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], Chang-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: daiy39@mail2.sysu.edu.cn;
linkzh5@mail2.sysu.edu.cn; zhaochan3@mail.sysu.edu.cn;
zhouzijian122006@163.com;

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 causes an expensive computational cost on many pairing-friendly curves. Recently, Scott proposed efficient methods of subgroup membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_\mathrm{T}$ on the BLS family. In this paper, we generalize these methods and show that the new techniques are applicable to a large class of pairing-friendly curves. In particular, we also confirm that our new methods lead to a significant speedup for subgroup membership testings on many popular pairing-friendly curves at high security level.

Keywords: Pairing-based cryptography, Small-subgroup attacks, Group membership testing, High security level.

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 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 two 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 results in potential risks of secret key exposures under small-subgroup attacks [8, 9]. Specially, we assume that 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 a if the point $[a]P$ is published. For the worst case, the cofactor h could provide enough small prime factors such that attackers 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 reducing the chances of such attacks is to increase the size of parameters such that the cofactor h has no prime factors smaller than r [9]. In this case, we call $\mathbb{G}$ 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 inputs by the corresponding cofactor h to force them into the correct subgroup. If the result of the cofactor multiplication is exactly the identity element, then the protocol is aborted. In the case of $\mathbb{G}_1$, the cofactor h is small on many pairing-friendly curves. Thus, the cofactor can be "cleared" at a 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 [14–17]. Even though this method can resist small-subgroup attacks, it also causes other problems. As pointed out by Hamburg [18], implementors must determine which points to execute "clearing cofactors" on. Moreover, cofactor multiplication also changes system parameters. This would lead to additional troubles for implementors [19].

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 check whether a candidate element has order r, i.e., raise it 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 whole performance of pairing-based cryptographic protocols. Recently, Scott [19] proposed a novel method for subgroup membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on the Barreto-Lynn-Scott (BLS) [20] 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) [21] family.

1.3 Our contributions

Motivated by the work of Scott [19], we propose more general membership testing methods. We show that our new techniques are suitable for a large class of pairing-friendly curves, including BN, BLS and Kachisa-Schaefer-Scott (KSS) [22] families. We summarize our contributions as follows.

- We present a general method for $\mathbb{G}_2$ membership testing on pairing-friendly curves. It is shown that this method requires around $\log r/\varphi(k)$ bit operations on many pairing-friendly curves. It is particularly interesting to see that the number of bit operations can be further reduced to around $\log r/(2\varphi(k))$ on some certain curves.
- Fast methods for $\mathbb{G}_1$ and $\mathbb{G}_T$ membership testings are also proposed, which require approximately $\log r/2$ and $\log r/\varphi(k)$ bit operations, respectively. For $\mathbb{G}_1$ membership testing, our method mainly aims to ordinary elliptic 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 [23] 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. In Section 5, we present implementation results. The conclusion is given in Section 6.

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 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 $E(\mathbb{F}_{p^k})$ [24]. The p-power Frobenius endomorphism $\pi : (x, y) \rightarrow (x^p, y^p)$ on E satisfies the characteristic equation

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

where the Frobenius 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 [25]. 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 for subgroup membership testings:

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

where $\mathcal{O}_{E'}$ denotes the identity point of E'. Following Enge and Milan [26], 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 $r \nmid \Phi_k(1)$ [27, §.IX.7.4], [28, §.26.6.1], [29] membership testing for $\mathbb{G}_2$ on such a 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 the prime r is very large, the naive method is extremely slow in practice.

2.2 Endomorphisms of ordinary elliptic curves

Consider an ordinary elliptic curve E_1 over $\mathbb{F}_p$ with j-invariant 0 first. Then the curve is defined by the equation $y^2 = x^3 + b$ for some $b \in \mathbb{F}_p^*$ and $p \equiv 1 \bmod 3$ [30, Proposition 4.33]. Consequently, there is an endomorphism $\tau : (x, y) \to (\alpha \cdot x, y)$ on E_1, where α 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 $\mathbb{G}_1$ (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 an endomorphism $\tau : (x, y) \to (-x, \beta \cdot y)$ on E_2, where β 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 [31], 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' [32], 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 $E'(\mathbb{F}_{p^e})$. 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 [32]. Furthermore, it also leads to a high dimensional GLV method on a large class of elliptic curves [33]. Fast implementation of this method on ordinary curves with j-invariant 0 was studied in [34].

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 [29, 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 subgroup secure if the relevant cofactors h_1, h_2 and h_T contain no prime factors smaller than r. In Table 1, we have collected several popular pairing-friendly curves that can be parameterized by polynomials $p(z)$, $r(z)$ and $t(z)$ given a seed z. Note that the CP6-P782 and BW6-P761 curves can be used in ZEXE [35] and Geppetto [36, 37] construction, respectively. The small factors of h_1, h_2 and h_T can be obtained using the `ECM()` function in Magma [38]. 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 have been unable to obtain a small factor of the cofactor h_T (c_{1336}) of BN-P446 limited by our computational power. But it is not recommended for skipping the $\mathbb{G}_T$ membership testing on the curve as the cofactor is composite.

Table 1 Subgroup security for a list of popular pairing-friendly curves. The symbol c_m denotes a composite number of size m bits.

family	$\log p$	$\log r$	seed z	h_1	h_2	h_T
CP6	782	377	$2^{63}+2^{58}+2^{56}+2^{51}+2^{47}+2^{46}+1$[35]	$c_{50}\cdot c_{357}$	$c_{192}\cdot c_{1778}$	$c_{77}\cdot c_{1111}$
BW6	761	377	$2^{63}+2^{58}+2^{56}+2^{51}+2^{47}+2^{46}+1$[39]	$c_{56}\cdot c_{328}$	$c_{97}\cdot c_{288}$	$c_{18}\cdot c_{1126}$
BN	446	446	$2^{110}+2^{36}+1$[40]	1	$13c_{610}$	c_{1336}
BLS12	461	308	$-2^{77}+2^{50}+2^{33}$[41]	c_{153}	$c_{25}\cdot c_{442}$	$c_{39}\cdot c_{1495}$
KSS16	330	257	$-2^{34}+2^{27}-2^{33}+2^{20}-2^{11}+1$[41]	c_{75}	$c_{93}\cdot c_{1052}$	$34\cdot c_{2379}$
KSS18	348	256	$2^{44}+2^{22}-2^{9}+2$[41]	c_{93}	$c_{78}\cdot c_{710}$	$c_{131}\cdot c_{1595}$
BW13	310	267	-2224[42]	c_{43}	$c_{83}\cdot c_{3368}$	$c_{126}\cdot c_{3368}$
BW19	286	259	-145[42]	c_{28}	$c_{50}\cdot c_{4861}$	$c_{41}\cdot c_{5101}$

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.* [42] found that the BW13-P310 and BW19-P286 curves may be suitable for several cryptographic schemes, such as Enhanced Privacy ID [43] and Direct Anonymous Attestation [44]. 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

Scott [19] proposed an efficient method for $\mathbb{G}_2$ membership testing on a curve E admitting a twist E' over $\mathbb{F}_{p^e}$. The main idea can be summarized as follows:

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

under the condition that $\gcd(h_1, h_2) = 1$. The computational cost of this method largely comes from the scalar multiplication by $t-1$. When checking a candidate element using the above technique, one 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 of $Q \in \mathbb{G}_2$. Therefore, the technique proposed in [32] can not be applied as it only works for elements in $\mathbb{G}_2$.

In this subsection, we propose a more general method that requires around $\log r/\varphi(k)$ bit operations on many pairing-friendly curves. In addition, it does not rely on the condition that $\gcd(h_1, h_2) = 1$ and thus has a wide applicability. To illustrate it, we first recall the modular lattice defined in [32, Section 3]:

$$\mathcal{L}_\psi = \{(\alpha_0, \alpha_1, \cdots, \alpha_{\varphi(k)-1}) \in \mathbb{Z}^{\varphi(k)} \mid \sum_{i=0}^{\varphi(k)-1} \alpha_i \cdot p^i \equiv 0 \bmod r\}.$$

A basis of $\mathcal{L}_\psi$ is given by

$$\{(r, 0, \cdots, 0), (-p, 1, 0, \cdots, 0), (-p^2, 0, 1, 0 \cdots, 0), \cdots, (-p^{\varphi(k)-1}, 0, \cdots, 0, 1)\}.$$

For a given vector $(c_0, c_1, \cdots, c_{\varphi(k)-1}) \in \mathcal{L}_\psi$ and a random point $R \in \mathbb{G}_2$, it is obvious that

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

Furthermore, let $Q \in E'(\mathbb{F}_{p^e})$ be a point whose order is unknown satisfying that

$$\sum_{i=0}^{\varphi(k)-1} [c_i]\psi^i(Q) = \mathcal{O}_{E'}. \tag{5}$$

It is natural to ask whether the order of Q can be determined by Eq. (5). In the following, we will show that Eq. (5) actually gives a multiple of the order Q. Since the point Q also satisfies Eq. (2), it is equivalent to express Eq. (5) as

$$(b_0 + b_1\psi)(Q) = \mathcal{O}_{E'}. \tag{6}$$

where b_0 and b_1 are given by

$$b_0 + b_1\psi = \sum\nolimits_{i=0}^{\varphi(k)-1} c_i\psi^i \bmod (\psi^2 - t\psi + p). \tag{7}$$

Denote $\hat{\psi}$ as the dual of ψ. Then, the dual of $b_0 + b_1\psi$ is $b_0 + b_1\hat{\psi}$ and thus we have

$$\begin{aligned}(b_0 + b_1\hat{\psi})(b_0 + b_1\psi) &= b_0^2 + b_0 \cdot b_1 \cdot (\psi + \hat{\psi}) + b_1^2(\psi\hat{\psi})\\ &= b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p.\end{aligned}$$

Thus, acting the endomorphism $b_0 + b_1\hat{\psi}$ on the both sides of Eq. (6), we get

$$[b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p]Q = \mathcal{O}_{E'}.$$

Putting it all together, one can obtain a multiple of the order Q from Eq. (5). On the other hand, since $Q \in E'(\mathbb{F}_{p^e})$, we conclude that the order of Q divides $\gcd(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, h_2 \cdot r)$. Inspired by the above observation, we give the following theorem.

Theorem 1 *Let E be an ordinary elliptic curve over $\mathbb{F}_p$ and r a large prime such that $r \parallel \#E(\mathbb{F}_p)$. Denote by t the trace of the Frobenius endomorphism π. Let E' be a twist of E over $\mathbb{F}_{p^e}$ such that $r \parallel \#E'(\mathbb{F}_{p^e})$. Let $(c_0, c_1, \cdots, c_{\varphi(k)-1})$ be a vector in $\mathcal{L}_\psi$, and b_0, b_1 the corresponding parameters given by Eq. (7). Assume that*

$$\gcd\left(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, h_2 \cdot r\right) = r. \tag{8}$$

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

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

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

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

Conversely, it follows from Eq. (2) that

$$\psi^2(Q) - [t]\psi(Q) + [p]Q = \mathcal{O}_{E'}. \tag{9}$$

If $\sum_{i=0}^{\varphi(k)-1}[c_i]\psi^i(Q)=\mathcal{O}_{E'}$, Eqs. (7) and (9) imply that

$$[b_1]\psi(Q)=-[b_0]Q. \tag{10}$$

Together with Eqs. (9) and (10), it yields that

$$\begin{aligned}&[b_0^2+b_0\cdot b_1\cdot t+b_1^2\cdot p]Q\\ =&[b_1^2]\psi^2(Q)-[b_1^2\cdot t]\psi(Q)+[b_1^2\cdot p]Q\\ =&\mathcal{O}_{E'}.\end{aligned} \tag{11}$$

Furthermore, since $Q\in E'(\mathbb{F}_{p^e})$, we have the order of Q divides gcd $\left(b_0^2+b_0\cdot b_1\cdot t+b_1^2\cdot p, h_2\cdot r\right)$. By Eq. (8), we conclude that $Q\in\mathbb{G}_2$, which completes the proof of the theorem. □

Remark 1 From the proof of Theorem 1, it is interesting to observe that

$$\begin{aligned}&b_0^2+b_0\cdot b_1\cdot t+b_1^2\cdot p\\ =&b_1^2\left((-b_0/b_1)^2-t(-b_0/b_1)+p\right)\\ =&\mathrm{Res}(b_0+b_1\psi,\psi^2-t\psi+p)\\ =&\mathrm{Res}\left(\sum_{i=0}^{\varphi(k)-1}c_i\psi^i,\psi^2-t\psi+p\right),\end{aligned}$$

where $\mathrm{Res}(f,g)$ represents the resultant of two polynomials f and g.

Define $h_2'=(b_0^2+b_0\cdot b_1\cdot t+b_1^2\cdot p)/r$. It can be seen from Eq. (7) that $b_0+b_1\cdot p\equiv 0 \bmod r$, which implies that

$$\begin{aligned}h_2'\cdot r&\equiv(b_0^2+b_0\cdot b_1\cdot t+b_1^2\cdot p)\\ &\equiv(b_0+b_1)(b_0+b_1\cdot p)\\ &\equiv 0 \bmod r.\end{aligned}$$

Thus $h_2'\in\mathbb{Z}$ and Eq. (8) is equivalent to $\gcd(h_2,h_2')=1$. A question raised here is how to find out a short vector in $\mathcal{L}_\psi$ such that $\gcd(h_2,h_2')=1$. In fact, we can always select the target vector as $(r,0,\cdots,0)$, so $b_0=r$ and $b_1=0$, meaning $h_2'=r$. Since $\mathbb{G}_2$ is the unique subgroup of $E'(\mathbb{F}_{p^e})$ with order r, the condition $\gcd(h_2,h_2')=1$ clearly holds. Indeed, this vector actually corresponds to the naive method, which is inefficient in practical applications.

In Algorithm 1, we present a Magma code for finding out a short vector for $\mathbb{G}_2$ membership testing. It proceeds as follows. Lines 1-7 construct the target lattice; Lines 8-17 check whether there is such a shortest vector (for Euclidean norm) meeting the condition that $\gcd(h_2,h_2')=1$. If so, then Algorithm 1 returns this vector; otherwise, Lines 18-27 enumerate short vectors in a process V until a target one is found or the process has been completed with returning "NULL". The latter case indicates there exists no valid short vector in V.

We emphasize that one must set an appropriate range of norm in the `ShortVectorsProcess()` function such that the output of Algorithm 1 is not "NULL". Since we expect that the target short vector is "closed" to the shortest ones, it is reasonable to set the lower bound as the norm of shortest vectors.

However, there is no standard for the selection of the upper bound. In our setting the value is selected as a small multiple v of the norm of shortest vectors. The specific values of v on different pairing-friendly curves are presented in Table 2.

Algorithm 1 Finding out a short vector for $\mathbb{G}_2$ membership testing

Input: The characteristic p, the trace t, the prime r, the embedding degree k, the cofactor h_2 and the small multiple v

Output: a short vector C or NULL

```
u:=EulerPhi(k);
B:=RMatrixSpace(Integers(), u,u)!0;
B[1][1]:=r;
for i:=2 to u do
    B[i][1]:=-p^(i-1);B[i][i]:=1;
end for;
L:=LatticeWithBasis(B);
S:=ShortestVectors(L);
R<x>:=PolynomialRing(Integers());
for i:=1 to #S do
    C:=S[i];
    b:=R!Eltseq(C);
    h2d:=Resultant(b, x^2-t*x+p) div r;
        if GCD(h2,h2d) eq 1 then
           return C;
        end if;
end for;
min:=Norm(ShortestVector(L));max:=v*min;
V:=ShortVectorsProcess(L, min, max);
repeat
        C:=NextVector(V);
        if Norm(C) eq 0 then
           return "NULL";
        end if;
        b:= R!Eltseq(C);
        h2d:=Resultant(b, x^2-t*x+p) div r;
until GCD(h2,h2d) eq 1;
return C;
```

3.1.1 Comparison

We now reinterpret the previous method using Theorem 1. Since $r \mid (p + 1 - t)$, the vector $(t-1, -1, 0, \cdots, 0) \in \mathcal{L}_\psi$. In fact, the previous method can be regarded as always selecting the short vector as $(t-1, -1, 0, \cdots, 0)$.

Table 2 The short vectors of $\mathbb{G}_2$ membership testing on a list of pairing-friendly curves admitting a twist. On KSS16-P330, the value u is equal to $(-z-25)/70$. On BW6-P761, the previous method is not recommended as the bit length of t is larger than that of r.

Curve	v	gcd(h_1,h_2)	Short vector (The previous method [19])	Short vector (This method)
BW6-P761	1	1	–	$\left(\frac{z-1}{3}(z^2-2)+z, \frac{z-1}{3}(z^2-2)-1\right)$
CP6-P782	3	4	–	$\left(\frac{2z-2}{3}(z^2-2)+z-1, \frac{1-z}{3}(z^2-2)+1\right)$
BN-P446	1	1	$(6z^2, -1, 0, 0)$	$(z+1, z, z, -2z)$
BLS12-P461	1	1	$(z, -1, 0, 0)$	$(z, -1, 0, 0)$
KSS16-P330	2	4	–	$(11u+4, -9u-3, 3u+1, 3u+1,$ $-13u-5, 7u+3, u, 11u+4)$
KSS18-P348	1	1	$\left(\frac{z^4+16z}{7}, -1, 0, 0, 0, 0\right)$	$\left(\frac{2z}{7}, 1, 0, \frac{z}{7}, 0, 0\right)$

For this vector, the corresponding parameters of b_0 and b_1 are $t-1$ and -1 respectively, so

$$\gcd(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, h_2 \cdot r) = r \Leftrightarrow \gcd(h_1, h_2) = 1.$$

Therefore, our method can be seen as an extension and generalization of the previous one proposed by Scott. In https://github.com/eccdaiy39/smt-magma/tree/main/vector, we provide the source code to look for target short vectors on different pairing-friendly curves. The related data is summarized in Table 2. For BW6-P761, BN-P446, BLS12-P461 and KSS18-P348, the given vectors are exactly the shortest vector in $\mathcal{L}_\psi$. In fact, the shortest vectors on BN-P446 and KSS18-P348 were recommended in [45, Section IV] to construct optimal ate pairings. For CP6-P782 and KSS16-P330, there exists no shortest vector meeting the condition (8). Fortunately, we find out valid short vectors that are very "closed" to the shortest ones on the two curves. By the property of shortest vectors [45, Theorem 2], $\mathbb{G}_2$ membership testing requires around $\log r/\varphi(k)$ bit operations on these curves. In Table 2, we also list the short vectors of the previous method on these curves. It is clear that our method is in effect identical to the previous one on BLS12-P446, and more efficient than the previous one on BN-P446 and KSS18-P348.

3.1.2 Examples

In the following, we present two examples to illustrate the main mechanics of the new method in detail. The first one is to show that the performance benefits resulting from the new method. The second one aims to explain that the new method is also suitable for curves with $\gcd(h_1, h_2) \neq 1$.

Example 1 The BN family is parameterized by

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

In this family, one of shortest vectors in $\mathcal{L}_\psi$ is given by $(z+1, z, z, -2z)$. In the following, we prove that this vector can be used for the $\mathbb{G}_2$ membership testing on all curves in the family with $z \not\equiv 5422 \bmod 21961$. Firstly, according to the form of the target vector and [9, Proposition 1] the parameters h_2' and h_2 can be expressed as polynomials

$$\begin{aligned} h_2'(z) =& 5184z^{10} + 10368z^9 + 12528z^8 + 9072z^7 + 4716z^6 + 1620z^5 + 444z^4 + \\ & 102z^3 + 18z^2 + 1, \\ h_2(z) =& 36z^4 + 36z^3 + 30z^2 + 6z + 1. \end{aligned}$$

Computing $\gcd\big(h_2(z), h_2'(z)\big)$ by the XGCD() function in Magma reveals that

$$A \cdot h_2(z) + A' \cdot h_2'(z) = B, \tag{12}$$

where

$$\begin{aligned} A =& -4662144z^9 - 13696128z^8 - 18896544z^7 - 16628256z^6 - 9402216z^5 \\ & - 3696120z^4 - 910224z^3 - 206418z^2 - 38102z - 1917, \\ A' =& 32376z^3 + 62736z^2 + 49604z + 23878, \\ B =& 21961. \end{aligned}$$

Since the parameter B is prime, Eq.(12) indicates that $\gcd(h_2(z_0), h_2'(z_0))$ is equal to 1 or B for any given seed z_0. Then we have

$$\gcd(h_2(z_0), h_2'(z_0)) = B \Leftrightarrow \gcd(h_2(z_0), h_2'(z_0)) \equiv 0 \bmod B. \tag{13}$$

Since $\gcd(h_2(z), h_2'(z)) = z - 5422$ over $\mathbb{F}_B$, it follows that $z_0 \equiv 5422 \bmod B$. In conclusion,

$$\gcd(h_2, h_2') = 1 \Leftrightarrow z \not\equiv 5422 \bmod 21961. \tag{14}$$

The right side of (14) actually holds for many popular curves in the BN family, such as

$$\begin{aligned} &(1)\text{BN-P254} : z = -(2^{62} + 2^{55} + 1), \\ &(2)\text{BN-P382} : z = -(2^{94} + 2^{78} + 2^{67} + 2^{64} + 2^{48} + 1), \\ &(3)\text{BN-P446} : z = 2^{110} + 2^{36} + 1. \end{aligned}$$

Now we consider the procedure of $\mathbb{G}_2$ membership testing on these curves. 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

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

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

The previous leading work of the $\mathbb{G}_2$ membership testing in the BN family was proposed in [13], which requires approximately one scalar multiplication by $6z^2$. Clearly, our method is more efficient than the previous one.

Remark 2 For the $\mathbb{G}_2$ membership testing in the BN family, there also exist the following two candidate short vectors:

$$V_1 = (2z, z+1, -z, z),\ V_2 = (6z+2, 1, -1, 1).$$

Following the same technique as described in Example 1, we find that the vector V_1 requires $z \not\equiv 564 \bmod 3061$, and V_2 requires $z \not\equiv 4 \bmod 13$ and $z \not\equiv 92 \bmod 97$. In particular, the vector V_2 is recommended for the construction of Miller iteration, which allows to perform $\mathbb{G}_2$ membership testing during pairing computation in some certain protocols.

Example 2 The KSS16 family is parameterized by

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

With parameters as above and from [25, Proposition 2], the cofactors h_1 and h_2 are expressed as polynomials
$h_1(z) = 125/2z^2 + 125z + 625/2$,
$h_2(z) = (z^{32} + 8z^{31} + 44z^{30} + 152z^{29} + 550z^{28} + 2136z^{27} + 8780z^{26} + 28936z^{25} + 83108z^{24} + 236072z^{23} + 754020z^{22} + 2287480z^{21} + 5986066z^{20} + 14139064z^{19} + 35932740z^{18} + 97017000z^{17} + 237924870z^{16} + 498534968z^{15} + 1023955620z^{14} + 2353482920z^{13} + 5383092978z^{12} + 10357467880z^{11} + 17391227652z^{10} + 31819075896z^{9} + 65442538660z^{8} + 117077934360z^{7} + 162104974700z^{6} + 208762740168z^{5} + 338870825094z^{4} + 552745197960z^{3} + 632358687500z^{2} + 414961135000z + 126854087873)/15059072$.
Since the parameterization of the KSS16 family requires $z \equiv \pm 25 \mod 70$, it is easy to check that $\gcd(h_1, h_2)$ always has a factor of 2. For this reason, the previous fastest method for the $\mathbb{G}_2$ membership does not work on all curves in this family. We now investigate how to perform the $\mathbb{G}_2$ membership testing using the new method on KSS16-P330. Using Algorithm 1, we obtain a short vector $(c_0, c_1, \cdots, c_7)$ as

$$(11u+4, -9u-3, 3u+1, 3u+1, -13u-5, 7u+3, u, 11u+4)$$

where $u = (-z-25)/70$. By Theorem 1, a candidate point Q is a member of $\mathbb{G}_2$ if and only if

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

To compute $[c_i]Q$ for $i = 0, 1, \cdots, 7$, the following sequence is performed:

$$\begin{aligned} &[u]Q \to [u+1]Q \to [2u+1]Q \to [3u+1]Q \to [6u+2]Q \to [7u+3]Q \to \\ &[-9u-3]Q \to [11u+4]Q \to [-13u-5]Q. \end{aligned} \tag{15}$$

The cost of computing (15) is one multiplication by u, seven point additions and one point doubling. On this basis, the points $\sum_{i=0}^{6} \psi^i([c_i]Q)$ and $-\psi([c_7]Q)$ can be computed at a cost of six point additions and seven applications of the endomorphism ψ.

Neglecting the cost of checking $Q \in E'(\mathbb{F}_{p^4})$, our method requires one multiplication by u, thirteen point additions, one point doubling and seven applications of the endomorphism ψ. The most costly part is the scalar multiplication by u, which is roughly $\log r/\varphi(k)$ bits.

Remark 3 In Example 2, we do not give a general result of the $\mathbb{G}_2$ membership testing in the KSS16 family with seed $z \equiv -25 \bmod 70$. For the selected vector, it is easy to find two polynomials $A, A' \in \mathbb{Z}[z]$ and an integer B such that $A \cdot h_2(z) + A' h_2'(z) = B$. Unfortunately, the parameter B is too large and thus we have been unable to find out all "bad" seeds in $[0, B-1]$ such that $\gcd(h_2, h_2') \neq 1$.

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

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

where $\mathcal{G}_2 = \mathrm{Ker}\big(\Phi_k(\pi)\big)$. 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. Let r be a large prime such that $r \parallel \#E(\mathbb{F}_p)$, t the trace of the Frobenius endomorphism π, and k the embedding degree of E with respect to r. Let $(c_0, c_1, \cdots, c_{\varphi(k)-1}) \in \mathcal{L}_\psi$, and b_0 and b_1 be integers such that

$$b_0 + b_1\pi = \sum\nolimits_{i=0}^{\varphi(k)-1} c_i \pi^i \bmod (\pi^2 - t\pi + p). \tag{16}$$

Assume that

$$\gcd(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, h_2 \cdot r) = r. \tag{17}$$

Given a non-identity point Q of $E(\mathbb{F}_{p^k})$, then $Q \in \mathbb{G}_2$ if and only if $\sum\limits_{i=0}^{\varphi(k)-1} [c_i]\pi^i(Q) = \mathcal{O}_E$ and $Q \in \mathcal{G}_2$.

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

$$\pi^2(Q) - [t]\pi(Q) + [p]Q = \mathcal{O}_E. \tag{18}$$

Similar to the proof in Theorem 1, the condition $\sum_{i=0}^{\varphi(k)-1} [c_i]\pi^i(Q) = \mathcal{O}_E$ and Eq. (18) 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.(17) 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 for the $\mathbb{G}_2$ membership testing on pairing-friendly curves with the lack of twists. Likewise, this method requires around $\log r/\varphi(k)$ bit operations.

Let E be an ordinary curve over $\mathbb{F}_p$ with j-invariant 0 or 1728. Recall from Section 2.2 that there exists a GLV endomorphism τ acting as multiplication by an integer λ on $\mathbb{G}_2$. 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 $\gcd(k, 6) = 1$ [29, Section 1], meaning $\gcd(k, d) = 1$. For any $R \in \mathbb{G}_2$ and positive integer i, it is clear that

$$\pi^i(R) = [(t-1)^i]R \in \mathbb{G}_2, \quad \tau(R) = [\lambda]R \in \mathbb{G}_2.$$

Since $\mathbb{G}_2$ is cyclic, there exists an integer b such that

$$\pi^i(R) = [b]\tau(R).$$

Furthermore, let $Q \in E(\mathbb{F}_{p^k})$ be a point whose order is unknown satisfying that

$$\pi^i(Q) = [b]\tau(Q). \tag{19}$$

Similar to the case of pairing-friendly curves admitting a twist, we expect to obtain a multiple of the order Q from Eq. (19) by taking full advantage of the properties of π and τ. Following this idea, we propose a new method to further reduce the computational cost of $\mathbb{G}_2$ membership testing on this class of curves 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 endomorphism π, 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 on $\mathbb{G}_2$. 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*

$$\gcd(b^{2d \cdot m} - t \cdot b^{d \cdot m} + p, h_2 \cdot r) = r, \tag{20}$$

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 discussion. Under the assumption that $\gcd(k, i) = 1$, we have $\gcd(d \cdot i, k) = 1$ 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, from $\tau(Q) = [\lambda]Q$ 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

$$\pi(Q) = \pi^{1+n\cdot k}(Q) = \pi^{d\cdot m\cdot i}(Q) = [b^{d\cdot m}]Q. \tag{21}$$

Furthermore, it follows from Eq. (1) that

$$\pi^2(Q) - [t]\pi(Q) + [p]Q = \mathcal{O}_E. \tag{22}$$

Combining Eqs. (21) and (22), it yields that

$$[b^{2d\cdot m} - t \cdot b^{d\cdot m} + p]Q = \mathcal{O}_E. \tag{23}$$

On the other hand, since $Q \in \mathcal{G}_2$, Eq. (23) indicates that the order of Q divides $\gcd\left(b^{2d\cdot m} - t\cdot b^{d\cdot m} + p, h_2 \cdot r\right)$. From Eq. (20), we conclude that $Q \in E[r] \cap \mathcal{G}_2 = \mathbb{G}_2$, which completes the proof. □

Let E be an ordinary curve over $\mathbb{F}_p$ with j-invariant 0 or 1728. Recall from Section 2.2 that there exists a GLV endomorphism τ acting as multiplication by an integer λ on $\mathbb{G}_2$. 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 (20). We fortunately find that Theorem 2 induces a fast method for $\mathbb{G}_2$ membership testing on BW13-P310 and BW19-P286.

In Table 3, we list important parameters of $\mathbb{G}_2$ membership testing on BW13-P310 and BW19-P286. By Theorem 2, the computational cost of the testing on the two curves is dominated by the multiplication by b. Since $\deg\left(r(z)\right) = 2\varphi(k)$, it is interesting to see that $\log|b| = \log|z| \approx \log r/\left(2\varphi(k)\right)$.

Table 3 Parameters of $\mathbb{G}_2$ membership testing on BW13-P310 and BW19-P286.

Curve	i	m	b
BW13-P310	1	9	$-z$
BW19-P286	1	13	$-z$

3.2.1 Example

In the following example, we show how to perform the $\mathbb{G}_2$ membership testing on BW13-P310.

Example 3 From Construction 6.6 in [46], 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 $z = -2224$ [40]. 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 $\gcd\big(b^{6\cdot m} - t\cdot b^{3\cdot m} + p, h_2 \cdot r\big) = r$, where $h_2 = \#E(\mathbb{F}_{p^{13}})/(r \cdot \#E(\mathbb{F}_p))$. By Theorem 2, the $\mathbb{G}_2$ membership testing requires to check that

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

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

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

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

Neglecting the cost of checking $Q \in E(\mathbb{F}_{p^{13}})$, our method requires one scalar multiplication by z, four point additions, five applications of the endomorphism π and one application of the endomorphism τ.

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

Let E be an ordinary curve with j-invariant 0 or 1728. Recall from Section 2.1 that a GLV endomorphism τ corresponds to a scalar multiplication by λ on $\mathbb{G}_1$, where

$$\begin{cases} \lambda^2 + \lambda + 1 \equiv 0 \bmod r, \text{if } j(E) = 0; \\ \lambda^2 + 1 \equiv 0 \bmod r, \text{if } j(E) = 1728. \end{cases} \tag{24}$$

If E is a curve in the BLS12 family, Scott [19] proved that

$$P \in \mathbb{G}_1 = E(\mathbb{F}_p)[r] \Leftrightarrow P \in E(\mathbb{F}_p) \text{ and } \tau(P) = [\lambda]P. \tag{25}$$

This observation induces a fast method for the $\mathbb{G}_1$ membership testing in the BLS12 family, whose computational cost comes mostly from the multiplication by λ. Define h_λ as

$$h_\lambda = \begin{cases} (\lambda^2 + \lambda + 1)/r, \text{if } j(E) = 0; \\ (\lambda^2 + 1)/r, \text{if } j(E) = 1728. \end{cases} \tag{26}$$

Recently, Housni *et al*. [13, Proposition 2] summarized that this method is actually suitable for all curves satisfying that $\gcd(h_1, h_\lambda) = 1$.

Inspired by this method, we propose a general one that can be used in many popular pairing-friendly curves with $\gcd(h_1, h_\lambda) \neq 1$. To illustrate it clearly, we start by defining the GLV lattice as

$$L_\tau = \{(a_0, a_1) \in \mathbb{Z}^2 | a_0 + a_1 \cdot \lambda \equiv 0 \bmod r\}.$$

Then a general method for $\mathbb{G}_1$ membership testing is derived from the following theorem.

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 $r \parallel \#E(F_p)$. Let τ be a* GLV *endomorphism on E, and act as multiplication by an integer λ on $\mathbb{G}_1$. Let $(a_0, a_1) \in \mathcal{L}_\tau$ such that*

$$\begin{cases} \gcd\left(a_0^2 - a_0 \cdot a_1 + a_1^2, h_1 \cdot r\right) = r, \text{if } j(E) = 0; \\ \gcd\left(a_0^2 + a_1^2, h_1 \cdot r\right) = r, \text{if } j(E) = 1728. \end{cases} \tag{27}$$

Given a non-identity point $P \in E(\mathbb{F}_p)$, then $P \in \mathbb{G}_1$ 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

$$[a_1^2]\tau^2(P) + [a_1^2]\tau(P) + [a_1^2]P = \mathcal{O}_E. \tag{28}$$

By the conditions $P \in E(\mathbb{F}_p)$ and $[a_0]P + [a_1]\tau(P) = \mathcal{O}_E$, we obtain from Eq. (28) that

$$\begin{aligned} &[a_0^2 - a_0 \cdot a_1 + a_1^2]P = \mathcal{O}_E, \\ &[h_1 \cdot r]P = \mathcal{O}_E. \end{aligned}$$

Since $\gcd\left(a_0^2 - a_0 \cdot a_1 + a_1^2, h_1 \cdot r\right) = r$, we conclude that $P \in \mathbb{G}_1$, which completes the proof of the theorem. □

In Algorithm 2, we describe how to find out a short vector for $\mathbb{G}_1$ membership testing in Magma code. Table 4 presents the specific values of v on different pairing-friendly curves such that this function outputs valid short vectors.

4.1.1 Comparison

In Table 4, we also collect the values of $\gcd(h_1, h_\lambda)$ and the short vectors output by Algorithm 2 on different pairing-friendly curves. Since the previous method works under the condition that $\gcd(h_1, h_\lambda) = 1$, it not suitable for KSS16-P330, KSS18-P348, BW13-P310 and BW19-P286. As a comparison, our method do not rely on this condition. In fact, the previous method is equivalent to the proposed one by fixing the short vector (a_0, a_1) as $(\lambda, -1)$. Thus, we

Algorithm 2 Finding out a short vector for $\mathbb{G}_1$ membership testing

Input: The prime r, the scalar λ (lambda), the cofactor h_1, the small multiple v and the CM discriminant D ($D = -3$ if $j(E) = 0$, and $D = -4$ if $j(E) = 1728$)

Output: a short vector C or NULL

```
B:=RMatrixSpace(Integers(), 2,2)![r,0,-lambda,1];
L:=LatticeWithBasis(B);
S:=ShortestVectors(L);
for i:=1 to #S do
    C:=S[i];
    gcd:=GCD(C[1]^2-(D mod 2)*C[1]*C[2]+C[2]^2, h1*r);
    if gcd eq r then
       return C;
    end if;
end for;
min:=Norm(ShortestVector(L));max:=v*min;
V:=ShortVectorsProcess(L, min, max);
repeat
      C:=NextVector(V);
         if Norm(C) eq 0 then
            return "NULL";
     end if;
until GCD(C[1]^2-(D mod 2)*C[1]*C[2]+C[2]^2,h1*r) eq r;
return C;
```

Table 4 The short vectors for $\mathbb{G}_1$ membership testing on a list of pairing-friendly curves with j-invariant 0 or 1728.

Curve	v	λ	$\gcd(h_1, h_\lambda)$	(a_0, a_1)
BW6-P761	1	$z^5-3z^4+3z^3-z+1$	1	$\left(\frac{z-1}{3}(z^2-2)-1, \frac{1-z}{3}(z^2-2)-z\right)$
BLS12-P461	1	z^2	1	$(z^2, 1)$
KSS16-P330	1	$-\frac{(z^4+24)}{7}$	1250	$\left(\frac{31z^4+625}{8750}, \frac{-17z^4-625}{8750}\right)$
KSS18-P348	1	z^3+18	343	$\left((\frac{z}{7})^3, -18a_0-1\right)$
BW13-P310	1	$-z^{13}$	z^2-z+1	$\left(-(z^7+z)(z^4+z^3-z-1), a_0 \cdot z-1\right)$
BW19-P286	1	$-z^{19}$	z^2-z+1	$\left((z-z^{10})(z^6-z^3+1)(z+1), a_0 \cdot z-1\right)$

have generalized the previous method such that it can be applied into pairing-friendly curves with $\gcd(h_1, h_\lambda) \neq 1$. Analogous to $\mathbb{G}_2$ membership testing, there always exists a short vector $(a_0, a_1) \in \mathcal{L}_\tau$ meeting the condition (27). As we have seen in Table 4, the selected short vectors guarantee that $\mathbb{G}_1$ membership testing requires approximately $\log r/2$ bit operations.

Remark 4 The selected short vectors (a_0, a_1) listed in Table 4 satisfy that

$$\begin{cases} a_0^2 - a_0 \cdot a_1 + a_1^2 = r, \text{if } j(E) = 0; \\ a_0^2 + a_1^2 = r, \text{if } j(E) = 1728. \end{cases}$$

By Theorem 3, the recommended short vectors are actually independent with the selection of seeds.

4.1.2 Example

We now take the KSS16 family as an example to give a detailed description for $\mathbb{G}_1$ membership testing.

Example 4 Recall that the prime r in the KSS16 family is expressed as

$$r(z) = \frac{z^8 + 48z^4 + 625}{61250} = \frac{(z^4 + 24)^2 + 7^2}{61250}.$$

Since $z \equiv \pm 25 \bmod 70$, we have $z^4 \equiv 25 \bmod 70$, meaning $(z^4 + 24)/7 \in \mathbb{Z}$. With parameters as above, it is straightforward to see that

$$\left((z^4 + 24)/7\right)^2 + 1 \equiv 0 \bmod r,$$

which implies that $\lambda = \pm(z^4 + 24)/7$. We select $\lambda = -(z^4 + 24)/7$, then one of shortest vectors in $\mathcal{L}_\tau$ is given by (a_0, a_1), where

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

It is easy to check that $a_0^2 + a_1^2 = r$, and subsequently deduce that

$$\gcd\left(a_0^2 + a_1^2, h_1 \cdot r\right) = r$$

for any given seed z. By Theorem 3, the short vector (a_0, a_1) can be used for $\mathbb{G}_1$ membership testing on all curves in the KSS16 family. Furthermore, we also find that $-17a_0 - 31a_1 = 1$. If $17 \nmid h_1$ (eg. KSS16-P330) it would be convenient to substitute a_0 and a_1 by $17a_0$ and $17a_1$, respectively. As a consequence, given a point Q that is claimed to be a member of $\mathbb{G}_1$, we have

$$\begin{aligned} [a_0]Q + \tau([a_1]Q) = \mathcal{O}_E &\Leftrightarrow [17a_0]Q + \tau([17a_1]Q) = \mathcal{O}_E \\ &\Leftrightarrow \tau([17a_1]Q) - [31a_1]Q = Q. \end{aligned}$$

Thus, the $\mathbb{G}_1$ membership testing can be accomplished by checking that

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

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

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

Neglecting the cost of checking $Q \in E(\mathbb{F}_p)$, our method requires 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, which is about $\log r/2$ bits.

4.2 The $\mathbb{G}_T$ case

The first efficient method for $\mathbb{G}_T$ membership testing was proposed by Scott [11]. Recently, Scott [19] concluded that this method is actually suitable for all pairing-friendly curves with $\gcd(h_1, h_T) = 1$, which is tailored to the BN and BLS families. In detail, given a random element $\alpha \in \mathbb{F}_{p^k}^*$, Scott proved that

$$\alpha \in \mathbb{G}_T \Leftrightarrow \alpha \in \mathbb{G}_{\Phi_k(p)} \text{ and } \alpha^{p+1} = \alpha^t$$

under the condition that $\gcd(h_1, h_T) = 1$. Since the Frobenius map can be computed efficiently, the computational cost of this method is dominated by the exponentiation by t. Moreover, in the case that the embedding degree k is divided by 6, once the candidate element α is proved to be a member of $\mathbb{G}_{\Phi_k(p)}$, the fixed exponentiation by t can be further optimized by the techniques of fast cyclotomic squaring [47, 48].

Inspired by the method for $\mathbb{G}_2$ membership testing on pairing-friendly curves admitting a twist, we propose a general and efficient method for $\mathbb{G}_T$ membership testing that can be used for many pairing-friendly curves.

Theorem 4 *Let* $(c_0, c_1, \cdots, c_{\varphi(k)-1})$ *be a vector in* $\mathcal{L}_\psi$ *and* $\eta = \sum_{i=0}^{\varphi(k)-1} c_i \cdot p^i$. *Assume that* $\gcd\big(\eta, \Phi_k(p)\big) = r$. *Given a non-identity element* $\alpha \in \mathbb{F}_{p^k}^*$*, then* $\alpha \in \mathbb{G}_T$ *if and only if*

$$\alpha^{\Phi_k(p)} = 1 \quad \text{and} \quad \prod_{i=0}^{\varphi(k)-1} \alpha^{c_i \cdot p^i} = 1.$$

Proof Since $r \mid \Phi_k(p)$ and $r \mid \eta$, the necessity is straightforward. Conversely, if $\alpha^{\Phi_k(p)} = 1$ and $\prod_{i=0}^{\varphi(k)-1} \alpha^{c_i \cdot p^i} = 1$, then the order of α divides $\gcd\big(\eta, \Phi_k(p)\big)$. Since $\gcd\big(\eta, \Phi_k(p)\big) = r$ and $\alpha \neq 1$, it is clear that the order of α is equal to r and thus $\alpha \in \mathbb{G}_T$, which completes the proof of the theorem. □

Theorem 4 proved that any vector $(c_0, c_1, \cdots, c_{\varphi(k)-1})$ in $\mathcal{L}_\psi$ can be used for $\mathbb{G}_T$ membership testing if and only if $\gcd(h_T, h'_T) = 1$, where the parameter h'_T is defined as

$$h'_T = \Big(\sum_{i=0}^{\varphi(k)-1} c_i \cdot p^i\Big)/r.$$

Magma code is presented in Algorithm 3 for finding out a short vector for $\mathbb{G}_T$ membership testing . The specific values of v on different pairing-friendly curves are presented in Table 5.

4.2.1 Comparison

Similar to $\mathbb{G}_2$ membership testing, the previous method for $\mathbb{G}_T$ membership testing can be viewed as fixing the short vector as $(t-1, -1, 0, \cdots, 0)$. In other words, we have extended the previous method by expanding the range of choice of short vectors in $\mathcal{L}_\psi$ under a mild condition. In Table 5, we also collect the short vectors of our method (output by Algorithm 3) and of the

Algorithm 3 Finding out a short vector for $\mathbb{G}_T$ membership testing

Input: The characteristic p, the prime r, the embedding degree k, the cofactor h_T and the small multiple v

Output: a short vector C or NULL

```
u:=EulerPhi(k);
B:=RMatrixSpace(Integers(), u,u)!0;
B[1][1]:=r;
for i:=2 to u do
    B[i][1]:=-p^(i-1);B[i][i]:=1;
end for;
L:=LatticeWithBasis(B);
S:=ShortestVectors(L);
for i:=1 to #S do
    C:=S[i];
    b:=0;
    for j:=1 to u do
        b:=(b+C[j]*p^(j-1));
    end for;
    htd:=b div r;
    if GCD(ht,htd) eq 1 then
       return C;
    end if;
end for;
min:=Norm(ShortestVector(L));max:=v*min;
V:=ShortVectorsProcess(L, min, max);
repeat
        C:=NextVector(V);
        if Norm(C) eq 0 then
           return "NULL";
        end if;
        b:=0;
        for j:=1 to u do
            b:=(b+C[j]*p^(j-1));
        end for;
        htd:=b div r;
until GCD(ht,htd) eq 1;
return C;
```

previous one on different pairing-friendly curves. It is clear that our method for $\mathbb{G}_T$ membership testing requires around $\log r/\varphi(k)$ bit operations on these curves. Moreover, by the comparison of the above two methods we have the following observations.

- The two methods provide the same short vector on BLS12-P461.

Table 5 The short vectors of $\mathbb{G}_T$ membership testing for a list of pairing-friendly curves. On KSS16-P330, the value u is equal to $(-z-25)/70$. On BW6-P761 and CP6-P782, the previous method is not recommended as the bit length of t is larger than that of r.

Curve	v	$\gcd(h_1, h_T)$	Short vector (The previous method [19])	Short vector (This method)
BW6-P761	1	1	–	$\big(\frac{z-1}{3}(z^2-2)+z, \frac{z-1}{3}(z^2-2)-1\big)$
CP6-P782	1	1	–	$\big(\frac{z-1}{3}(z^2-2)-1, \frac{z-1}{3}(z^2-2)+z\big)$
BN-P446	1	1	$\big(6z^2, -1, 0, 0\big)$	$\big(z+1, z, z, -2z\big)$
BLS12-P461	1	1	$\big(z, -1, 0, 0\big)$	$\big(z, -1, 0, 0\big)$
KSS16-P330	2	4	–	$\big(11u+4, -9u-3, 3u+1, 3u+1,$ $-13u-5, 7u+3, u, 11u+4\big)$
KSS18-P348	1	1	$\big(\frac{z^4+16z}{7}, -1, 0, 0, 0, 0\big)$	$\big(\frac{2z}{7}, 1, 0, \frac{z}{7}, 0, 0\big)$
BW13-P310	1	1	$\big(-z^{14}+z, -1, 0, \ldots, 0\big)$	$\big(z^2, -z, 1, 0, \ldots, 0\big)$
BW19-P286	1	1	$\big(-z^{20}+z, -1, 0, \ldots, 0\big)$	$\big(z^2, -z, 1, 0, \cdots, 0\big)$

- Our method provides more shorter vectors than the previous one on BN-P446, KSS18-P348, BW13-P310 and BW19-P286.

4.2.2 Example

We now take the BN family as an example to illustrate how to perform $\mathbb{G}_T$ membership testing in detail.

Example 5 In the BN family, the cofactor h_T is can be parameterized by a polynomial

$$\begin{aligned} h_T(z) =& 46656z^{12} + 139968z^{11} + 241056z^{10} + 272160z^9 + 225504z^8 + 138672z^7 \\ &+ 65448z^6 + 23112z^5 + 6264z^4 + 1188z^3 + 174z^2 + 6z + 1. \end{aligned}$$

As mentioned before, one of shortest vectors in $\mathcal{L}_\psi$ for the Euclidean norm is given by $(z+1, z, z, -2z)$. We now prove that this vector can be used for the $\mathbb{G}_T$ membership testing on all curves in the BN family. For the selected short vector, the parameter h'_T is expressed as a polynomial

$$\begin{aligned} h'_T(z) =& -2592z^9 - 5184z^8 - 6480z^7 - 4752z^6 - 2484z^5 - 756z^4 - 162z^3 - 6z^2 \\ &- 5z + 1. \end{aligned}$$

Using the XGCD() function in Magma, we find that there exist two polynomials $A, A' \in \mathbb{Z}[z]$ such that

$$A \cdot h_T(z) + A' \cdot h'_T(z) = 1.$$

Thus, we conclude that $\gcd(h_T, h'_T) = 1$ for any given seed z. Or equivalently, the short vector $(z+1, z, z, -2z)$ can be used for $\mathbb{G}_T$ membership testing on all curves in the BN family. By Theorem 4, a candidate element $\alpha \in \mathbb{G}_T$ if and only if

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

This testing totally requires one exponentiation by z, four field multiplications, one field squaring and five applications of the endomorphism π. For many popular members in the BN family, such as BN-P254, BN-P382 and BN-P446, the seed z has a low Hamming weight. Thus, it is efficient to perform the exponentiation by z using the compression technique proposed in [48].

It is clear that our method reduces the computational cost compared to the previous one [11], which require approximately one exponentiation by $6z^2$.

5 Efficiency Analysis and Implementation Results

In Table 6, we give the number of bit operations of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings for different pairing-friendly curves. It should be noted that CP6-P782 is not equipped with a GLV endomorphism. Therefore, the only viable approach for the $\mathbb{G}_1$ membership testing on this curve is to multiply a candidate element by r so far.

Table 6 The number of bit operations of $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ membership testings for different pairing-friendly curves.

Curve	$\lceil \log r/2 \rceil$	$\lceil \log r/\varphi(k) \rceil$	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_T$
BW6-P761	189	189	190	190	190
CP6-P782	189	189	377	190	190
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

Table 7 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

Magma implementation for subgroup membership testings on pairing-friendly curves listed in Table 6 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 perform poorly. In order to accurately evaluate the performance improvements that are gained from the proposed techniques, we also present high speed software implementation on the BN-P446 and BW13-P310 curves within the RELIC [23] 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 same library. In Table 7, we summarize the results of benchmarks on a 64-bit Intel Core i7-8550U@1.8GHz processor running Ubuntu 18.04.1 LTS with TurboBoost and hyper-threading features disabled. Timing results are obtained averaged over 10,000 executions. As shown in Table 7, on the BN-P446 curve the new algorithm for the $\mathbb{G}_2$ membership testing is about 105.1% faster than that from [13], while the $\mathbb{G}_T$ membership testing is about 87.3% faster than that from [11]. As far as we know, the problem of subgroup membership testings 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.

6 Conclusion and Future Work

The threat of small-subgroup attacks are non-negligible in pairing-based protocols. Subgroup membership testing is a useful countermeasure to defense such attacks. In this paper, we revisited this problem and described efficient methods for $\mathbb{G}_1$, $\mathbb{G}_2$ 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. As future work we could design new algorithms to find out short vectors for subgroup membership testings, which are independent of the selection of seeds.

Acknowledgment

We would like to thank Michael Scott for finding out all bad seeds in Example 1. We are also grateful for two anonymous referees to adjust the structure of the paper, illustrate Theorem 1 from the view of resultant and provide a simplified Magma code. This work is supported by Guangdong Major Project of Basic and Applied Basic Research(No. 2019B030302008) and the National Natural Science Foundation of China(No. 61972428).

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. In: Batina, L., Daemen, J. (eds.) Progress in Cryptology – AFRICACRYPT 2022, pp. 518–536. Springer, Cham (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] Kim, T., Kim, S., Cheon, J.H.: On the final exponentiation in Tate pairing computations. IEEE Transactions on Information Theory **59**(6), 4033–4041 (2013)

[17] 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)

[18] 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)

[19] 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

[20] 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)

[21] 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)

[22] 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)

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

[24] 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)

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

[26] 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)

[27] Galbraith, S.: Pairings. In: Blake, I.F., Seroussi, G., Smart, N.P. (eds.) Advances in Elliptic Curve Cryptography. London Mathematical Society Lecture Note Series, vol. 317, pp. 183–214. Cambridge University Press, Cambridge (2005). https://doi.org/10.1017/CBO9780511546570.011

[28] Galbraith, S.: Mathematics of Public Key Cryptography. Cambridge University Press, ??? (2018). version 2

[29] 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

[30] Washington, L.C.: Elliptic Curves. Number Theory and Cryptography, 2nd edn. CRC Press, ??? (2008). https://doi.org/10.1201/9781420071474

[31] 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)

[32] 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)

[33] 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)

[34] 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)

[35] Bowe, S., Chiesa, A., Green, M., Miers, I., Mishra, P., Wu, H.: Zexe: Enabling decentralized private computation. In: 2020 IEEE Symposium on Security and Privacy (SP), pp. 947–964 (2020)

[36] Costello, C., Fournet, C., Howell, J., Kohlweiss, M., Kreuter, B., Naehrig, M., Parno, B., Zahur, S.: Geppetto: Versatile verifiable computation. In: 2015 IEEE Symposium on Security and Privacy, pp. 253–270 (2015)

[37] Aranha, D.F., El Housni, Y., Guillevic, A.: A survey of elliptic curves for proof systems. Accepted by Designs, Codes and Cryptography (2022)

[38] 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)

[39] El Housni, Y., Guillevic, A.: Optimized and Secure Pairing-Friendly Elliptic Curves Suitable for One Layer Proof Composition. In: Krenn, S., Shulman, H., Vaudenay, S. (eds.) Cryptology and Network Security (2020)

[40] 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)

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

[42] 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)

[43] 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)

[44] 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)

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

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

[47] 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)

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