Fast Subgroup Membership Testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on Pairing-friendly Curves

Yu Dai[1], Kaizhan Lin[1], Chan-an Zhao*[1,2] and Zijian Zhou[3]

[1]Department of Mathematics, Sun Yat-sen University, Guangzhou 510275, P.R.China.
[2]Guangdong Key Laboratory of Information Security, Guangzhou 510006, P.R.China.
[3]Department of Liberal Arts and Sciences, National University of Defense Technology, Changsha 410073, P.R.China.

Contributing authors: zhaochan3@mail.sysu.edu.cn;

Abstract

Pairing-based cryptographic protocols are typically vulnerable to small-subgroup attacks in the absence of protective measures. Subgroup membership testing is one of the feasible methods to address this security weakness. However, it generally leads to an expensive computational cost on most of pairing-friendly curves. Recently, Scott proposed efficient methods of subgroup membership testings for $\mathbb{G_1}$, $\mathbb{G_2}$ and $\mathbb{G_T}$ on the BLS family. In this paper, we generalize these methods proposed by Scott and show that the new techniques are applicable to a large class of pairing-friendly curves. In addition, we also confirm that our new methods result in a significant speedup for subgroup membership testings on many popular pairing-friendly curves.

Keywords: Small-subgroup attacks, Group membership testing, Pairing-friendly curves.

1 Introduction

Ever since the three party key agreement protocol was proposed by Joux [1], pairings have found various interesting applications in the area of public key cryptography [2–4]. Given an ordinary curve E defined over a prime field $\mathbb{F}_p$,

a pairing on E is a bilinear map of the form $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$, where $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are three cyclic subgroups with large prime order r. In the asymmetric case, the input groups $\mathbb{G}_1$ and $\mathbb{G}_2$ are distinct subgroups of $E(\mathbb{F}_{p^k})$, while the output group $\mathbb{G}_T$ is a subgroup of $\mathbb{F}_{p^k}^*$. The integer k is referred to as the embedding degree of E with respect to r. The security of pairing-based protocols relies on the difficulty of solving Discrete Logarithm Problems (DLP) in the above three subgroups [5–7]. However, since the running environment of a cryptographic protocol is possibly untrustworthy, powerful attackers may force the system to offer a point with small order. It leads to potential risks of secret key exposures under small-subgroup attacks [8, 9]. Specially, we assume a pairing-based protocol is designed for using the group $\mathbb{G}$ ($\mathbb{G} \in \{\mathbb{G}_1, \mathbb{G}_2\}$) to perform group operation, where $\mathbb{G}$ is contained in a large group $\mathcal{G}$ with order $h \cdot r$. If h has a non-trival small prime factor n and P is an element with order n in the group $\mathcal{G}$, an adversary may force the protocol to use P for the public parameter. Since solving the DLP in $\langle P \rangle$ is easy, a participant would leak partial information of his secret key s if the point $[s]P$ is published. For the worst case, the cofactor h could provide enough small prime factors such that attacks can recover the full information of the secret key by using the Pohlig-Hellman algorithm [10]. It should be noted that small-subgroup attacks can be also mounted on $\mathbb{G}_T$ [11, 12]. One efficient way of minimizing the chances of such attacks is to increase the size of parameters such that the cofactor h has no prime factor smaller than r [9]. In this case, we call $\mathbb{G}$ is *subgroup secure*. However, according to the construction of pairing-friendly curves, it is hard for $\mathbb{G}_1$ to be subgroup secure in most cases. In order to completely eliminate the hidden dangers, clearing cofactors and subgroup membership testings are the two feasible approaches until now.

1.1 Clearing cofactors

Clearing cofactors aim to multiply input elements by the cofactor h to force them into the correct subgroup. In the case of $\mathbb{G}_1$, the cofactor h is small on many pairing-friendly curves. Thus, the cofactor can be "cleared" at low cost. Recently, fast cofactor multiplication for $\mathbb{G}_1$ was proposed in [13], which may further reduce the computational cost. In the case of $\mathbb{G}_2$, the cofactor h is typically large. In this situation, the cofactor multiplication can be accelerated using the techniques from [14–16]. Even though this method can resist small-subgroup attacks, it also causes other problems. As pointed out by Hamburg in [17], implementors must determine which points to execute "clearing cofactors" on. Moreover, cofactor multiplication also changed system parameters. This would lead to additional troubles for implementors [18].

1.2 Subgroup membership testing

The negative effects of clearing cofactors can be avoided by performing subgroup membership testings. The essence of this method is to raise a candidate element to the power of r and compare the result with the identity element.

Since r is a large prime, this operation is quite costly and consequently affects the performance of pairing-based cryptographic protocols. Recently, Scott [18] proposed a novel method of subgroup membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on the Barreto-Lynn-Scott (BLS) [19] family, which achieves the same effect as scalar multiplication/exponentiation by r at the price of a relatively small overhead. Housni *et al.* [13] showed this method was also suitable for the Barreto-Naehrig (BN) [20] family.

1.3 Our contributions

Motivated by the work of Scott [18], we propose more general membership testing methods. We show that our new techniques are suitable for a large class of ordinary pairing-friendly curves, including BN, BLS and Kachisa-Schaefer-Scott (KSS) [21] families. We summarize our contributions as follows.

- The previous method of $\mathbb{G}_2$ membership testing [18] works under the condition that $\gcd(h_1, h_2) = 1$, where h_1 and h_2 are cofactors of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively. In this paper, we propose a new $\mathbb{G}_2$ membership testing method that does not rely on the above condition. Moreover, we show that the time complexity of this method would be in $O(\log r/\varphi(k))$ on many pairing-friendly curves. It is particularly interesting to see that the complexity can be further reduced to $O\big(\log r/(2\varphi(k))\big)$ on some certain curves.
- Fast methods of $\mathbb{G}_1$ and $\mathbb{G}_T$ membership testings are also proposed. The time complexity of the two methods would be in $O(\log r/2)$ and $O(\log r/\varphi(k))$, respectively. It should be noted that the method of the $\mathbb{G}_1$ membership testing is only suitable for ordinary curves with j-invariant 0 or 1728.
- Finally, we implement the proposed techniques over different pairing-friendly curves on a 64-bit computing platform within the RELIC [22] cryptographic library. In particular, the new methods run in approximately 0.49 and 0.53 the time of the previous best ones for the $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings on the BN-P446 curve, respectively.

Outlines of this paper. The remainder of this paper is organized as follows. Section 2 gives an overview of pairing subgroups, endomorphisms of elliptic curves and small-subgroup attacks on pairing-friendly curves. Sections 3 and 4 describe efficient methods of membership testings for different pairing subgroups. Section 5 provides a detailed explanation of our methods by applying them into several popular pairing-friendly curves. In Section 6, we present implementation results of our methods. The conclusion is given in Section 7.

2 Preliminaries

In this section, we first recall elementary definitions of pairing subgroups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$. After that, we briefly introduce efficiently computable endomorphisms on ordinary elliptic curves. Finally, we discuss small-subgroup attacks on several popular pairing-friendly curves.

2.1 Pairing subgroups

Let E be an ordinary elliptic curve defined over a prime field $\mathbb{F}_p$ and $\mathcal{O}_E$ denote the identity point of E. Let r be a large prime such that $r \parallel \#E(\mathbb{F}_p)$. The embedding degree k of E with respect to r is the smallest positive integer such that $r \mid \Phi_k(p)$, where $\Phi_k(\cdot)$ is the k-th cyclotomic polynomial. When $k > 1$, the group $E[r]$ is contained in $E(\mathbb{F}_{p^k})$ [23]. The p-power Frobenius endomorphism $\pi : (x, y) \to (x^p, y^p)$ on E satisfies the characteristic equation

$$\pi^2 - t \cdot \pi + p = 0, \tag{1}$$

where the trace $t = p+1-\#E(\mathbb{F}_p)$. Define $\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\pi-[1]) = E(\mathbb{F}_p)[r]$, $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\pi - [p])$ and $\mathbb{G}_T \subseteq \mathbb{F}_{p^k}^*$ to be the subgroup of r-th roots of unity. Denote by ℓ the order of the automorphism group of E. If $\ell \mid k$, then E admits a twist E' over $\mathbb{F}_{p^e}$, where $e = k/\ell$. Write ϕ as the twisting isomorphism from E' to E. Then $E'(\mathbb{F}_{p^e})[r]$ is the preimage of $\mathbb{G}_2$ under the map ϕ [24]. Therefore, it is convenient to represent $\mathbb{G}_2$ as $E'(\mathbb{F}_{p^e})[r]$. The definitions of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ give rise to the following naive method of subgroup membership testings:

$$(1) P \in \mathbb{G}_1 \Leftrightarrow P \in E(\mathbb{F}_p) \text{ and } [r]P = \mathcal{O}_E,$$
$$(2) Q \in \mathbb{G}_2 = E'(\mathbb{F}_{p^e})[r] \Leftrightarrow Q \in E'(\mathbb{F}_{p^e}) \text{ and } [r]Q = \mathcal{O}_{E'},$$
$$(3) \alpha \in \mathbb{G}_T \Leftrightarrow \alpha^r = 1,$$

where $\mathcal{O}_{E'}$ denotes the identity point of E'. Following Enge and Milan [25], we call E as a **curve with the lack of twists** if the subgroup $\mathbb{G}_2$ can be only represented as $E[r] \cap \mathrm{Ker}(\pi-[p])$. Since $E[r] \cap \mathrm{Ker}(\pi-[p]) = E[r] \cap \mathrm{Ker}(\Phi_k(\pi))$ under the condition that $r \nmid \Phi_k(1)$ [26], membership testing for $\mathbb{G}_2$ on such type of curves can be accomplished by checking that

$$Q \in E(\mathbb{F}_{p^k}), [r]Q = \mathcal{O}_E \text{ and } \Phi_k(\pi)(Q) = \mathcal{O}_E.$$

In total, membership testing for each subgroup requires at least one scalar multiplication/exponentiation by r. Since r is a large prime, the naive method is extremely slow in practice.

2.2 Endomorphisms of ordinary elliptic curves

Consider an ordinary curve E_1 over $\mathbb{F}_p$ with j-invariant 0. Then the curve is defined by the equation $y^2 = x^3 + b$ for some $b \in \mathbb{F}_p^*$ and $p \equiv 1 \bmod 3$ [27, Proposition 4.33]. Consequently, there is an endomorphism $\tau : (x, y) \to (\omega \cdot x, y)$ on E_1, where ω is a primitive cube root of unity in $\mathbb{F}_p^*$. This endomorphism corresponds to a scalar multiplication by λ_1 (resp. λ_2) in $\mathbb{G}_1$ and (resp. $\mathbb{G}_2$), where λ_1 and λ_2 are two distinct roots of the equation $\lambda^2 + \lambda + 1 \equiv 0 \bmod r$. Likewise, given an ordinary curve E_2 over $\mathbb{F}_p$ with j-invariant 1728, the curve is defined by the equation $y^2 = x^3 + ax$ for some $a \in \mathbb{F}_p^*$ and $p \equiv 1 \bmod 4$. There is the

endomorphism $\tau : (x, y) \to (-x, i \cdot y)$ on E_2, where i is a primitive fourth root of unity in $\mathbb{F}_p^*$. This efficiently computable endomorphism is equivalent to a scalar multiplication by λ_1 (resp. λ_2) in $\mathbb{G}_1$ (resp. $\mathbb{G}_2$), where λ_1 and λ_2 are two distinct roots of the equation $\lambda^2 + 1 \equiv 0 \bmod r$. Using the Gallant-Lambert-Vanstone (GLV) method [28], these efficiently computable endomorphisms allow fast elliptic curve scalar multiplication. Throughout the paper, we call such efficiently computable endomorphisms as GLV endomorphisms.

Another well known efficiently computable endomorphism is $\psi = \phi^{-1} \circ \pi \circ \phi$ on E' [29], which satisfies the characteristic equation

$$\psi^2 - t \cdot \psi + p = 0. \tag{2}$$

It is clear that $\psi^i = \phi^{-1} \circ \pi^i \circ \phi$ for all $i \in \mathbb{Z}^+$. This means that the order of ψ is precisely k restricted in $E'(\mathbb{F}_{p^k})$. Note that

$$\pi \circ \phi(Q) = [p]\phi(Q) \tag{3}$$

for all $Q \in \mathbb{G}_2$. Acting the map ϕ^{-1} on both sides of Eq. (3), it yields that

$$\psi(Q) = \phi^{-1} \circ \pi \circ \phi(Q) = \phi^{-1} \circ [p]\phi(Q) = [p]Q = [t-1]Q. \tag{4}$$

This endomorphism was exploited to speed up scalar multiplication in $\mathbb{G}_2$ by Galbraith and Scott [29]. Furthermore, it also leads to a high dimensional GLV method on a large class of elliptic curves [30]. Fast implementation of this method on ordinary curves with j-invariant 0 was studied in [31].

2.3 Small-subgroup attacks on pairing-friendly curves

The pairing subgroups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are typically contained in larger groups $\mathcal{G}_1$, $\mathcal{G}_2$ and $\mathcal{G}_T$, respectively. Following Barreto *et al.* [9], the groups $\mathcal{G}_1$, $\mathcal{G}_2$ and $\mathcal{G}_T$ are defined as

$$\mathbb{G}_1 \subseteq \mathcal{G}_1 = E(\mathbb{F}_p), \ \mathbb{G}_2 \subseteq \mathcal{G}_2 = E'(\mathbb{F}_{p^e}), \ \mathbb{G}_T \subseteq \mathcal{G}_T = \mathbb{G}_{\Phi_k(p)},$$

where $\mathbb{G}_{\Phi_k(p)}$ is the k-th cyclotomic subgroup of $\mathbb{F}_{p^k}^*$, i.e., $\mathbb{G}_{\Phi_k(p)} = \{\alpha \in \mathbb{F}_{p^k}^* | \alpha^{\Phi_k(p)} = 1\}$. If E is a curve with the lack of twists, we define $\mathcal{G}_2$ as

$$\mathbb{G}_2 \subseteq \mathcal{G}_2 = \mathrm{Ker}\big(\Phi_k(\pi)\big).$$

Explicit formula for computing $\#\mathrm{Ker}\big(\Phi_k(\pi)\big)$ is given in [26, Proposition 2]. On this basis, the associated cofactors h_1, h_2 and h_T are defined as follows:

$$h_1 = \#\mathcal{G}_1/r, \ h_2 = \#\mathcal{G}_2/r, \ h_T = \#\mathcal{G}_T/r.$$

Note that group membership testings for $\mathcal{G}_i$ are easy, where $i \in \{1, 2, T\}$. Thus, according to the principle of small-subgroup attacks, a curve E could be

Table 1 Subgroup security of pairing-friendly curves at the 128-bit security level. The symbol c_m denotes a composite number of size m bits. The BW family is derived from Construction 6.6 in [35].

k	family	$\log p$	$\log r$	seed z	h_1	h_2	h_T
12	BN	446	446	$2^{110} + 2^{36} + 1$[36]	1	$13 c_{610}$	c_{1336}
12	BLS	461	308	$-2^{77} + 2^{50} + 2^{33}$[36]	c_{153}	$c_{25} \cdot c_{442}$	$c_{39} \cdot c_{1495}$
16	KSS	330	257	$-2^{34} + 2^{27} - 2^{33} + 2^{20} - 2^{11} + 1$[36]	c_{75}	$c_{93} \cdot c_{1052}$	$34 \cdot c_{2379}$
18	KSS	348	256	$2^{44} + 2^{22} - 2^9 + 2$[36]	c_{93}	$c_{78} \cdot c_{710}$	$c_{131} \cdot c_{1595}$
13	BW	310	267	-2224[37]	c_{43}	$c_{83} \cdot c_{3368}$	$c_{126} \cdot c_{3368}$
19	BW	286	259	-145[37]	c_{28}	$c_{50} \cdot c_{4861}$	$c_{41} \cdot c_{5101}$

subgroup secure if the relevant cofactors h_1, h_2 and h_T contain no prime factor smaller than r. In Table 1, we list several popular pairing-friendly curves at the 128-bit security level under the attacks of Number Field Sieve and its variants [32, 33]. These curves can be parameterized by polynomials $p(z)$, $r(z)$ and $t(z)$ given a seed z. The small factors of h_2 and h_T can be obtained using the ECM function in Magma [34]. It can be seen from Table 1 that small-subgroup attacks can be easily mounted on cryptographic protocols constructed on these curves. Note that we are unable to obtain a small factor of the cofactor h_T (c_{1336}) of BN-P446. But it is not recommended for skipping the $\mathbb{G}_T$ membership testing on the curve as the cofactor is composite.

3 $\mathbb{G}_2$ Membership Testing

For efficiency, most of pairing-based protocols are instantiated with pairing-friendly curves admitting a twist. Recently, a few curves with the lack of twists also find their own applications in the cryptographic protocols that the implementation efficiency of one party mostly relies on the performance of scalar multiplication in $\mathbb{G}_1$. For example, Clarisse *et al.* [38] found that the BW13-P310 and BW19-P286 curves are suitable for several cryptographic schemes, such as Enhanced Privacy ID [39] and Direct Anonymous Attestation [40]. In this section, we investigate the problem of $\mathbb{G}_2$ membership testing on both types of curves.

3.1 Pairing-friendly curves admitting a twist

For a curve E admitting a twist E' over $\mathbb{F}_{p^e}$, Scott [18] proved that

$$Q \in \mathbb{G}_2 = E'(\mathbb{F}_{p^e})[r] \Leftrightarrow Q \in E'(\mathbb{F}_{p^e}) \text{ and } \psi(Q) = [t-1]Q$$

under the condition that $\gcd(h_1, h_2) = 1$. The computational cost is of approximately one scalar multiplication by $t - 1$. Apparently, this method is more efficient than the naive one. When we check a candidate element using the above technique, it should be careful to select the formulas of scalar multiplication. In particular, in the whole process of this testing, it is not allowed to

use any assumptions about $Q \in \mathbb{G}_2$. Therefore, the technique proposed in [29] can not be applied as it only works for elements in $\mathbb{G}_2$.

In this subsection, we propose a more general method with time complexity $O(\log r/\varphi(k))$ on many pairing-friendly curves. Moreover, the new method does not rely on the condition that $\gcd(h_1, h_2) = 1$ and thus has a wide applicability.

Theorem 1 *Let E be an ordinary elliptic curve over $\mathbb{F}_p$ and t the trace of the Frobenius endomorphism π. Let $\phi : E' \to E$ be the twisting isomorphism, where E' is defined over $\mathbb{F}_{p^e}$. Let r be a large prime such that $r \parallel E(\mathbb{F}_p)$ and $r \parallel E'(\mathbb{F}_{p^e})$. Define $\psi = \phi^{-1} \circ \pi \circ \phi$ with the characteristic polynomial $g(\psi) = \psi^2 - t \cdot \psi + p$. Let $\eta = \sum\limits_{i=0}^{s} c_i \cdot p^i$ be a multiple of r and $f(\psi) = \sum\limits_{i=0}^{s} c_i \psi^i$ a polynomial with respect to ψ. Denote by $b_0 + b_1\psi$ the remainder for $f(\psi)$ divided by $g(\psi)$, i.e.,*

$$b_0 + b_1\psi = f(\psi) \bmod g(\psi). \tag{5}$$

Assume

$$\gcd\left(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, \#E'(\mathbb{F}_{p^e})\right) = r. \tag{6}$$

Given a non-identity point $Q \in E'(\mathbb{F}_{p^e})$, then $Q \in \mathbb{G}_2 = E'(\mathbb{F}_{p^e})[r]$ if and only if $f(\psi)(Q) = \mathcal{O}_{E'}$.

Proof If $Q \in \mathbb{G}_2$, then $\psi(Q) = [p]Q$ (see Eq. (4)) and thus we conclude that

$$f(\psi)(Q) = \sum_{i=0}^{s} [c_i]\psi^i(Q) = \sum_{i=0}^{s} [c_i \cdot p^i]Q = [\eta]Q = \mathcal{O}_{E'}.$$

Conversely, it follows from Eq. (2) that

$$\psi^2(Q) - [t]\psi(Q) + [p]Q = \mathcal{O}_{E'}. \tag{7}$$

If $f(\psi)(Q) = \mathcal{O}_{E'}$, Eqs. (5) and (7) imply that

$$[b_1]\psi(Q) = -[b_0]Q. \tag{8}$$

Together with Eqs. (7) and (8), it yields that

$$\begin{aligned} &[b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p]Q \\ =&[b_1^2]\psi^2(Q) - [b_1^2 \cdot t]\psi(Q) + [b_1^2 \cdot p]Q \\ =&\mathcal{O}_{E'}. \end{aligned}$$

Since $\gcd\left(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, \#E'(\mathbb{F}_{p^e})\right) = r$, we conclude that $Q \in E'(\mathbb{F}_{p^e})[r]$, which completes the proof. $\square$

We use C to denote the vector $[c_0, c_1, \cdots, c_s]$, where each c_i is defined in Theorem 1. One may naturally ask whether there is such a vector C meeting the constraint (6). In fact, we can always select C as $[r, 0, \cdots, 0]$, which implies that $b_0 = r$ and $b_1 = 0$. Since $\mathbb{G}_2$ is the unique subgroup of $E'(\mathbb{F}_{p^e})$ of order r, we clearly have $\gcd\left(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, \#E'(\mathbb{F}_{p^e})\right) = r$. It is pointed out that this vector actually corresponds to the naive method, which is inefficient in practical applications.

In order to reduce the computational cost of $\mathbb{G}_2$ membership testing, we expect that the size of $n = max\{|c_0|, |c_1|, \cdots, |c_s|\}$ in bits is as small as possible. By the definition of the embedding degree k, we know that $r \mid \Phi_k(p)$. It is natural to take $\eta = \Phi_k(p)$, which means that $n = 1$ in many cases. Therefore, given a candidate element Q which is claimed to be a member of $\mathbb{G}_2$, the verifier only needs to check that $\Phi_k(\psi)(Q) = \mathcal{O}_{E'}$. Unfortunately, we verified this equality actually holds for all points in $E'(\mathbb{F}_{p^e})$ on most of popular pairing-friendly curves, such as the BN, BLS and KSS families. Hence, the verifier can not distinguish between valid elements and invalid ones. Fuentes *et al.* [15, Section 6.5] pointed out that Miyaji-Nakabayashi-Takano (MNT) [41] and Freeman [42] families do not satisfy the above equality in general. However, it seems still infeasible in this situation. Indeed, our experimental results show that the values $\gcd\left(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, \#E'(\mathbb{F}_{p^e})\right)$ are not equal to r on these two families of curves if we take $\eta = \Phi_k(p)$.

In practice, we fortunately find that the vector C can be selected as the same as the Miller iteration parameters of optimal pairings [43] on many popular pairing-friendly curves. It indicates that the bit length of n is about $\log r / \varphi(k)$ on these curves. This result induces an efficient method of $\mathbb{G}_2$ membership testing.

3.2 Pairing-friendly curves with the lack of twists

Let E be an ordinary curve with the lack of twists. Recall from Section 2.1 that

$$Q \in \mathbb{G}_2 = E[r] \cap \text{Ker}(\pi - [p]) \Leftrightarrow Q \in E(\mathbb{F}_{p^k}), Q \in E[r] \text{ and } Q \in \mathcal{G}_2,$$

where $\mathcal{G}_2 = \text{Ker}\left(\Phi_k(\pi)\right)$. Since checking $Q \in \mathcal{G}_2$ only requires a few point additions and applications of the endomorphism π, the computational cost of the testing comes largely from checking $Q \in E[r]$. It is interesting to observe that Theorem 1 can be generalized to accomplish this checking by substituting the endomorphism ψ by π. We summarize the observation in the following corollary.

Corollary 1 Let E be an ordinary elliptic curve over $\mathbb{F}_p$ with the lack of twists, and other notations as in Theorem 1. Assume that b_0, $b_1 \in \mathbb{Z}$ with

$$\gcd(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, \#\mathcal{G}_2) = r. \tag{9}$$

Given a non-identity point Q of $E(\mathbb{F}_{p^k})$, then $Q \in \mathbb{G}_2$ if and only if $f(\pi)(Q) = \mathcal{O}_E$ and $Q \in \mathcal{G}_2$.

Proof The necessity is obvious and we now prove the sufficiency. It follows from Eq.(1) that

$$\pi^2(Q) - [t]\pi(Q) + [p]Q = \mathcal{O}_E. \tag{10}$$

Similar to the proof in Theorem 1, the condition $f(\pi)(Q) = \mathcal{O}_E$ and Eq. (10) indicate that the order of Q divides $b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p$. Furthermore, since $Q \in \mathcal{G}_2$ and

$Q \neq \mathcal{O}_E$, Eq.(9) implies that the order of Q is precisely r. Thus, we conclude that $Q \in E[r] \cap \mathcal{G}_2 = \mathbb{G}_2$, which completes the proof.   □

Corollary 1 induces an efficient method of $\mathbb{G}_2$ membership testing on pairing-friendly curves with the lack of twists. Likewise, the complexity of the method is about $O(\log r / \varphi(k))$ in many cases.

Given an ordinary curve E over $\mathbb{F}_p$ with j-invariant 0 or 1728. Recall from Section 2.2 that there exists a GLV endomorphism τ on E. Denote d to be the order of τ. It is obvious that $d \in \{3, 4\}$. If E is a curve with the lack of twists, then $\gcd(k, 6) = 1$ [26, Section 1], and thus we have $\gcd(k, d) = 1$. In the following, we further optimize the efficiency of the $\mathbb{G}_2$ membership testing on this class of curves. The new method works under a mild condition. Our general understanding of the construction of this method comes mostly from the following theorem.

Theorem 2 *Let E be an ordinary elliptic curve over $\mathbb{F}_p$ with the lack of twists, and j-invariant 0 or 1728. Let r be a large prime such that $r \parallel \#E(\mathbb{F}_p)$, t the trace of the Frobenius π on E, and k the embedding degree of E with respect to r. Let τ be a GLV endomorphism on E with order d, and act as multiplication by an integer λ in $\mathbb{G}_2$. Let i be a positive integer with $\gcd(k, i) = 1$, and denote m to be the inverse of $d \cdot i$ modulo k. Assume that*

$$\gcd(b^{2d \cdot m} - t \cdot b^{d \cdot m} + p, \#\mathcal{G}_2) = r, \tag{11}$$

where $b = (t-1)^i \cdot \lambda^{-1} \bmod r$. Given a non-identity point $Q \in E(\mathbb{F}_{p^k})$, then $Q \in \mathbb{G}_2$ if and only if $\pi^i(Q) = [b]\tau(Q)$ and $Q \in \mathcal{G}_2$.

Proof Recall that $\gcd(k, d) = 1$ on pairing-friendly curves with the lack of twists according to the previous discussions. By the assumption, we have $\gcd(k, i) = 1$. This means that $\gcd(d \cdot i, k) = 1$ and so there exists an integer m that is the inverse of $d \cdot i$ modulo k.

If $Q \in \mathbb{G}_2$, it is obvious that $Q \in \mathcal{G}_2$ as $\mathbb{G}_2 \subset \mathcal{G}_2$. Furthermore, since $\tau(Q) = [\lambda]Q$ and $\pi(Q) = [t-1]Q$ we have

$$\pi^i(Q) = [(t-1)^i \bmod r]Q = [b \cdot \lambda]Q = [b]\tau(Q).$$

Conversely, if $\pi^i(Q) = [b]\tau(Q)$ we get

$$\pi^{d \cdot i}(Q) = [b^d]\tau^d(Q) = [b^d]Q,$$

as the order of τ is d. Since $d \cdot i \cdot m \equiv 1 \bmod k$, there exists an integer n such that $d \cdot m \cdot i - n \cdot k = 1$. This implies that

$$\pi(Q) = \pi^{1+n \cdot k}(Q) = \pi^{d \cdot m \cdot i}(Q) = [b^{d \cdot m}]Q. \tag{12}$$

Furthermore, it follows from Eq. (1) that

$$\pi^2(Q) - [t]\pi(Q) + [p]Q = \mathcal{O}_E. \tag{13}$$

Combining Eqs. (12) and (13), it yields that

$$[b^{2d \cdot m} - t \cdot b^{d \cdot m} + p]Q = \mathcal{O}_E. \tag{14}$$

On the other hand, since $Q \in \mathcal{G}_2$, Eq. (14) indicates that the order of Q divides $\gcd\left(b^{2d \cdot m} - t \cdot b^{d \cdot m} + p, \#\mathcal{G}_2\right)$. From Eq. (11), we conclude that $Q \in E[r] \cap \mathcal{G}_2 = \mathbb{G}_2$, which completes the proof.   □

In Theorem 2, the integer m can be calculated by the extended Euclidean algorithm once the parameter i is fixed. To minimize the computational cost, we expect that the bit length of b is as small as possible. Since $t-1$ is a primitive k-th root of unity modulo r, the optimal parameter b can be obtained by exhausting $i \in \{0, 1, \cdots k-1\}$ such that $\gcd(k, i) = 1$ under the assumption (11). We fortunately find that Theorem 2 induces a fast $\mathbb{G}_2$ membership testing method on the BW13-P310 and BW19-P286 curves. It is interesting to observe that the time complexity is reduced to $O\big(\log r/(2\varphi(k))\big)$ on these curves. We will give the details in Section 5.

4 $\mathbb{G}_1$ and $\mathbb{G}_T$ Membership Testings

In this section, we investigate the problems of membership testings for $\mathbb{G}_1$ and $\mathbb{G}_T$.

4.1 The $\mathbb{G}_1$ case

If E is a curve in the BN or BLS family, it is confirmed from [13, 18] that

$$P \in \mathbb{G}_1 = E(\mathbb{F}_p)[r] \Leftrightarrow P \in E(\mathbb{F}_p) \text{ and } \tau(P) = [\lambda]P,$$

where λ is one of the roots of the equation $x^2 + x + 1 \equiv 0 \bmod r$. The new technique significantly reduces the computational cost compared to the naive one. In this subsection, we generalize this method to all ordinary curves with j-invariant 0 or 1728.

Theorem 3 *Let E be an ordinary elliptic curve over $\mathbb{F}_p$ with j-invariant 0 or 1728, and r a large prime such that $r \parallel \#E(\mathbb{F}_p)$. Let τ be a GLV endomorphism on E, and act as multiplication by an integer λ in $\mathbb{G}_1$. Let $a_0, a_1 \in \mathbb{Z}$ with $a_0 + a_1 \cdot \lambda \equiv 0 \bmod r$. Assume*

$$\begin{cases} \gcd\left(a_0^2 - a_0 \cdot a_1 + a_1^2, \#E(\mathbb{F}_p)\right) = r, \text{if } j(E) = 0, \\ \gcd\left(a_0^2 + a_1^2, \#E(\mathbb{F}_p)\right) = r, \text{if } j(E) = 1728. \end{cases} \tag{15}$$

Given a non-identity point $P \in E(\mathbb{F}_p)$, then the candidate point $P \in \mathbb{G}_1$ if and only if $[a_0]P + [a_1]\tau(P) = \mathcal{O}_E$.

Proof We only give the proof for the case $j(E) = 0$ as the other case is analogous. If $P \in \mathbb{G}_1$, then the order of P is r and $\tau(P) = [\lambda]P$. Since $a_0 + a_1 \cdot \lambda \equiv 0 \bmod r$ we have

$$[a_0]P + [a_1]\tau(P) = [a_0 + a_1 \cdot \lambda]P = \mathcal{O}_E.$$

Conversely, since $\tau^2 + \tau + 1 = 0$ we get

$$[a_1^2]\tau^2(P) + [a_1^2]\tau(P) + [a_1^2]P = \mathcal{O}_E. \tag{16}$$

If $[a_0]P + [a_1]\tau(P) = \mathcal{O}_E$, we obtain from Eq. (16) that

$$[a_0^2 - a_0 \cdot a_1 + a_1^2]P = \mathcal{O}_E.$$

Since $\gcd\left(a_0^2 - a_0 \cdot a_1 + a_1^2, \#E(\mathbb{F}_p)\right) = r$, we conclude that $P \in \mathbb{G}_1$, which completes the proof. □

Analogous to $\mathbb{G}_2$ membership testing, there always exist a_0 and a_1 satisfying the constraint (15). In practice, the bit length of $max\{|a_0|, |a_1|\}$ is of about $\log r/2$ on many pairing-friendly curves. Based on the analysis above, our method may be a better choice than the method of clearing cofactor even in efficiency if the ratio of $\log h_1$ to $\log r$ is no less than 0.5. For example, on pairing-friendly curves with embedding degrees 6 and 8 constructed by Guillevic *et al.* [44], the cofactors h_1 are even larger than r. In this situation our method is clearly a winner.

4.2 The $\mathbb{G}_T$ case

Scott [18] proposed an efficient method of $\mathbb{G}_T$ membership testing under the condition that $\gcd(h_1, h_T) = 1$, which is tailored to the BN and BLS families. In particular, let α be a candidate element which is claimed to be a member of $\mathbb{G}_T$. The verifier requires to check whether $\alpha \in \mathbb{G}_{\Phi_k(p)}$ and $\alpha^{p+1} = \alpha^t$. Since the Frobenius map can be computed efficiently, the computational cost of the testing is dominated by one exponentiation by t. Inspired by the technique of $\mathbb{G}_2$ membership testing on pairing-friendly curves admitting a twist, we propose an efficient method of $\mathbb{G}_T$ membership testing.

Proposition 4 *Let η be a multiple of r and write η in the basis of p as $\eta = \sum\limits_{i=0}^{s} c_i \cdot p^i$. Assume $\alpha \neq 1$ be an element of $\mathbb{F}_{p^k}^*$ and $\gcd\left(\eta, \Phi_k(p)\right) = r$. Then $\alpha \in \mathbb{G}_T$ if and only if*

$$\alpha^{\Phi_k(p)} = 1 \ \text{ and } \ \alpha^{\eta} = 1.$$

Proof Since $r \mid \Phi_k(p)$ and $r \mid \eta$, the necessity is straightforward. Conversely, if $\alpha^{\Phi_k(p)} = 1$ and $\alpha^{\eta} = 1$ then the order of α divides $\gcd\left(\eta, \Phi_k(p)\right)$. Since $\gcd\left(\eta, \Phi_k(p)\right) = r$ and $\alpha \neq 1$, it is clear that the order of α is precisely r and thus $\alpha \in \mathbb{G}_T$, which completes the proof. $\square$

In Proposition 4, we provide a general method of $\mathbb{G}_T$ membership testing that does not depend on the condition $\gcd(h_1, h_T) = 1$. Similar to $\mathbb{G}_2$ membership testing, the vector $C = [c_0, c_1, \cdots, c_s]$ can be selected as the same as the Miller iteration parameters of optimal pairings on many popular pairing-friendly curves. It means that $\log n \approx \log r/\varphi(k)$, where $n = max\{|c_0|, |c_1|, \cdots, |c_s|\}$. Moreover, once the candidate element α is proved to be a member of $\mathbb{G}_{\Phi_k(p)}$, the fixed exponentiation by n can be further optimized by techniques of fast cyclotomic squaring [45, 46] in the case that the embedding degree k is divided by 6.

5 Applications

Sections 3 and 4 induce efficient methods of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings. In this section, we investigate how to apply these techniques to

Table 2 Short vectors of the membership testings on a list of pairing-friendly curves at the 128-bit security level. For the BW13-P310 and BW19-P286 curves, the vectors C in the column of $\mathbb{G}_2$ are denoted by $[i, m, b]$, where the parameters i, m and b are defined in Theorem 2. For the KSS16-P330 curve, the vectors C for $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings are presented in Section 5.2.

Curve	$[a_0, a_1]$	$C(\mathbb{G}_2)$	$C(\mathbb{G}_T)$
BN-P446	—	$[2z, z+1, -z, z]$	$[2z, z+1, -z, z]$
BLS12-P461	$[z^2, 1]$	$[z, -1, 0, 0]$	$[z, -1, 0, 0]$
KSS16-P330	$[(31z^4 + 625)/8750, -(17z^4 + 625)/8750]$	—	—
KSS18-P348	$[(z/7)^3, -18a_0 - 1]$	$[2z/7, 1, 0, z/7, 0, 0]$	$[2z/7, 1, 0, z/7, 0, 0]$
BW13-P310	$[-(z^7 + z)(z^4 + z^3 - z - 1), a_0 \cdot z - 1]$	$[1, 9, -z]$	$[z^2, -z, 1, 0, \ldots, 0]$
BW19-P286	$[(z - z^{10})(z^6 - z^3 + 1)(z + 1), a_0 \cdot z - 1]$	$[1, 13, -z]$	$[z^2, -z, 1, 0, \cdots, 0]$

different pairing-friendly curves in detail. To this aim, we first provide a Magma code to search target coefficient vectors that ensure the associated computational costs are as small as possible. The code is available in https://github.com/eccdaiy39/smt-magma/tree/main/vector. The related datas are collected in Table 2. On this basis, we take the BN-P446, KSS16-P330 and BW13-P310 curves as examples to further illustrate the main mechanics of the proposed techniques.

5.1 BN-P446

The BN family is parameterized by

$$\begin{cases} r(z) = 36z^4 + 36z^3 + 18z^2 + 6z + 1, \\ t(z) = 6z^2 + 1, \\ p(z) = 36z^4 + 36z^3 + 24z^2 + 6z + 1. \end{cases}$$

The seed z is recommended as $z = 2^{110} + 2^{36} + 1$ [37] to achieve the 128-bit security level. Let $E(\mathbb{F}_p)$ and $E'(\mathbb{F}_{p^2})$ define the BN curve and its sextic twist, respectively. Note that the $\mathbb{G}_1$ membership testing is not necessary as $h_1 = 1$ on the curve. For both $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings the coefficient vectors are taken as $[2z, z+1, -z, z]$. Let Q be a point that purports to be an element of $\mathbb{G}_2$. By Theorem 1, the point Q is valid if and only if

$$\begin{cases} Q \in E'(\mathbb{F}_{p^2}), \\ [2z]Q + \psi([z+1]Q) + \psi^3([z]Q) = \psi^2([z]Q). \end{cases}$$

In total, it requires approximately one scalar multiplication by z, three point additions, one point doubling and three applications of the endomorphism ψ. The above computational overhead is actually dominated by the scalar multiplication by z. By the form of the polynomial $r(z)$, we can see that $\log|z| \approx \log r/4$.

Likewise, by Proposition 1, a candidate element $\alpha \in \mathbb{G}_T$ if and only if

$$\begin{cases} a \cdot \alpha^{p^4} = \alpha^{p^2}, \\ \alpha^{2z} \cdot (\alpha^{z+1})^p \cdot (\alpha^z)^{p^3} = (\alpha^z)^{p^2}. \end{cases}$$

Thus, this membership testing requires one exponentiation by z, four field multiplications, one field squaring and five applications of the endomorphism π. Since the selected parameter z has a low Hamming weight, it is efficient to perform the exponentiation by z using the compression technique proposed in [46].

Remark 1 The previous leading works of $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings on the BN family were proposed in [11, 13]. To be precise, both of the two computational costs are of approximately one scalar multiplication/exponentiation by $6z^2$. Clearly, our method is more efficient as compared to the previous one.

Remark 2 We fortunately find that the vector $C = [z + 1, z, z, -2z]$ is suitable for both $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings on other curves in the family, such as BN-P254 $(z = -(2^{62} + 2^{55} + 1))$ and BN-P382 $(z = -(2^{94} + 2^{78} + 2^{67} + 2^{64} + 2^{48} + 1))$. But it does not mean that the short vector is independent of the seed z. Indeed, for such a vector the associated parameters b_0 and b_1 are given as

$$b_0 = -216z^7 - 216z^6 - 144z^5 - 36z^4 - 6z^3 + 2z,$$
$$b_1 = -36z^4 - 18z^3 - 6z^2 + 1.$$

Then we have $b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p = h_2' \cdot r$, where

$$h_2' = 1296z^{10} + 2592z^9 + 3024z^8 + 2160z^7 + 1044z^6 +$$
$$252z^5 - 60z^4 - 66z^3 - 14z^2 + 2z + 1.$$

On the other hand, the cofactor $h_2 = 36z^4 + 30z^3 + 30z^2 + 6z + 1$ [9, Proposition 1]. As shown in Theorem 1, the short vector is desired for $\mathbb{G}_2$ membership testing if $\gcd(h_2, h_2') = 1$. However, the condition does not always hold. For example, taking $z = 9853$ we find that $\gcd(h_2, h_2') = 95$.

5.2 KSS16-P330

The KSS16 family is parameterized by

$$\begin{cases} r(z) = \dfrac{z^8 + 48z^4 + 625}{61250}, \\ t(z) = \dfrac{2z^5 + 41z + 35}{35}, \\ p(z) = \dfrac{z^{10} + 2z^9 + 5z^8 + 48z^6 + 152z^5 + 240z^4 + 625z^2 + 2398z + 3125}{980}. \end{cases}$$

Following the recommendation in [36], we take $z = -2^{34}+2^{27}-2^{23}+2^{20}-2^{11}+1$ to achieve the 128-bit security level. In the subsection, we use $E(\mathbb{F}_p)$ and $E'(\mathbb{F}_{p^4})$ to denote the KSS16 curve and its quartic twist, respectively.

5.2.1 the $\mathbb{G}_1$ case

For the $\mathbb{G}_1$ membership testing, the parameters a_0 and a_1 are given as

$$\begin{cases} a_0 = (31z^4 + 625)/8750, \\ a_1 = -(17z^4 + 625)/8750. \end{cases}$$

Let $a_0' = 17a_0$ and $a_1' = 17a_1$. Since $-17a_0 - 31a_1 = 1$ and $\gcd\left(a_0'^2 + a_1'^2, \#E(\mathbb{F}_p)\right) = r$, we substitute the values a_0 and a_1 by a_0' and a_1', respectively. As a consequence, given a point Q that is claimed to be a member of $\mathbb{G}_1$, the associated membership testing can be accomplished by checking that

$$\begin{cases} Q \in E(\mathbb{F}_p), \\ \tau([17a_1]Q) - [31a_1]Q = Q. \end{cases}$$

Given the point $R = [a_1]Q$, we then obtain $[17]R$ and $[31]R$ by performing the following calculations:

$$R \to [2]R \to [4]R \to [8]R \to [16]R \to [17]R \to [32]R \to [31]R.$$

In conclusion, the $\mathbb{G}_1$ membership testing requires approximately one scalar multiplication by a_1, five point doublings, three point additions and one application of the endomorphism τ. Clearly, the overhead of this testing comes mostly from the scalar multiplication by a_1. This operation requires to perform about $\lceil \log r/2 \rceil$ iterations.

5.2.2 the $\mathbb{G}_2$ and $\mathbb{G}_T$ cases

We find that $\gcd(h_1, h_2) = \gcd(h_1, h_T) = 4$. Thus the method of Scott [18] for $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings is not suitable for the curve. Let $u = (-z-25)/70$. For both $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings, the coefficient vectors are taken as $[c_0, c_1, \cdots, c_7]$, where

$$\begin{aligned} &c_6 = u, c_2 = c_3 = 3c_6 + 1, c_1 = -3c_2, c_5 = 2c_2 + c_6 + 1, \\ &c_4 = -2c_5 + c_6 + 1, c_0 = c_7 = 2c_6 - c_1 + 1. \end{aligned}$$

Let Q be a point whch is claimed to be a member of $\mathbb{G}_2$ on the curve. By Theorem 1, the point Q is valid if and only if

$$
\begin{cases}
Q \in E'(\mathbb{F}_{p^4}), \\
\displaystyle\sum_{i=0}^{6} \psi^i([c_i]Q) = -\psi([c_7]Q),
\end{cases}
$$

which requires approximately one scalar multiplication by u, three point doublings, thirteen point additions and seven applications of the endomorphism ψ. The most costly part of this testing is the scalar multiplication by u, which is roughly $\lceil \log r/8 \rceil$ bits. Here we omit the details of the $\mathbb{G}_T$ membership testing as it is similar.

5.3 BW13-P310

The methods of the membership testings for $\mathbb{G}_1$ and $\mathbb{G}_T$ have no difference between pairing-friendly curves admitting a twist and with the lack of twists. For brevity, we only discuss the membership testing for $\mathbb{G}_2$ on the BW13-P310 curve. From Construction 6.6 in [35], a family of curves with $k = 13$ and j-invariant 0 can be parameterized by:

$$
\begin{cases}
r(z) = \Phi_{78}(z), \\
t(z) = -z^{14} + z + 1, \\
p(z) = \dfrac{1}{3}(z+1)^2(z^{26} - z^{13} + 1) - z^{27}.
\end{cases}
$$

In order to reach the 128-bit security level, the seed z is recommended as $z = -2224$ [37]. The curve is defined by the equation $y^2 = x^3 - 17$. By the form of the polynomial $r(z)$, we can see that

$$
z^{26} - z^{13} + 1 \equiv 0 \bmod r.
$$

Thus, there exists a GLV endomorphisms τ with eigenvalue $\lambda = z^{13} - 1$ restricted in $\mathbb{G}_2$. Let notations i, m and b be defined as in Theorem 2. Taking $i = 1$, we have $b = -z$, $m = 9$ and $\gcd\left(b^{6 \cdot m} - t \cdot b^{3 \cdot m} + p, \#\mathcal{G}_2\right) = r$, where $\#\mathcal{G}_2 = \#E(\mathbb{F}_{p^{13}})/\#E(\mathbb{F}_p)$. By Theorem 2, the $\mathbb{G}_2$ membership testing requires to check that

$$
\begin{cases}
Q \in E(\mathbb{F}_{p^{13}}), \\
\pi(Q) = [-z]\tau(Q), \\
\displaystyle\sum_{i=1}^{12} \pi^i(Q) = -Q.
\end{cases}
$$

Note that $\sum_{i=1}^{12} \pi^i(Q)$ can be calculated by using the following formulas:

$$
R_1 = \pi(Q) + \pi^2(Q), \; R_2 = \pi^2(R_1), \; R_3 = R_1 + R_2,
$$

Table 3 The number of bit operations of subgroup membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ across different pairing-friendly curves

Curve	$\lceil \log r/2 \rceil$	$\lceil \log r/\varphi(k) \rceil$	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_T$
BN-P446	224	112	−	111	111
BLS12-P461	154	77	154	77	77
KSS16-P330	129	33	133	31	31
KSS18-P348	128	43	124	43	43
BW13-P310	134	23	134	12	23
BW19-P286	130	15	130	8	15

$$R_4 = \pi^4(R_3), R_5 = \pi^4(R_4), \sum_{i=1}^{12} \pi^i(Q) = R_3 + R_4 + R_5.$$

Neglecting the cost of checking $Q \in E(\mathbb{F}_{p^{13}})$, it totally costs one scalar multiplication by z, four point additions, five applications of the endomorphism π and one application of the endomorphism τ. Note that the computational cost comes largely from one scalar multiplication by z. Since $\deg\big(r(z)\big) = 2\varphi(k)$, it is interesting to see that $\log|z| \approx \log r/\big(2\varphi(k)\big)$.

5.4 Efficiency analysis

In Table 3, we give the number of bit operations of subgroup membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ across different pairing-friendly curves. Specifically,

- For $\mathbb{G}_1$ and $\mathbb{G}_T$ membership testings on these curves, the time complexities of the proposed techniques are in $O(\log r/2)$ and $O(\log r/\varphi(k))$, respectively;
- For $\mathbb{G}_2$ membership testing on the four pairing-friendly curves admitting a twist, the time complexity of the new technique is in $O(\log r/\varphi(k))$;
- For $\mathbb{G}_2$ membership testing on the BW13-P310 and BW19-P286 curves, the time complexity of the new technique is in $O(\log r/(2\varphi(k)))$.

In summary, these results are consistent with the theoretical analysis of Sections 3 and 4.

6 Implementation Results

Magma implementation for subgroup membership testings on pairing-friendly curves listed in Table 2 was provided in https://github.com/eccdaiy39/ smt-magma/tree/main/test. It can be used to verify the correctness of the new methods even though performs poorly. In order to accurately evaluate the performance improvements that are gained from the proposed techniques, we also present software implementation results on the BN-P446 and BW13-P310 curves within the RELIC [22] cryptographic library. The code is available at https://github.com/eccdaiy39/smt. We notice that the previous leading works [11, 13] of the $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings on the BN-P446 curve were implemented in the library. In Table 4, we summarize the results of benchmarks on a 64-bit Intel Core i7-8550U@1.8GHz processor running Ubuntu

Table 4 Timings for subgroup membership testings on the BN-P446 and BW13-P310 curves. The results are given in clock cycles ($\times 10^3$).

Curve	Method	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_T$
BN-P446	Previous work [11, 13]	−	722	882
BN-P446	This work	−	352	471
BW13-P310	This work	293	1220	225

18.04.1 LTS with TurboBoost and hyper-threading features disabled. Timing results are obtained averaged over 10,000 executions. As shown in Table 4, on the BN-P446 curve the new algorithm for the $\mathbb{G}_2$ membership testing is about 105.1% times faster than that from [13], while the $\mathbb{G}_T$ membership testing is about 87.3% times faster than that from [11]. As far as we know, the problem of subgroup membership testing on the BW13-P310 curve has not yet considered in the literature. Applying the new techniques, we find that subgroup membership testings on this curve are also efficient.

7 Conclusion

The threat of small-subgroup attacks are non-negligible in pairing-based protocols. Subgroup membership testing is a useful measure to defense such attacks. In this paper, we revisited this problem and described efficient methods of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings, which were suitable for a large class of ordinary pairing-friendly curves. Fast software implementation of subgroup membership testings was presented to further confirm the performance of the proposed algorithms. On the BN-P446 curve, our timing results are significantly faster than those in the previous leading work.

Acknowledgement

References

[1] Joux, A.: A One Round Protocol for Tripartite Diffie–Hellman. In: Bosma, W. (ed.) Algorithmic Number Theory Symposium – ANTS 2000, pp. 385–393. Springer, Berlin, Heidelberg (2000)

[2] 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 (2001)

[3] Chen, L., Cheng, Z., Smart, N.P.: Identity-based Key Agreement Protocols from Pairings. International Journal of Information Security **6**(4), 213–241 (2007)

[4] Joye, M., Neven, G.: Identity-based Cryptography. Cryptology and Information Security. IOS press, Amsterdam (2009)

[5] Diem, C., Thomé, E.: Index Calculus in Class Groups of Non-hyperelliptic Curves of Genus Three. Journal of Cryptology **21**(4), 593–611 (2008)

[6] Gaudry, P., Hess, F., Smart, N.P.: Constructive and Destructive Facets of Weil Descent on Elliptic Curves. Journal of Cryptology **15**(1), 19–46 (2002)

[7] Tian, S., Li, B., Wang, K., Yu, W.: Cover Attacks for Elliptic Curves with Cofactor Two. Designs, Codes and Cryptography **86**(11), 2451–2468 (2018)

[8] Lim, C.H., Lee, P.J.: A Key Recovery Attack on Discrete Log-Based Schemes Using a Prime Order Subgroup. In: Kaliski, B.S. (ed.) Advances in Cryptology – CRYPTO 1997, pp. 249–263. Springer, Berlin, Heidelberg (1997)

[9] Barreto, P.S.L.M., Costello, C., Misoczki, R., Naehrig, M., Pereira, G.C.C.F., Zanon, G.: Subgroup Security in Pairing-Based Cryptography. In: Lauter, K., Rodríguez-Henríquez, F. (eds.) Progress in Cryptology – LATINCRYPT 2015, pp. 245–265. Springer, Cham (2015)

[10] Pohlig, S., Hellman, M.: An Improved Algorithm for Computing Logarithms over GF(p) and Its Cryptographic Significance. IEEE Transactions on Information Theory **24**(1), 106–110 (1978)

[11] Scott, M.: Unbalancing Pairing-Based Key Exchange Protocols. Cryptology ePrint Archive, Paper 2013/688 (2013). https://eprint.iacr.org/2013/688

[12] Aranha, D.F., Pagnin, E., Rodríguez-Henríquez, F.: LOVE a Pairing. In: Longa, P., Ràfols, C. (eds.) Progress in Cryptology – LATINCRYPT 2021, pp. 320–340. Springer, Cham (2021)

[13] El Housni, Y., Guillevic, A., Piellard, T.: Co-factor Clearing and Subgroup Membership Testing on Pairing-friendly Curves. Cryptology ePrint Archive, Report 2022/352. https://ia.cr/2022/352 (2022)

[14] Scott, M., Benger, N., Charlemagne, M., Dominguez Perez, L.J., Kachisa, E.J.: Fast Hashing to $\mathbb{G}_2$ on Pairing-Friendly Curves. In: Shacham, H., Waters, B. (eds.) Pairing-Based Cryptography – Pairing 2009, pp. 102–113. Springer, Berlin, Heidelberg (2009)

[15] Fuentes-Castañeda, L., Knapp, E., Rodríguez-Henríquez, F.: Faster Hashing to $\mathbb{G}_2$. In: Miri, A., Vaudenay, S. (eds.) Selected Areas in Cryptography

– SAC 2011, pp. 412–430. Springer, Berlin, Heidelberg (2012)

[16] Budroni, A., Pintore, F.: Efficient Hash Maps to $\mathbb{G}_2$ on BLS Curves. Applicable Algebra in Engineering, Communication and Computing **33**(3), 261–281 (2022)

[17] Hamburg, M.: Decaf: Eliminating Cofactors Through Point Compression. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology – CRYPTO 2015, pp. 705–723. Springer, Berlin, Heidelberg (2015)

[18] Scott, M.: 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). https://eprint.iacr.org/2021/1130

[19] Barreto, P.S.L.M., Lynn, B., Scott, M.: On the Selection of Pairing-Friendly Groups. In: Matsui, M., Zuccherato, R.J. (eds.) Selected Areas in Cryptography – SAC 2003, pp. 17–25. Springer, Berlin, Heidelberg (2004)

[20] Barreto, P.S.L.M., Naehrig, M.: Pairing-Friendly Elliptic Curves of Prime Order. In: Preneel, B., Tavares, S. (eds.) Selected Areas in Cryptography – SAC 2005, pp. 319–331. Springer, Berlin, Heidelberg (2006)

[21] 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 (2008)

[22] Aranha, D.F., Gouvêa, C.P.L.: RELIC is an Efficient LIbrary for Cryptography. https://github.com/relic-toolkit/relic

[23] Balasubramanian, R., Koblitz, N.: The Improbability That an Elliptic Curve Has Subexponential Discrete Log Problem under the Menezes-Okamoto-Vanstone Algorithm. Journal of Cryptology **11**(2), 141–145 (1998)

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

[25] Enge, A., Milan, J.: Implementing Cryptographic Pairings at Standard Security Levels. In: Chakraborty, R.S., Matyas, V., Schaumont, P. (eds.) Security, Privacy, and Applied Cryptography Engineering – SPACE 2014, pp. 28–46. Springer, Cham (2014)

[26] Dai, Y., Zhang, F., Zhao, C.-A.: Fast Hashing to $\mathbb{G}_2$ in Direct Anonymous Attestation. Cryptology ePrint Archive, Paper 2022/996 (2022). https://eprint.iacr.org/2022/996

[27] Washington, L.C.: Elliptic Curves: Number Theory and Cryptography. Chapman and Hall/CRC, Boca Raton (2008)

[28] 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 (2001)

[29] Galbraith, S.D., Scott, M.: Exponentiation in Pairing-Friendly Groups Using Homomorphisms. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing-Based Cryptography – Pairing 2008, pp. 211–224. Springer, Berlin, Heidelberg (2008)

[30] Galbraith, S.D., Lin, X., Scott, M.: Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves. In: Joux, A. (ed.) Advances in Cryptology – EUROCRYPT 2009, pp. 518–535. Springer, Berlin, Heidelberg (2009)

[31] Hu, Z., Longa, P., Xu, M.: Implementing the 4-dimensional GLV Method on GLS Elliptic Curves with j-invariant 0. Designs, Codes and Cryptography **63**(3), 331–343 (2012)

[32] Joux, A., Pierrot, C.: The Special Number Field Sieve in $\mathbb{F}_{p^n}$. In: Cao, Z., Zhang, F. (eds.) Pairing-Based Cryptography – Pairing 2013, pp. 45–61. Springer, Cham (2014)

[33] 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 (2016)

[34] Bosma, W., Cannon, J., Playoust, C.: The Magma Algebra System. I. The User Language. J. Symbolic Comput. **24**(3-4), 235–265 (1997). Computational algebra and number theory (London, 1993)

[35] Freeman, D., Scott, M., Teske, E.: A Taxonomy of Pairing-Friendly Elliptic Curves. Journal of Cryptology **23**(2), 224–280 (2010)

[36] Barbulescu, R., Duquesne, S.: Updating Key Size Estimations for Pairings. Journal of Cryptology **32**(4), 1298–1336 (2019)

[37] 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, Cham (2020)

[38] Clarisse, R., Duquesne, S., Sanders, O.: Curves with Fast Computations in

the First Pairing Group. In: Krenn, S., Shulman, H., Vaudenay, S. (eds.) Cryptology and Network Security – CANS 2020, pp. 280–298. Springer, Cham (2020)

[39] 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)

[40] Brickell, E., Camenisch, J., Chen, L.: Direct Anonymous Attestation. In: Proceedings of the 11th ACM Conference on Computer and Communications Security – CCS2004, pp. 132–145. Association for Computing Machinery, New York (2004)

[41] Miyaji, A., Nakabayashi, M., Takano, S.: Characterization of Elliptic Curve Traces Under FR-Reduction. In: Won, D. (ed.) Information Security and Cryptology – ICISC 2000, pp. 90–108. Springer, Berlin, Heidelberg (2001)

[42] Freeman, D.: Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10. In: Hess, F., Pauli, S., Pohst, M. (eds.) Algorithmic Number Theory – ANTS 2006, pp. 452–465. Springer, Berlin, Heidelberg (2006)

[43] Vercauteren, F.: Optimal Pairings. IEEE Transactions on Information Theory **56**(1), 455–461 (2009)

[44] Guillevic, A., Masson, S., Thomé, E.: Cocks-Pinch Curves of Embedding Degrees Five to Eight and Optimal Ate Pairing Computation. Designs, Codes and Cryptography **88**(6), 1047–1081 (2020)

[45] Granger, R., Scott, M.: Faster Squaring in the Cyclotomic Subgroup of Sixth Degree Extensions. In: Nguyen, P.Q., Pointcheval, D. (eds.) Public Key Cryptography – PKC 2010, pp. 209–223. Springer, Berlin, Heidelberg (2010)

[46] Karabina, K.: Squaring in Cyclotomic Subgroups. Mathematics of Computation **82**(281), 555–579 (2012)