZZ criterion for $\mathbb{G}_1$-membership testing on more pairing-friendly curves.

Based on the above analysis, our generalization enables the DLZZ criterion to be compatible with a broader range of GLV-curves. We state the following example to illustrate our extended approach and make a cost comparison.

Example 4 (FM16-488). Consider the following family (FM16) of pairing curves proposed by Fotiadis and Martindale (refer to [27]) with embedding degree $k = 10$ and CM-discriminant $D = 2$

$$\begin{aligned} r(x) &= x^{16} - x^{12} + x^8 - x^4 + 1, \\ t(x) &= -x^{12} + x^8 - x^4 + 2, \\ p(x) &= \frac{1}{8}(x^{30} - 2x^{26} + 2x^{24} + x^{22} - 2x^{20} + 2x^{16} - 10x^{12} + x^{10} + 10x^8 - 2x^6 - 8x^4 \\ &\quad + x^2 + 8). \end{aligned}$$

By taking $x = \texttt{0x1430c}$, the above three polynomials correspond to the curve FM16-488 with 141-bit security level [27, Table 5]. The previous method is to find a short vector such that $\gcd(\mathrm{Res}(h(\psi), g(\psi)), h_2 \cdot r) = r$. By utilizing [15, Algorithm 1], we obtain the following short vector

$$V = (0, 0, 1, x^4).$$

It implies that the testing requires to perform $\psi^3(Q) + [x^4]\psi^4(Q)$, which needs a scalar multiplication by x^4, a point addition and four actions of the endomorphism $\psi = \phi^{-1} \circ \pi \circ \phi$. The main computational cost is the scalar multiplication $[x^4]$.

We now apply Theorem 3. By the condition we know that there exists a **degree-2 endomorphism** σ associated with $\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}] = \mathrm{End}_p(E)$. Therefore, the composited map $\tau = \phi^{-1} \circ \sigma \circ \pi \circ \phi$ corresponds to $\alpha = \sqrt{-2} \cdot \zeta_{10} \in \mathbb{Q}\left(\sqrt{-2}, \zeta_{10}\right)$. Since $\sqrt{-2} \notin \mathbb{Q}(\zeta_{10})$ and $k \neq 0 \mod 4$, by Theorem 3 we deduce that τ admits a dimension-$2\varphi(k)$ expansion. By exploiting the technique in [15, Algorithm 1], we obtain a short vector satisfying $\gcd(\mathrm{Res}(h(\tau), g(\tau)), h_2 \cdot r) = r$

$$V = (64u^2 - 15, -8u, -32u^2 + 8, 4u, 16u^2 - 4, -2u, -8u^2 + 2, (32u - 31)u + 8),$$

where $u = \frac{x+4}{8}$. Consequently, we can go through the scalar multiplications in V by performing the computation of the following sequence

$$\begin{aligned} &2u \to 4u \to 8u \to 8u^2 - 2 \to 16u^2 - 4 \to (32u - 31)u + 8 \\ &\to 32u^2 - 8 \to 64u^2 - 15, \end{aligned}$$

which requires eight point doublings, five point additions, and two scalar multiplications by u. Thus, the total computational cost becomes eight point doublings, twelve point additions, two scalar multiplications $[u]$ together with seven actions of τ. The most expensive part is two scalar multiplications $[u]$, which can be roughly regarded as the scalar multiplication $[x^2]$. Table 3 illustrates the comparison for the operations

required in the approach in [15] and our generalized method on curve FM16-488. Hence, it can be derived that our approach can reduce the bit-length of the scalar multiplication for the $\mathbb{G}_2$-membership testing from $\log_2(r)/4$ to $\log_2(r)/8$.

Table 3 The operations involved in our method and the approach in [15] for the $\mathbb{G}_2$ membership testing on family FM16. The notations PADD and PDBL denote the point additions and doublings, respectively.

Family	This work	[15]
FM16	2 scalars $[\frac{x+4}{8}]$ 7 actions of τ 8 PDBL + 12 PADD	1 scalar $[x^4]$ 4 actions of ψ 1 PADD

4 Cost Analysis and Implementation Results

We first give a detailed cost analysis for KSS16-330 and then report the implementation results for KSS16-329, KSS16-330, and KSS16-766. The RELIC implementation represents points of $E'(\mathbb{F}_{p^4})$ in projective coordinates $(X : Y : Z)$ with $x = X/Z$ and $y = Y/Z$. The explicit-formula database [9] gives the costs

$$\mathsf{PADD} = 12\mathbf{m}_4, \qquad \mathsf{PDBL} = 8\mathbf{m}_4 + 3\mathbf{s}_4.$$

One action of ψ costs $3\mathbf{f}_4$. By Algorithm 2, the quadratic symbol in Example 3.1 costs $3\mathbf{f}_4+3\mathbf{m}_4$. The action of σ consists only of inexpensive multiplications by precomputed constants and is omitted.

The DLZZ criterion on KSS16-330 uses $30\mathsf{PDBL} + 24\mathsf{PADD}$ and seven actions of ψ, whereas our test uses $36\mathsf{PDBL} + 8\mathsf{PADD}$, one action each of ψ and σ, and one quadratic-symbol computation. The complete costs are therefore

$$\begin{aligned} \text{DLZZ:} \quad & 30(8\mathbf{m}_4 + 3\mathbf{s}_4) + 24(12\mathbf{m}_4) + 7(3\mathbf{f}_4) = 528\mathbf{m}_4 + 90\mathbf{s}_4 + 21\mathbf{f}_4, \\ \text{this work:} \quad & 36(8\mathbf{m}_4 + 3\mathbf{s}_4) + 8(12\mathbf{m}_4) + 3\mathbf{f}_4 + (3\mathbf{f}_4 + 3\mathbf{m}_4) \\ & = 387\mathbf{m}_4 + 108\mathbf{s}_4 + 6\mathbf{f}_4. \end{aligned}$$

Thus the $387\mathbf{m}_4$ count includes the $3\mathbf{m}_4$ required by the quadratic symbol; the point-arithmetic subtotal alone is $384\mathbf{m}_4$.

We integrated the new test into RELIC [1]. The code was compiled and benchmarked on an Intel Core i9-12900K at 3.20 GHz, with Turbo Boost and Hyper-Threading disabled. Each cycle result in Table 4 is the mean of 10^4 executions. For the approximately 330-bit fields, the conversion

$$\mathbf{m}_4 = 9\mathbf{m}, \qquad \mathbf{s}_4 = 6\mathbf{m}, \qquad \mathbf{f}_4 = 2\mathbf{m}$$

is used [3, Table 9]. KSS16-766 uses a 766-bit prime, represented by twelve 64-bit limbs. Its base-field multiplication is normalized by $\frac{2\cdot 12^2+12}{2\cdot 6^2+6}\,\mathbf{m} \approx 3.846\mathbf{m}$ [3, Section 3.4].

For completeness, we compare both optimized methods with the naive definition-based test $[r]Q = \mathcal{O}_{E'}$. A width-one NAF of r requires $255\mathsf{PDBL} + 76\mathsf{PADD}$,

255PDBL+87PADD, and 605PDBL+214PADD on KSS16-329, KSS16-330, and KSS16-766, respectively. We report this comparison in the same field-operation model as the optimized tests. We do not infer synthetic cycle counts for the naive method from the operation counts.

Table 4 The computational cost and benchmarking results of $\mathbb{G}_2$ membership testing on curves KSS16-329 and KSS16-330 at the 128-bit security level, together with KSS16-766 at the 192-bit security level, reported in $\mathbb{F}_p$-multiplications with the characteristic of 6 digits (represented by 6 64-bit limbs) and $\times 10^3$ CPU clock cycles, respectively. The results of the clock cycles are averaged over 10^4 executions. Note that the result has been rounded.

Curve	Seed x	Method	Cycles (10^3)	Cost ($\mathbf{m}$)	Speedup over naive
KSS16-329	`0x38fab7583`	This work	874	4,683	6.65×
		DLZZ [15]	1,149	5,334	5.84×
		Naive $[r]Q$	–	31,158	1.00×
KSS16-330	`0x3c4803fe1`	This work	720	4,143	7.81×
		DLZZ [15]	1,079	5,334	6.06×
		Naive $[r]Q$	–	32,346	1.00×
KSS16-766	$2^{78} - 2^{76} - 2^{28} + 2^{14} + 2^7 + 1$	This work	4,456	30,749	9.70×
		DLZZ [15]	6,291	40,729	7.32×
		Naive $[r]Q$	–	298,315	1.00×

The measured cycle counts show that our method is 24.0%, 33.3%, and 29.2% faster than DLZZ on KSS16-329, KSS16-330, and KSS16-766, respectively. In the common operation-count model, our test is between 6.65× and 9.70× faster than the naive scalar-multiplication test, while DLZZ is between 5.84× and 7.32× faster.

5 Conclusion

Subgroup membership testing is relevant for resisting small subgroup attacks. In this work, we investigated the $\mathbb{G}_2$ membership testing on the KSS16 family, and proposed a new efficient method of the testing for $\mathbb{G}_2$ on the curves constructed by the KSS method. Besides, we revisited the previous methods of membership testing for $\mathbb{G}_2$, and generalized these techniques to make them applicable to more generic pairing-friendly curves. We also made an efficient software implementation of $\mathbb{G}_2$ membership testing on three popular curves KSS16-329, KSS16-330, and KSS16-766, and benchmarked our code in the cryptographic library RELIC. The experimental result showed that our algorithm crucially outperforms those in the previous work. In conclusion, our methods may benefit some cryptographic schemes that require $\mathbb{G}_2$ membership testing on KSS16 families.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (Nos. 12441107 and 62402347), the National Key Research and Development Program of China (No. 2025YFA1017100).

References

[1] Diego F Aranha. RELIC is an Efficient Library for Cryptography. *http://code.google. com/p/relic-toolkit/*, 2020.

[2] Diego F Aranha, Youssef El Housni, and Aurore Guillevic. A survey of elliptic curves for proof systems. *Designs, Codes and Cryptography*, 91(11):3333–3378, 2023.

[3] Diego F. Aranha, Georgios Fotiadis, and Aurore Guillevic. A short-list of pairing-friendly curves resistant to the Special TNFS algorithm at the 192-bit security level. *IACR Communications in Cryptology*, 1(3), 2024.

[4] Diego F. Aranha, Laura Fuentes-Castañeda, Edward Knapp, Alfred Menezes, and Francisco Rodríguez-Henríquez. Implementing Pairings at the 192-Bit Security Level. In Michel Abdalla and Tanja Lange, editors, *Pairing-Based Cryptography – Pairing 2012*, pages 177–195, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[5] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. *Journal of cryptology*, 32:1298–1336, 2019.

[6] Paulo S. L. M. Barreto, Craig Costello, Rafael Misoczki, Michael Naehrig, Geovandro C. C. F. Pereira, and Gustavo Zanon. Subgroup Security in Pairing-Based Cryptography. In Kristin Lauter and Francisco Rodríguez-Henríquez, editors, *Progress in Cryptology – LATINCRYPT 2015*, pages 245–265, Cham, 2015. Springer International Publishing.

[7] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. On the Selection of Pairing-Friendly Group. In Mitsuru Matsui and Robert J. Zuccherato, editors, *Selected Areas in Cryptography*, pages 17–25, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

[8] Paulo S. L. M. Barreto and Michael Naehrig. Pairing-Friendly Elliptic Curves of Prime Order. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography*, pages 319–331, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[9] Daniel J Bernstein. Explicit-formulas database. *http://www. hyperelliptic. org/EFD*, 2007.

[10] Dan Boneh and Matt Franklin. Identity-Based Encryption from the Weil Pairing. In Joe Kilian, editor, *Advances in Cryptology — CRYPTO 2001*, pages 213–229, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[11] Dan Boneh, Ben Lynn, and Hovav Shacham. Short Signatures from the Weil Pairing. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 514–532, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[12] Friederike Brezing and Annegret Weng. Elliptic curves suitable for pairing based cryptography. *Designs, Codes and Cryptography*, 37(1):133–141, 2005.

[13] Alessandro Budroni and Federico Pintore. Efficient hash maps to $\mathbb{G}_2$ on BLS curves. *Applicable Algebra in Engineering, Communication and Computing*, 33(3):261–281, 2022.

[14] Yu Dai, Debiao He, Dmitri Koshelev, Cong Peng, and Zhijian Yang. Revisiting subgroup membership testing on pairing-friendly curves via the Tate pairing. Cryptology ePrint Archive, Paper 2024/1790, 2024.

[15] Yu Dai, Kaizhan Lin, Chang-An Zhao, and Zijian Zhou. Fast subgroup membership testings for $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ on pairing-friendly curves. *Des. Codes Cryptography*, 91(10):3141–3166, may 2023.

[16] Claus Diem and Emmanuel Thomé. Index calculus in class groups of non-hyperelliptic curves of genus three. *Journal of Cryptology*, 21(4):593–611, 2008.

[17] Youssef El Housni and Aurore Guillevic. Optimized and Secure Pairing-Friendly Elliptic Curves Suitable for One Layer Proof Composition. In Stephan Krenn, Haya Shulman, and Serge Vaudenay, editors, *Cryptology and Network Security*, pages 259–279, Cham, 2020. Springer International Publishing.

[18] Youssef El Housni and Aurore Guillevic. Families of SNARK-Friendly 2-Chains of Elliptic Curves. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology – EUROCRYPT 2022*, pages 367–396, Cham, 2022. Springer International Publishing.

[19] Youssef El Housni, Aurore Guillevic, and Thomas Piellard. Co-factor Clearing and Subgroup Membership Testing on Pairing-Friendly Curves. In Lejla Batina and Joan Daemen, editors, *Progress in Cryptology - AFRICACRYPT 2022*, pages 518–536, Cham, 2022. Springer Nature Switzerland.

[20] Kamel Mohamed Faraoun. Extending constant-time simplified SWU mapping to handle twists of BLS24 and BLS48 pairing-friendly curves. *J. Inf. Secur. Appl.*, 93:104107, 2025.

[21] David Freeman, Michael Scott, and Edlyn Teske. A taxonomy of pairing-friendly elliptic curves. *Journal of cryptology*, 23:224–280, 2010.

[22] Laura Fuentes-Castaneda, Edward Knapp, and Francisco Rodríguez-Henríquez. Faster hashing to $\mathbb{G}_2$. In *International workshop on selected areas in cryptography*, pages 412–430. Springer, 2011.

[23] Steven D. Galbraith. *Mathematics of Public Key Cryptography*. Cambridge University Press, USA, 1st edition, 2012.

[24] Steven D. Galbraith and Michael Scott. Exponentiation in Pairing-Friendly Groups Using Homomorphisms. In Steven D. Galbraith and Kenneth G. Paterson, editors, *Pairing-Based Cryptography – Pairing 2008*, pages 211–224, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[25] Robert P. Gallant, Robert J. Lambert, and Scott A. Vanstone. Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms. In Joe Kilian, editor, *Advances in Cryptology — CRYPTO 2001*, pages 190–200, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[26] Pierrick Gaudry, Florian Hess, and Nigel P Smart. Constructive and destructive facets of Weil descent on elliptic curves. *Journal of Cryptology*, 15:19–46, 2002.

[27] Aurore Guillevic. A Short-List of Pairing-Friendly Curves Resistant to Special TNFS at the 128-Bit Security Level. In Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, editors, *Public-Key Cryptography – PKC 2020*, pages 535–564, Cham, 2020. Springer International Publishing.

[28] F. Hess, N.P. Smart, and F. Vercauteren. The Eta Pairing Revisited. *IEEE Transactions on Information Theory*, 52(10):4595–4602, 2006.

[29] Marc Joye, Oleksandra Lapiha, Ky Nguyen, and David Naccache. The Eleventh

Power Residue Symbol. *Journal of Mathematical Cryptology*, 15(1):111–122, 2021.

[30] Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field. In Steven D. Galbraith and Kenneth G. Paterson, editors, *Pairing-Based Cryptography – Pairing 2008*, pages 126–135, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[31] Tadaki Kanenari, Yuto Takahashi, Yuta Hashimoto, Yuta Kodera, Takuya Kusaka, Yasuyuki Nogami, and Toru Nakanishi. A comparison of relic-toolkit and elips libraries for a pairing-based homomorphic encryption. In *34th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)*, pages 1–6. IEEE, 2019.

[32] Taechan Kim and Razvan Barbulescu. Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*, pages 543–571, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.

[33] Taechan Kim, Sungwook Kim, and Jung Hee Cheon. On the Final Exponentiation in Tate Pairing Computations. *IEEE Transactions on Information Theory*, 59(6):4033–4041, 2013.

[34] Dmitrii Koshelev. Subgroup membership testing on elliptic curves via the Tate pairing. *Journal of Cryptographic Engineering*, 13(1):125–128, 2023.

[35] A. K. Lenstra, H. W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[36] Chae Hoon Lim and Pil Joong Lee. A key recovery attack on discrete log-based schemes using a prime order subgroup. In Burton S. Kaliski, editor, *Advances in Cryptology — CRYPTO '97*, pages 249–263, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.

[37] Chao Lin, Debiao He, Xinyi Huang, Xiang Xie, and Kim-Kwang Raymond Choo. Blockchain-based system for secure outsourcing of bilinear pairings. *Inf. Sci.*, 527:590–601, 2020.

[38] Victor S Miller. The Weil pairing, and its efficient calculation. *Journal of cryptology*, 17:235–261, 2004.

[39] Michael Scott. A note on group membership tests for $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ on BLS pairing-friendly curves. Cryptology ePrint Archive, Paper 2021/1130, 2021.

[40] Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa. Fast Hashing to $\mathbb{G}_2$ on Pairing-Friendly Curves. In Hovav Shacham and Brent Waters, editors, *Pairing-Based Cryptography – Pairing 2009*, pages 102–113, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[41] Song Tian, Bao Li, Kunpeng Wang, and Wei Yu. Cover attacks for elliptic curves with cofactor two. *Designs, Codes and Cryptography*, 86:2451–2468, 2018.

[42] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2008.

[43] Libing Wu, Jing Wang, Kim-Kwang Raymond Choo, Yuangang Li, and Debiao He. An efficient provably-secure identity-based authentication scheme using bilinear pairings for Ad hoc network. *J. Inf. Secur. Appl.*, 37:112–121, 2017.

[44] Kang Yang, Liqun Chen, Zhenfeng Zhang, Christopher J. P. Newton, Bo Yang, and Li Xi. Direct Anonymous Attestation With Optimal TPM Signing Efficiency. *IEEE Transactions on Information Forensics and Security*, 16:2260–2275, 2021.

[45] Kisoon Yoon. 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.

[46] Xusheng Zhang and Dongdai Lin. Analysis of optimum pairing products at high security levels. In Steven Galbraith and Mridul Nandi, editors, *Progress in Cryptology - INDOCRYPT 2012*, pages 412–430, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.