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

Yu Dai, Kaizhan Lin, Zijian Zhou and Chang-An Zhao*

Abstract

Pairing-based cryptographic protocols are typically vulnerable to small-subgroup attacks in the absence of protective measures. To thwart them, one of effective measures is to execute subgroup membership testings for the three r-order subgroups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$, which are generally considered expensive. Inspired by the method given by Scott, we revisit this issue and generalize the testing method in this paper. Our method can be applied to a large class of curves, including curves admitting a twist and without a twist. The resulting implementation shows that for many popular pairing-friendly curves, the proposed technique significantly improves the performance of membership testings for the above three subgroups as compared with the fastest previously known one. More precisely, for $\mathbb{G}_2$ testing on curves admitting a twist, the new technique is about 1.9, 5.1, and 3.6 times faster than the previous one on *BN-446*, *KSS16-P310* and *KSS18-P348*, respectively. For $\mathbb{G}_2$ testing on curves without a twist, there exists no efficient testing method for $\mathbb{G}_2$ in the literature until now. In this situation, the proposed method is about 17.3 and 20 times faster than the naive one on *BW13-P310* and *BW9-P286*, respectively.

Index Terms

Small-subgroup attacks, group membership testings, pairing-friendly curves.

I. Introduction

Past two decades have witnessed the development of pairings in the field of public key cryptography [1]–[3]. Recently, pairings also find their applications in succinct non-interactive argument of knowledge(SNARKs) [4]. In pairing-based cryptographic protocols, the two input

Y. Dai, K.Z Lin and C.-A, Zhao is with School of Mathematics, Sun Yat-sen University, Guangzhou 510275, P.R.China and with Guangdong Key Laboratory of Information Security, Guangzhou 510006, P.R. China.

Z.J. Zhou is with College of Liberal Arts and Sciences National University of Defense Technology, Changsha 410073, P.R.China.

∗ Corresponding author (E-mail: zhaochan3@mail.sysu.edu.cn)

subgroups $\mathbb{G}_1$, $\mathbb{G}_2$ and the output subgroup $\mathbb{G}_T$ have the same large prime order r. In particular, $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive subgroups on a certain elliptic curve E over an extension field $\mathbb{F}_{p^k}$, and $\mathbb{G}_T$ is a multiplicative subgroup in $\mathbb{F}_{p^k}$. The security of a cryptographic protocol mainly relies on the difficulty of solving discrete logarithm problems in the above three subgroups [5]–[7]. Moreover, since the running environment of the protocol is possibly untrustworthy, it is vulnerable to small-subgroup attacks [8]. In particular, on most of pairing-friendly curves, the subgroups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ are generally contained in larger groups with order $h_1 \cdot r$, $h_2 \cdot r$ and $h_T \cdot r$, respectively. A powerful attacker may forge the system parameters to offer a point of small order. Once implementors perform a scalar multiplication of the untested element by a secret key directly, the attacker has a chance to fully recover the information of the secret key. More details of the attacks on pairing-based cryptographic protocols are given in [9, Section 1]. Note that small-subgroup attacks can be also mounted on $\mathbb{G}_T$ as the scenario described in [10]. One of methods to prevent these attacks is to increase the size of curve parameters of such that h_2 and h_T contain no factors smaller than r [9]. However, since the cofactor h_1 is smaller than r on most of pairing-friendly curves, it is hard for $\mathbb{G}_1$ to be subgroup secure on many pairing-friendly curves. In order to completely eliminate the hidden dangers, until now clearing cofactors and subgroup membership testing are the two feasible approaches.

A. Clearing cofactors

The method of clearing cofactors is mainly used for $\mathbb{G}_1$ and $\mathbb{G}_2$. In particular, implementors multiply the candidate points by the corresponding cofactors to force them into the target subgroups. In the case of $\mathbb{G}_1$, this method is efficient when the cofactor h_1 is quite small, which is suitable for many popular pairing-friendly curves; in the case of $\mathbb{G}_2$, even though h_2 is larger than r, this method is still worth being considered since it is identical to the procedure of hashing to $\mathbb{G}_2$, which can be accelerated by the method proposed in [11], [12]. However, it may give rise to additional troubles. As pointed in [13], implementors must determine which points to execute "clearing cofactors" on. Moreover, the original point has been changed, which might lead to additional troubles for implementors [14].

B. Subgroup membership testing

The negative effects of clearing cofactors can be removed by using subgroup membership testing. In the case of $\mathbb{G}_1$ (resp. $\mathbb{G}_T$), the cofactor h_1 (resp. h_T) is typically not equal to 1 for

most of pairing-friendly curves. Therefore, the verifier needs to perform a multiplication(resp. an exponentiation) of the candidate element by r and compare the result against the corresponding identity element. Pairing-friendly curves can be roughly divided into two kinds: **curves admitting a twist** and **curves without a twist**. In the case of $\mathbb{G}_2$, the membership testing on the two types of curves are different. On pairing-friendly curves admitting a twist E' of degree d, the candidate point can be regarded as an element of $E'(\mathbb{F}_{p^e})$, where $e = k/d$. Therefore, it is sufficient to check that the candidate point is an r-order element in $E'(\mathbb{F}_{p^e})$. However, on pairing-friendly curves without a twist, the testing is relatively complicated and costly. Let Q be a point which is claimed to be a membership of $\mathbb{G}_2$ on a curve without a twist. The verifier needs to check that $Q \in E(\mathbb{F}_{p^k})$, $[r]Q = \mathcal{O}_E$ and $\pi(Q) = [p]Q$, where $\mathcal{O}_E$ denotes the identity point of E and π is the p-power Frobenius endomorphism.

C. Our contributions

Recently, several novel approaches of subgroup membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on the *BLS* families of curves are proposed by Scott [14], achieving the same effect as multiplication/exponentiation by r, but more efficient. Inspired by his work, we propose more general membership testing methods for the above three subgroups. To be precise, we summarize our contributions as follows.

- We present an efficient method of the membership testing for $\mathbb{G}_2$ on pairing-friendly curves admitting a twist. On many popular pairing-friendly curves, this method is faster than the previous leading work in the literature. In particular, on *BN-P446* and *KSS18-P348* [15], our method is about twice and four times faster than the one given by Scott [14], respectively. On *KSS16-P330* [15], the method given by Scott is not applicable anymore. In this situation, our method is about 5.1 times faster than the schoolbook method, which is the unique previously known one.
- To the best of our knowledge, we are the first to optimize the method of the membership testing for $\mathbb{G}_2$ on **curves without a twist**. On some certain curves, such as *BW13-P310* and *BW19-P286* given in [16], the overhead of our method mainly requires a scalar multiplication by a cofactor in approximately $\log r/\big(2\varphi(k)\big)$ bits, which is significantly faster than the schoolbook method. More specially, experimental results show that our method is about 17.3 and 20 times faster than the schoolbook method on *BW13-P310* and *BW19-P286*, respectively.

- We also propose fast testing methods for $\mathbb{G}_1$ and $\mathbb{G}_T$, respectively. These methods are about twice and $\varphi(k)$ times faster than the multiplication/exponentiation by r for $\mathbb{G}_1$ and $\mathbb{G}_T$, respectively.

Outlines of this paper. The remainder of this paper is organized as follows. Section II provides a brief necessary background on pairing subgroups, schoolbook method of subgroup membership testing, endomorphisms of elliptic curves and small-subgroup attacks on pairing-friendly curves. Sections III and IV describe efficient membership testing methods for $\mathbb{G}_2$, and $\mathbb{G}_1$ and $\mathbb{G}_T$, respectively. Two examples of applications of our methods are given in Section V. In Section VI, we present efficiency comparisons between our methods and the previous work in the literature. The conclusion is given in Section VII.

II. Background

A. Pairing subgroups

Let E be an elliptic curve defined over $\mathbb{F}_p$ where p is prime. Denote by $\mathcal{O}_E$ the identity point of E. Let r be a large prime factor of $\#E(\mathbb{F}_p)$ and $r^2 \nmid \#E(F_p)$. The embedding degree k of E with respect to r is the smallest positive integer such that $r|\Phi_k(p)$, where Φ_k is the k-th cyclotomic polynomial. Whenever $k > 1$, the r-torsion group $E[r]$ is contained in $E(\mathbb{F}_{p^k})$. Let $\pi : (x, y) \to (x^p, y^p)$ be the p-power Frobenius endomorphism. The characteristic equation of π is

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

where the Frobenius trace t satisfies that $t = p + 1 - \#E(\mathbb{F}_p)$. Let $\mathbb{G}_T \subseteq \mathbb{F}_{p^k}^*$ be the subgroup of r-th roots of unity. A pairing is a bilinear and non-degenerate map:

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T,$$

where $\mathbb{G}_1 = E[r] \cap Ker(\pi - [1])$ and $\mathbb{G}_2 = E[r] \cap Ker(\pi - [p])$. Denote by d the order of the automorphism group of E. If $d|k$, then E admits a degree-d twist E' over $\mathbb{F}_{p^e}$ where $e = k/d$. Write ϕ as the associated twisting isomorphism from E' to E. Then $E'(\mathbb{F}_{p^e})[r]$ is the preimage of $\mathbb{G}_2$ under the map ϕ [17]. In this situation, it is convenient to represent $\mathbb{G}_2$ as $E'(\mathbb{F}_{p^e})[r]$.

B. Schoolbook methods of subgroup membership testing

Let P and α be two elements which are claimed to be members of $\mathbb{G}_1$ and $\mathbb{G}_T$, respectively. The schoolbook method of the subgroup membership testing for the two subgroups are to respectively check that

$$(i) P \in E(\mathbb{F}_p) \text{ and } [r]P = \mathcal{O}_E,$$

$$(ii) \alpha^r = 1.$$

The subgroup membership testing for $\mathbb{G}_2$ is divided into two cases. In particular, let Q be an element which is claimed to be a member of $\mathbb{G}_2$. In the case of E admitting a twist, one requires to check that

$$Q \in E'(\mathbb{F}_{p^e}) \text{ and } [r]Q = \mathcal{O}_{E'}.$$

In the case of E without a twist, one requires to check that

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

Since $r|(p+1-t)$ and $|t| \leq 2\sqrt{p}$ by Hass-Weil bound, it would be preferred to check that

$$Q \in E(\mathbb{F}_{p^k}), [r]Q = \mathcal{O}_E \text{ and } \pi(Q) = [t-1]Q,$$

which mainly costs a scalar multiplication by r.

C. Endomorphisms of elliptic curves

Efficiently computable endomorphisms allow fast elliptic curve scalar multiplication. This idea was first proposed in [18], called GLV method. In particular, consider the curve $E_1 : y^2 = x^3 + b$ defined over $\mathbb{F}_p$ with $p \equiv 1 \bmod 3$ and CM discriminant $D = -3$. The map $\tau : (x, y) \to (\omega \cdot x, y)$ is an endomorphism of E_1, where ω is a primitive cube root of unity in $\mathbb{F}_p$. This map corresponds to two scalar multiplications $[\lambda_1]$ and $[\lambda_2]$ in $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively, where λ_1 and λ_2 are roots of $\lambda^2+\lambda+1 \equiv 0 \bmod r$. Likewise, for the curve $E_2 : y^2 = x^3+ax$ defined over $\mathbb{F}_p$ with $p \equiv 1 \bmod 4$ and CM discriminant $D = -4$, the map $\tau : (x, y) \to (-x, i \cdot y)$ is an endomorphism of E_2, where i is a primitive fourth root of unity in $\mathbb{F}_p$. This map corresponds to two scalar multiplications $[\lambda_1]$ and $[\lambda_2]$ in $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively, where λ_1 and λ_2 are roots of $\lambda^2 + 1 \equiv 0 \bmod r$.

Another well known efficiently computable endomorphism is the map $\psi = \phi^{-1} \circ \pi \circ \phi$ on E', which is proposed by Galbraith $et\ al.$ [19]. The characteristic equation of ψ is

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

It is clear that $\psi^i = \phi^{-1} \circ \pi^i \circ \phi$ for any integer i, which implies the order of ψ is k. Note that

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

for all $Q \in \mathbb{G}_2 = E'(\mathbb{F}_{p^e})$. Acting the map ϕ^{-1} on the two sides of Equation (3), it follows that

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

On the basis of the above observations, Galbraith $et\ al.$ [19] confirm that the map ψ leads to a 4-dimensional GLV method on a large class of elliptic curves over $\mathbb{F}_{p^2}$. Fast implementation of this method on curves with j-invariant 0 is given in [20].

In Sections III and IV, we will show that the above endormorphisms can be applied to accelerating subgroup membership testing on pairing-friendly curves.

D. 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 G_1, G_2 and G_T, respectively. Followed by Barreto $et\ al.$ [9], on curves admitting a twist, the groups G_1, G_2 and G_T are defined as follows

$$\mathbb{G}_1 \subseteq G_1 = E(\mathbb{F}_p), \mathbb{G}_2 \subseteq G_2 = E'(\mathbb{F}_{p^e}), \mathbb{G}_T \subseteq G_T = G_{\Phi_k(p)},$$

where $G_{\Phi_k(p)}$ is the cyclotomic subgroups in $\mathbb{F}^*_{p^k}$. On curves without a twist, it is natural to define G_2 as

$$\mathbb{G}_2 \subseteq G_2 = E(F_{p^k}).$$

The associated cofactors h_1 and h_T are defined as follows:

$$h_1 = |G_1|/r, \quad h_T = |G_T|/r.$$

The definition of h_2 is divided the following two kinds:

$$h_2 = \begin{cases} |G_2|/r, & \text{on curves admitting a twist.} \\ |G_2|/r^2, & \text{on curves without a twist.} \end{cases}$$

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 I, we list several pairing-friendly curves at the 128-bit security level under the attacks of Number Field Sieve and its variants [21], [22]. The above pairing-friendly 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

TABLE I

Subgroup security of pairing-friendly curves at the 128-bit security level. The symbol c_m denotes a composite number of size m bits. Followed by [16], the *BW* family of curves are referred to curves from Construction 6.6 in [24].

k	*family*	$p(bits)$	$r(bits)$	seed z	h_1	h_2	h_T
12	*BN*	446	446	$2^{110}+2^{36}+1$ [15]	1	$13c_{610}$	c_{1336}
12	*BLS*	461	308	$-2^{77}+2^{50}+2^{33}$ [15]	c_{153}	$c_{25}\cdot c_{442}$	$c_{39}\cdot c_{1495}$
16	*KSS*	330	257	$-2^{34}+2^{27}-2^{33}+2^{20}-2^{11}+1$ [15]	c_{75}	$c_{93}\cdot c_{1052}$	$34\cdot c_{2379}$
18	*KSS*	348	256	$2^{44}+2^{22}-2^{9}+2$ [15]	c_{93}	$c_{78}\cdot c_{710}$	$c_{131}\cdot c_{1595}$
13	*BW*	310	267	-2224 [25]	c_{43}	$c_{59}\cdot c_{3435}$	$c_{126}\cdot c_{3368}$
19	*BW*	286	259	-145 [25]	c_{28}	$c_{50}\cdot c_{4861}$	$c_{41}\cdot c_{4842}$

using the ECM method in Magma [23]. It is easy to see that small-subgroup attacks can be easily mounted on cryptographic protocols for many popular pairing-friendly at the 128 security level. It should be noted that even though we fail to obtain a small factor of the cofactor $h_T(c_{1336})$ on *BN-P446* by using ECM method directly, it still can not prove it has no factor smaller than r. Therefore, we do not recommend skipping the membership testing for $\mathbb{G}_T$ on *BN-P446*.

III. Membership Testing for $\mathbb{G}_2$

For efficiency, most of pairing-based protocols are instantiated with pairing-friendly curves admitting a twist. Recently, several curves without a twist also find their own applications on the cryptographic protocols that the implementation efficiency of one party mainly relies on fast computation in $\mathbb{G}_1$. In particular, Clarisse $et\ al.$ [16] found that the two curves *BW13-*$P310$ and *BW19-*$P286$ are suitable for several cryptographic schemes, such as Enhanced Privacy ID [26] and Direct Anonymous Attestation [27]. In this section, we investigate the membership testing for $\mathbb{G}_2$ on both types of curves.

A. Pairing-friendly curves admitting a twist

For a candidate element Q which is claimed to be a member of $\mathbb{G}_2$, Scott [14] confirms that $\mathbb{G}_2$ testing can be replaced by checking that $Q \in E'(\mathbb{F}_{p^e})$ and $\psi(Q) = [t-1]Q$ under the condition that $gcd(h_1, h_2) = 1$. This method is well-suited to *BLS* family of curves. In this subsection, we extend the above method and show that our method would be better on the curve with a large size of the Frobenius trace t. Moreover, our method still works even though $gcd(h_1, h_2) \neq 1$.

Theorem 1 *Let E be an elliptic curve over $\mathbb{F}_p$, and r a large prime factor of $\#E(\mathbb{F}_p)$. Let π be the p-power Frobenius with trace t. Let E' be the associated d-twist of E over $\mathbb{F}_{p^e}$ and ϕ the twisting map from E' to E. Define $g(\psi) = \psi^2 - t\psi + p$ as the characteristic polynomial of ψ, where $\psi = \phi^{-1} \circ \pi \circ \phi$ is an endomorphism on E'. Let η be a multiple of r. Write η in the basis of p as $\eta = \sum_{i=0}^{s} c_i \cdot p^i$, where $c_i \in \mathbb{Z}$. Let b_0 and b_1 be integers such that*

$$b_0 + b_1\psi = f(\psi) \bmod g(\psi),$$

where $f(\psi) = \sum_{i=0}^{s} c_i\psi^i$. Suppose that b_0 and b_1 satisfy

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

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

Proof *If $Q \in \mathbb{G}_2$, we have $\psi(Q) = [p]Q$ from Equation (4). As a consequence, we can 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, we assume that $f(\psi)(Q) = \mathcal{O}_{E'}$. By the Euclidean algorithm, there exist two polynomials $q(\psi), r(\psi) \in \mathbb{Q}[\psi]$ such that

$$f(\psi) = q(\psi) \cdot g(\psi) + r(\psi),$$

where $r(\psi) = b_0 + b_1\psi$. Recall from Equation (2) that for any $Q \in E'(\mathbb{F}_{p^e})$ we have

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

It follows from $f(\psi)(Q) = \mathcal{O}_{E'}$ that

$$[b_1]\psi(Q) = f(\psi)(Q) - q(\psi)\big(g(\psi)(Q)\big) - [b_0]Q = -[b_0]Q.$$

This yields that

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

Since $\gcd\left(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, \#E'(\mathbb{F}_{p^e})\right) = r$ *and* $Q \neq \mathcal{O}_{E'}$*, it is clear that the order of* Q *is* r*, which completes the proof of Theorem 1.*■

Define $C = [c_0, c_1 \cdots, c_s]$ as the coefficient vector of η. One may naturally ask whether there is a vector C such that the corresponding parameters b_0 and b_1 meet the condition in Theorem 1. 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 [17, Section 5], we clearly have $\gcd\left(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, \#E'(\mathbb{F}_{p^e})\right) = r$.

Of course, it is inefficient to select vector C as above, which corresponds to the schoolbook method. In order to improve the efficiency, we expect that the value $n = max\{|c_0|, \cdots, |c_s|\}$ is as small as possible. By the definition of the embedding degree k, we know that $r|\Phi_k(p)$. It is natural to take $\eta = \Phi_k(p)$, which means that $n = 1$ in many cases. Therefore, for 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 all for points in $E'(\mathbb{F}_{p^e})$ for most of popular pairing-friendly curves, such as *BN*, *BLS* and *KSS* families of curves. Hence, the verifier can not distinguish between valid elements and invalid ones. Fuentes *et al.* [28, Section 6.5] pointed out that *MNT* [29] and *Freeman* [30] curves 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 much larger than r on these two families of curves if we take $\eta = \Phi_k(p)$.

In Algorithm 1 (see Appendix A), we present pseudo-code in Magma to search the target vector C for $\mathbb{G}_2$ testing on pairing-friendly curves admitting a twist. To be precise, Lines 1-6 generate the target lattice L, which is the same as the lattice used to find Miller iteration parameters of optimal pairings [31]; Lines 7-8 obtain one of the possible shortest vectors C in L(the norm of C is denoted as min); Lines 9-14 compute the associated parameters b_0 and b_1; Lines 15-16 check to see whether b_0 and b_1 meet the condition in Theorem 1. If so, we obtain the target vector C; otherwise, we execute the following steps: Line 18 collects a mount of candidate vectors whose norms are in range of min to max; Lines 19-26 repeat the previous work until the target vector C is obtained. In Algorithm 1, one requires to input an upper bound max of the norm of target vector C in advance. Once it fails to return a vector C, we swap min for max, and set a larger upper bound max. Then we run it again until a vector C is obtained. It is worth noting that Algorithm 1 is used only to find a target vector C, the overhead of this

process is not contained in that of $\mathbb{G}_2$ testing.

In practice, we find that the vector C can be chosen as the same as the Miller iteration parameters of optimal pairings on many popular pairing-friendly curves, which indicates that the bit length of n is about $\log r/\varphi(k)$.

B. Pairing-friendly curves without a twist

The membership testing for $\mathbb{G}_2$ on pairing-friendly curves without a twist is reasonably complicated. Recall from Section II that for a candidate point Q, the verifier needs to check $Q \in E(\mathbb{F}_{p^k})$, $[r]Q = \mathcal{O}_E$ and $\pi(Q) = [t-1]Q$. Therefore, it is not sufficient to only prove that the order of Q is r in this situation. In the following, we consider how to perform membership testing for $\mathbb{G}_2$ on this type of curves. Our general understanding of the construction of the membership testing for $\mathbb{G}_2$ on this type of curves comes mostly from the following two theorems.

Theorem 2 *Let E be an elliptic curve over $\mathbb{F}_p$ without a twist. Let r be a large prime factor of $\#E(\mathbb{F}_p)$ and k the embedding degree with respect to r. Denote by t the trace of Frobenius on E. Let i be a positive integer such that $\gcd(i,k) = 1$, with non-negative integers m and n satisfying that $i \cdot m - k \cdot n = 1$. Let $b \in \mathbb{Z}$ such that $(t-1)^i \equiv b \bmod r$. Suppose the integer b satisfies*

$$\gcd\left(b^{2m} - t \cdot b^m + p, \#E(\mathbb{F}_{p^k}), \Phi_k(b^m)\right) = r.$$

Then for any non-identity point Q of $E(\mathbb{F}_{p^k})$, the point $Q \in \mathbb{G}_2 = E(\mathbb{F}_{p^k})[r] \cap ker(\pi - [p])$ if and only if $\pi^i(Q) = [b]Q$ and $\Phi_k(\pi)(Q) = \mathcal{O}_E$.

Proof *If $Q \in \mathbb{G}_2$ it follows that the order of Q is r and $\pi(Q) = [t-1]Q$. As a result, we have*

$$\begin{cases} \pi^i(Q) = [(t-1)^i \bmod r]Q = [b]Q, \\ \Phi_k(\pi)(Q) = \Phi_k(t-1)(Q) = \mathcal{O}_E. \end{cases}$$

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

$$\pi(Q) = \pi^{1+k\cdot n}(Q) = \pi^{i\cdot m}(Q) = [b^m]Q. \tag{5}$$

Plugging the above result to Equation (1) and the equality $\Phi_k(\pi)(Q) = \mathcal{O}_E$, we immediately have

$$\begin{cases} [b^{2m} - t \cdot b^m + p]Q = \mathcal{O}_E, \\ [\Phi_k(b^m)]Q = \Phi_k(\pi)(Q) = \mathcal{O}_E. \end{cases}$$

Thus, the order of Q divides $\gcd\left(b^{2m}-t\cdot b^m+p, \#E(\mathbb{F}_{p^k}), \Phi_k(b^m)\right)$. *By assumption, it is easy to see that the order of Q is r. On the other hand, since $t-1$ is a primitive k-th root of unity modulo r, by Equation (5) we conclude that*

$$\pi(Q)=[b^m]Q=[(t-1)^{1+k\cdot n}]Q=[t-1]Q=[p]Q,$$

which completes the proof of Theorem 2.■

If we assume $\gcd(h_1, \Phi_k(t-1))=1$, then there always exists an integer b meeting the condition in Theorem 2. Indeed, we can take $i=1$, and thus $b=t-1$ and $m=1$. In this case, it is easy to see that

$$\begin{aligned}&\gcd\left(b^{2m}-t\cdot b^m+p, \#E(\mathbb{F}_{p^k}), \Phi_k(b^m)\right)\\ =&\gcd(p+1-t, \Phi_k(t-1))\\ =&\gcd(h_1\cdot r, \Phi_k(t-1))\\ =&r.\end{aligned}$$

In Theorem 2, we expect that the bit length of b is as small as possible under the condition that

$$\gcd\left(b^{2m}-t\cdot b^m+p, \#E(\mathbb{F}_{p^k}), \Phi_k(b^m)\right)=r.$$

Since $t-1$ is a primitive k-th root of unity modulo r, the target parameter b can be obtained by exhausting $i\in\{1,2,\cdots k-1\}$. As estimated in [32], the size of b would be in approximately $\log r/\varphi(k)$ bits on some certain curves. In the following, we further optimize the testing method for $\mathbb{G}_2$ on curves with CM discriminate $D=-3$ or -4.

Theorem 3 *Let E be an elliptic curve over $\mathbb{F}_p$ without a twist, and CM discriminant $D=-3$ or -4. Let r be a large prime factor of $\#E(\mathbb{F}_p)$ and k the embedding degree with respect to r. Denote by t the trace of Frobenius on E. Let $[\lambda]$ be the multiplication map in $\mathbb{G}_2=E(\mathbb{F}_{p^k})[r]\cap ker(\pi-[p])$ corresponding to a GLV endomorphism τ. Let $d=-D$ and i be an integer such that* $\gcd(d\cdot i, k)=1$, *with positive integers m and n satisfying that $d\cdot i\cdot m-n\cdot k=1$. Let $b\in\mathbb{Z}$ such that $(t-1)^i\equiv b\cdot\lambda \bmod r$. Suppose b satisfies*

$$\gcd\left(b^{2d\cdot m}-t\cdot b^{d\cdot m}+p, \#E(\mathbb{F}_{p^k}), \Phi_k(b^{d\cdot m})\right)=r.$$

Then for any non-identity point Q of $E(\mathbb{F}_{p^k})$, the point $Q\in\mathbb{G}_2$ if and only if $\pi^i(Q)=[b]\tau(Q)$ and $\Phi_k(\pi)(Q)=\mathcal{O}_E$.

Proof *If $Q \in \mathbb{G}_2$, the equality $\Phi_k(\pi)(Q) = \mathcal{O}_E$ has been proved in Theorem 2. 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, since $\pi^i(Q) = [b]\tau(Q)$ it follows that

$$\pi^{d \cdot i}(Q) = [b^d]Q, \tag{6}$$

which implies that

$$\pi(Q) = \pi^{1+n \cdot k}(Q) = \pi^{d \cdot m \cdot i}(Q) = [b^{d \cdot m}]Q. \tag{7}$$

Analogous to the proof of Theorem 2, we immediately have

$$\begin{cases} [b^{2d \cdot m} - t \cdot b^{d \cdot m} + p]Q = \mathcal{O}_E, \\ [\Phi_k(b^{d \cdot m})]Q = \Phi_k(\pi)(Q) = \mathcal{O}_E. \end{cases}$$

Thus, the order of Q divides $\gcd\left(b^{2d \cdot m} - t \cdot b^{d \cdot m} + p, \#E(\mathbb{F}_{p^k}), \Phi_k(\ b^{d \cdot m})\right)$*. By assumption, it is easy to see that the order of Q is r. Finally, it follows from (7) that we have*

$$\pi(Q) = [b^{d \cdot m}]Q = [(b\lambda)^{d \cdot m}]Q = [(t-1)^{1+n \cdot k}]Q = [t-1]Q = [p]Q,$$

which completes the proof of Theorem 3.■

Similar to Theorem 2, we can exhaust $i \in \{1, 2, \cdots k-1\}$ to search a parameter b such that the bit length of b is as small as possible under the condition that

$$\gcd\left(b^{2d \cdot m} - t \cdot b^{d \cdot m} + p, \#E(\mathbb{F}_{p^k}), \Phi_k(b^{d \cdot m})\right) = r.$$

We fortunately find that Theorem 3 can be applied into the membership testing for $\mathbb{G}_2$ on *BW13-P310* and *BW19-P286*. More details of this issue will be illustrated in Section V.

IV. Membership Testing for $\mathbb{G}_1$ and $\mathbb{G}_T$

In this section, we mainly discuss fast membership testings for $\mathbb{G}_1$ and $\mathbb{G}_T$. Similar as the case of $\mathbb{G}_2$, we find that efficiently computable endomorphisms on the above two subgroups also can be used to speed up testing efficiencies.

A. *Membership testing for* $\mathbb{G}_1$

Scott [14, Section 6] proposed a fast membership testing method for $\mathbb{G}_1$ on *BLS* families of curves. In particular, Scott proved that a candidate point $P \in \mathbb{G}_1$ if and only if $\tau(P) = [\lambda]P$ on the families of curves. This method is estimated to be approximately twice as fast as multiplication by r directly. In this subsection, we extend this method to all pairing-friendly curves with CM discriminant $D = -3$ or -4.

Theorem 4 *Let E be an elliptic curve over $\mathbb{F}_p$ with CM discriminant $D = -3$ or -4, and r a large prime factor of $\#E(\mathbb{F}_p)$. Let $[\lambda]$ be the scalar multiplication map in $\mathbb{G}_1 = E(\mathbb{F}_p)[r]$ corresponding to a GLV endomorphism τ. Suppose $a_0, a_1 \in \mathbb{Z}$ satisfy that*

$$(1) a_0 + a_1\lambda \equiv 0 \bmod r,$$

$$(2) \gcd\left(a_0^2 - a_0 \cdot a_1 + a_1^2, \#E(F_p)\right) = r, \textit{ if } D = -3;$$

$$\textit{or } \gcd\left(a_0^2 + a_1^2, \#E(F_p)\right) = r, \textit{ if } D = -4.$$

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

Proof *We only prove the case that $D = -3$ in detail, since the proof of the other case is similar. 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, we assume that $[a_0]P + [a_1]\tau(P) = \mathcal{O}_E$. Since the order of the endomorphism τ is 3, we get that

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

By the assumption that $\gcd\left(a_0^2 - a_0 \cdot a_1 + a_1^2, \#E(F_p)\right) = r$ and $P \neq \mathcal{O}_E$, it follows that the order of P is r, which finishes the proof of this theorem.■

Analogous to the membership testing for $\mathbb{G}_2$ on pairing friendly curves admitting a twist, there always exist a_0 and a_1 satisfying the condition in Theorem 4. Generally, the bit length of $max\{a_0, a_1\}$ is about $\log r/2$. Therefore, this method is roughly twice faster than the previous one. In Algorithm 2 (see Appendix A), we present pseudo-code in Magma to search a_0 and a_1 such that $max\{a_0, a_1\}$ is as small as possible. Here, we do not explain the working mechanism of Algorithm 2 in detail as it is similar to that of Algorithm 1.

Based on the analysis above, our method may be a better choice than the method of clearing cofactor even in efficiency if the ratio between $\log_2(h_1)$ and $\log_2(r)$ is no less than 0.5. For example, on curves with embedding degrees 6 and 8 proposed by Guillevic $et\ al.$ [33] using the modified Cocks-Pinch method, cofactors h_1 are even larger than r. In this situation our method is clearly a winner.

B. Membership testing for $\mathbb{G}_T$

The schoolbook method of the membership testing for $\mathbb{G}_T$ is to raise the candidate element to the power of r and compare the result against the identity element. Scott [14] described a new testing method under the condition that $\gcd(h_1, h_T) = r$, which is tailored to ***BLS*** families of curves. In particular, let α be a candidate element which is claimed to be a member of $\mathbb{G}_T$. The verifier requires to check that $\alpha \in \mathbb{G}_{\Phi_k(p)}$ and $\alpha^{p+1} = \alpha^t$. Since Frobenius map can be computed efficiently, the main cost of this method is one exponentiation by t.

Inspired by the method of the membership testing for $\mathbb{G}_2$ on pairing-friendly curves admitting a twist, we generalize the testing method in this subsection.

Proposition 1 *Let η be a multiple of r. Write η in the basis of p as $\eta = \sum_{i=0}^{s} c_i \cdot p^i$, where $c_i \in \mathbb{Z}$. Let $\alpha \neq 1$ be an element of $\mathbb{F}_{p^k}^*$. Suppose $\gcd\big(\eta, \Phi_k(p)\big) = r$. Then $\alpha \in \mathbb{G}_T$ if and only if*

$$\alpha^{\Phi_k(p)} = 1 \text{ and } \alpha^{\sum_{i=0}^{s} c_i \cdot p^i} = 1.$$

Proof *The necessity is obvious. We only prove the sufficiency. If $\alpha^{\Phi_k(p)} = 1$ and $\alpha^{\sum_{i=0}^{s} c_i \cdot p^i} = 1$, then the order of α divides $\gcd\big(\eta, \Phi_k(p)\big)$. By the condition that $\gcd\big(\eta, \Phi_k(p)\big) = r$, it is clear that the order of α is r.*■

As stated in Section III, there always exists a vector C meeting the condition in Proposition 1. Therefore, the overhead of the testing mainly requires an exponentiation by $n = max\{c_0, c_1 \cdots, c_s\}$. Similarly, Algorithm 3 (see Appendix) is presented to search the target vector C. 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 [34], [35] in the case that the embedding degree k is divided by 6.

V. APPLICATIONS

In this section, we illustrate the main mechanics of our methods by applying them to two different types of curves: *KSS16-P330* and *BW13-P310*. In the following, we denote by *nbits(A)* and *hw(A)* the bitlength and the Hamming weight in 2-non-adjacent form of A, respectively.

A. KSS16-P330

KSS16 family of curves are parameterized by the following polynomials

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

In order to reach the 128-bit security level, the seed z is recommended as $z = -2^{34} + 2^{27} - 2^{23} + 2^{20} - 2^{11} + 1$ [15]. The corresponding curve equations are given as

$$E : y^2 = x^3 + x, \quad E' : y^2 = x^3 + (1/u)x,$$

where $u \in \mathbb{F}_{p^4}$.

1) The case of $\mathbb{G}_1$: Using Algorithm 2 the parameters a_0 and a_1 can be selected as

$$\begin{cases} a_0 = 299609893663766701347795728932946474488, \\ a_1 = -164302199751097868481049270705164195687. \end{cases}$$

It is easy to find that $-17a_0 - 31a_1 = 1$ by using the Euclidean algorithm. Therefore, it seems more efficient to replace a_0 and a_1 by $a_0' = 17a_0$ and $a_1' = 17a_1$, respectively. We also check that $\gcd\left(a_0'^2 + a_1'^2, \#E(F_p)\right) = r$. Let Q be a point which is claimed to be a member of $\mathbb{G}_1$. By Theorem 4, the membership testing for $\mathbb{G}_1$ on the curve is equivalent to check that

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

Since $\mathit{nbits}(a_1) + \mathit{hw}(a_1) \approx \mathit{nbits}(z^4) + \mathit{hw}(z^4)$, we can roughly estimate that the cost of 1 scalar multiplication by a_1 is the same as that by z^4. In conclusion, it approximately requires 1 scalar multiplication by z^4, 5 point doublings, 3 point additions and 1 application of the endomorphism τ.

2) The case of $\mathbb{G}_2$*:* We first consider the vector C as $[2,0,0,z,1,0]$. It is the same as the Miller iteration parameters recommended in [36]. Then the parameters b_0 and b_1 in Theorem 1 are given by

$$b_0 = -t^2 \cdot p - t \cdot p \cdot z + p^2 + 2,$$
$$b_1 = t^3 + t^2 \cdot z - 2t \cdot p - p \cdot z.$$

Unfortunately, we find that $\gcd\left(b_0^2 + b_0 \cdot b_1 \cdot t + b_1^2 \cdot p, \#E'(\mathbb{F}_{p^4})\right)$ is equal to $4r$, which does not meet the condition in Theorem 1. Instead, we run Algorithm 1 to get the following target vector C:

$$[243614193, 2192527740, -1218070967, 730842580, 1705299354, 730842580, 1218070967, -4628669674].$$

The relations among terms c_i for $i \in \{0, 1, \cdots, 7\}$ are given as follows:

$$\begin{aligned} &c_3 = 3c_0 + 1, c_1 = 3c_3, c_2 = c_0 - c_1 + c_3, c_5 = c_3, \\ &c_4 = -c_2 + c_3 - c_0, c_6 = -c_2, c_7 = -c_1 + 2c_2. \end{aligned} \tag{8}$$

Let Q be a point of the *KSS16-P330* curve which is claimed to be a member of $\mathbb{G}_2$. Let S_i denote $[c_i]Q$ for $i \in \{0, 1, \cdots, 7\}$. By (8), the calculations of $S_0, S_1, \cdots, S_7$ require one multiplication by c_0, 3 point doublings and 8 point additions. By Theorem 1, the membership testing for $\mathbb{G}_2$ on the curve is equivalent to check that

$$\begin{cases} Q \in E'(\mathbb{F}_{p^4}), \\ \sum_{i=1}^{7} \psi^i(S_i) = -S_0., \end{cases}$$

Since $\mathit{nbits}(c_0) + \mathit{hw}(c_0) \approx \mathit{nbits}(z) + \mathit{hw}(z)$, we can roughly estimate the cost of 1 scalar multiplication by c_0 is the same as that by z. In total, the testing approximately costs 1 scalar multiplication by z, 3 point doublings, 14 point additions and 7 applications of the endomorphism ψ.

3) The case of $\mathbb{G}_T$*:* Using Algorithm 3 we obtain a vector C as

$$[2679756127, -2192527740, 730842580, 730842580, -3166984514, 1705299354, 243614193, 2679756127]$$

The relations among terms c_i for $i \in \{0, 1, \cdots, 7\}$ are given as follows:

$$\begin{aligned} &c_2 = c_3 = 3c_6 + 1, c_1 = -3c_2, c_0 = c_7 = 2c_6 - c_1 + 1, \\ &c_5 = 2c_2 + c_6 + 1, c_4 = -2c_5 + c_6 + 1. \end{aligned} \tag{9}$$

We first check that

$$\alpha^{p^8} \cdot \alpha = 1. \tag{10}$$

If the element α fails to pass the above testing, then one could claim that α is an invalid element; otherwise, we continue to the testing and thus have $\alpha^{-1} = \alpha^{p^8}$. Let g_i denote α^{c_i} for $i \in \{0, 1, \cdots, 7\}$. By (9), we have

$$\begin{aligned} &g_6 = \alpha^{c_6}, f_1 = g_6 \cdot \alpha, g_2 = g_3 = g_6^2 \cdot f_1, f_2 = g_2^2, g_1 = (f_2 \cdot g_2)^{p^8}, \\ &g_0 = g_7 = g_6 \cdot f \cdot g_1^{p^8}, g_5 = f_1 \cdot f_2, g_4 = g_5^{2 \cdot p^8} \cdot f_1. \end{aligned} \tag{11}$$

By Proposition 1, we finally check that

$$\prod_{\mathrm{i}=0}^{7} g_i^{p^i} = 1. \tag{12}$$

Since *nbits*(c_0)+*hw*$(c_0) \approx$ *nbits*(z)+*hw*(z), we can roughly estimate the cost of 1 exponentiation by c_7 is the same as that by z. In conclusion, the testing approximately costs one exponentiation by z, 3 squarings, 15 multiplications and 10 Frobenius maps.

B. BW13-P310

The methods of the membership testing for $\mathbb{G}_1$ and $\mathbb{G}_T$ have no difference between pairing-friendly curves admitting a twist and without a twist. Therefore, in the following we only discuss the membership testing for $\mathbb{G}_2$ on *BW13-P310*. From Construction 6.6 in [24], a family of curves with $k = 13$ and CM discriminant $D = -3$ can be parameterized as follows:

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

In order to reach the 128-bit security level, the seed z is recommended as $z = -2224$ [25], and the curve equation can be selected as $E : y^2 = x^3 - 17$. From the form of polynomial $r(z)$, we can see that

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

It is easy to see that there exists a GLV endomorphisms τ corresponding to scalar multiplication $[\lambda]$ where $\lambda = z^{13} - 1$. Let notations i, m and b defined as in Theorem 3. We fortunately find that when $i = 1$

$$\gcd\left(b^{6 \cdot m} - t \cdot b^{3 \cdot m} + p, \#E(\mathbb{F}_{p^k}), \Phi_k(b^{3 \cdot m})\right) = r,$$

TABLE II

Parameters of the membership testing on pairing-friendly curves at the 128-bit security level. On *BW13-P310* and *BW19-P286*, 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 3.

Curve	$\mathbb{G}_1$		$\mathbb{G}_2$	$\mathbb{G}_T$
	a_0	a_1	C	C
BN-P446	$-$	$-$	$[z+1, z, z, -2z]$	$[z+1, z, z, -2z]$
BLS12-P461	z^2	1	$[z, -1, 0, 0]$	$[z, -1, 0, 0]$
KSS18-P348	$(z/7)^3$	$-18a_0 - 1$	$[2z, 7, 0, z, 0, 0]$	$[2z, 7, 0, z, 0, 0]$
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	$-(z^{10} - z)(z^6 - z^3 + 1)(z + 1)$	$a_0 \cdot z - 1$	$[1, 13, -z]$	$[z^2, -z, 1, 0 \ldots, 0]$

and the bit length of b reaches the minimum(i.e., $b = -z$ and $m = 9$). By Theorem 3, the membership testing for $\mathbb{G}_2$ on this curve is equivalent to check that

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

The point $\sum_{i=1}^{12} \pi^i(Q)$ can be computed 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 $Q \in E(\mathbb{F}_{p^k})$, it totally requires 1 scalar multiplication by z, 4 point additions, 5 applications of the endomorphism π and 1 application of the endomorphism τ.

VI. Efficiency Comparisons

Besides *KSS16-P330* and *BW13-P310*, we consider more pairing-friendly curves as presented in Table I. Denote by Z_c, D and A the costs of scalar multiplication by z, point doubling and point addition, respectively. Likewise, we denote by Z_f, M and S the costs of exponentiation by z, multiplication and squaring in finite fields, respectively. In Table II, we list the parameters of the membership testing on each pairing-friendly curve by using our method. It should be noted that $\mathbb{G}_1$ testing on BN-446 can be skipped as the associated parameter h_1 is equal to 1.

TABLE III

Comparison of operation counts for the membership testing for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on pairing-friendly curves at the 128-bit security level with the previous leading work in the literature.

Curve	$gcd(h_1,h_2)$	$gcd(h_1,h_T)$	*The previous method*			*The proposed method*		
			$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_T$	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_T$
BN-P446	1	1	$-$	$2Z_c+2D+A$	$2Z_f+2S+M$	$-$	Z_c+3A+D	Z_f+S+3M
BLS12-P461	1	1	$2Z_c$	Z_c	Z_f+S+3M	$2Z_c$	Z_c	Z_f+S+3M
KSS16-P330	4	4	$8Z_c$	$8Z_c$	$8Z_f$	$4Z_c+5D+3A$	$Z_c+3D+14A$	$Z_f+3S+15M$
KSS18-P348	1	1	$6Z_c$	$4Z_c$	$4Z_f$	$3Z_c+4D+2A$	$Z_c+3D+3A$	$Z_f+4S+3M$
BW13-P310	$-$	1	$24Z_c+16A$	$24Z_c+16A$	$14Z_f+7M$	$12Z_c+4A$	Z_c+4A	$2Z_f+7M$
BW19-P286	$-$	1	$36Z_c+24A$	$36Z_c+24A$	$20Z_f+8M$	$18Z_c+5A$	Z_c+5A	$2Z_f+8M$

TABLE IV

Comparison of timing(ms) for the membership testing for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on pairing-friendly curves at the 128-bit security level with the previous leading work in the literature.

	The previous method			*The proposed method*		
	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_T$	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_T$
BN-P446	$-$	10.32	6.43	$-$	5.51	3.15
BLS12-P461	1.51	3.89	4.10	1.51	3.89	4.10
KSS16-P330	2.03	24.18	12.67	1.11	4.75	2.24
KSS18-P348	2.07	11.47	13.26	1.07	3.23	3.29
BW13-P310	1.97	115.71	5.01	1.03	6.68	0.95
BW19-P286	1.82	214.10	10.69	0.95	10.71	1.68

In Table III, we compare the operation counts of our results to the previous leading work, ignoring the cost of efficiently computable endomorphisms. Specially, Columns $2-3$ in Table III list the values $\gcd(h_1,h_2)$ and $\gcd(h_1,h_T)$. As we illustrate in Sections III and IV, in the case that $\gcd(h_1,h_2)=1$(resp. $\gcd(h_1,h_T)=1$), the method appearing in [14] represents the fastest previously known method for $\mathbb{G}_2$ (resp. $\mathbb{G}_T$) testing; otherwise, the naive schoolbook method by multiplication (resp. exponentiation) by r is the fastest previously known method. As for $\mathbb{G}_1$ testing, on *BLS12-P461* the previous leading work is proposed by Scott [14]; on *BN-P446*, the overhead of the testing is negligible as the cofactor h_1 is equal to 1; on other curves, the schoolbook method by multiplication by r is the fastest previously known method. Consequently, Columns $4-6$ in Table III summarize the operation counts of membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ using the fastest previously known method. Note that the prime r and the Frobenius trace t on *KSS18-P348* are parameterized by $(z^6+37z^3+343)/343$ and $(z^4+16z+7)/7$ respectively, and the

parameter $a_0 = (z/7)^3$. For simplicity, we roughly estimate that one multiplication/exponentiation by r, $t-1$ and a_0 costs $6Z_c/6Z_f$, $4Z_c/4Z_f$ and $3Z_c/3Z_f$, respectively. Likewise, we roughly estimate that one multiplication/exponentiation by r costs $8Z_c/8Z_f$ on *KSS16-P330*.

Columns $7-9$ in Table III list the operation counts of membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ by using our method, respectively. For $\mathbb{G}_1$ testing, the size of the scalar is reduced to roughly $\log r/2$ bits. For $\mathbb{G}_2$ testing, the size of the scalar is reduced to approximately $\log r/\varphi(k)$ bits on *BN-P446*, *BLS12-P461*, *KSS16-P330* and *KSS18-P348*. It is further reduced to roughly $\log r/(2\varphi(k))$ bits on *BW13-P310* and *BW19-P286*. Therefore, our method would be about $2\varphi(k)$ times faster than the previous one. For $\mathbb{G}_T$ testing, the size of the exponentiation is reduced to approximately $\log r/\varphi(k)$ bits across different curves.

In Table IV, implementation results in Magma are presented to verify the performance of our proposed method. On each curve, we compare the efficiency between our proposed method and the fastest previously known one for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ testings. In particular, our approach gives the same performance as the previous one on *BLS12-P461*. On other curves, the overhead has a reduction from $83\% - 93\%$ for $\mathbb{G}_1$ testing. This result is nearly consistent with the theoretical estimation. For $\mathbb{G}_2$ testing, the proposed technique reduces the overhead in the range of 87% to 1899%. It is specially worth noting that our method is about 17.3 and 20 times faster than the previous one on *BW13-P310* and *BW19-286* respectively, which is below expectations. The reason for the discrepancy is that the operation counts of the calculation of $\Phi_k(\pi(Q))$ is without taking into account for any candidate point Q on the two curves. For $\mathbb{G}_T$ testing, the overhead has a reduction from 104% to 536%. As we can see, our proposed method has noticeable lower overhead for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ testings on many target curves.

VII. Conclusion

The threat of small-subgroup attacks are non-negligible in pairing-based protocols. In this paper, we mainly developed the efficient ways to resist the attacks: subgroup membership testing. For $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ testings, several optimizations were proposed, which are suitable for many pairing-friendly curves including the curves admitting a twist and without a twist. We applied our methods to several pairing-friendly curves at the 128-bit security level. The results showed that the membership testing for the three subgroups can be performed efficiently.

References

[1] N. El Mrabet and M. Joye, *Guide to pairing-based cryptography*. Chapman and Hall/CRC, 2016.

[2] M. Joye and G. Neven, *Identity-based cryptography*. IOS press, 2009.

[3] I. F. Blake, G. Seroussi, and N. P. Smart, *Advances in elliptic curve cryptography*. Cambridge University Press, 2005.

[4] J. Groth, "On the Size of Pairing-Based Non-interactive Arguments," in *Advances in Cryptology – EUROCRYPT 2016*, M. Fischlin and J.-S. Coron, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 305–326.

[5] C. Diem and E. Thomé, "Index calculus in class groups of non-hyperelliptic curves of genus three," *Journal of Cryptology*, vol. 21, no. 4, pp. 593–611, 2008.

[6] P. Gaudry, F. Hess, and N. P. Smart, "Constructive and destructive facets of weil descent on elliptic curves," *Journal of Cryptology*, vol. 15, no. 1, pp. 19–46, 2002.

[7] S. Tian, B. Li, K. Wang, and W. Yu, "Cover attacks for elliptic curves with cofactor two," *Designs, Codes and Cryptography*, vol. 86, no. 11, pp. 2451–2468, 2018.

[8] C. H. Lim and P. J. Lee, "A Key Recovery Attack on Discrete Log-Based Schemes Using a Prime Order Subgroup," in *Advances in Cryptology — CRYPTO '97*, B. S. Kaliski, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997, pp. 249–263.

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

[10] M. Scott, "Unbalancing Pairing-Based Key Exchange Protocols," *IACR Cryptol. ePrint Arch.*, vol. 2013, p. 688, 2013.

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

[12] A. Budroni and F. Pintore, "Efficient Hash Maps to $\mathbb{G}_2$ on BLS Curves," *Applicable Algebra in Engineering, Communication and Computing*, p. to appear, 2020.

[13] M. Hamburg, "Decaf: Eliminating Cofactors Through Point Compression," in *Advances in Cryptology – CRYPTO 2015*, R. Gennaro and M. Robshaw, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 705–723.

[14] M. Scott, "A Note on Group Membership Tests for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on BLS Pairing-Friendly Curves," Cryptology ePrint Archive, Report 2021/1130, 2021, https://ia.cr/2021/1130.

[15] R. Barbulescu and S. Duquesne, "Updating Key Size Estimations for Pairings," *Journal of Cryptology*, vol. 32, no. 4, pp. 1298–1336, 2019.

[16] R. Clarisse, S. Duquesne, and O. Sanders, "Curves with Fast Computations in the First Pairing Group," in *Cryptology and Network Security*, S. Krenn, H. Shulman, and S. Vaudenay, Eds. Cham: Springer International Publishing, 2020, pp. 280–298.

[17] F. Hess, N. P. Smart, and F. Vercauteren, "The Eta Pairing Revisited," *IEEE Transactions on Information Theory*, vol. 52, no. 10, pp. 4595–4602, 2006.

[18] R. P. Gallant, R. J. Lambert, and S. A. Vanstone, "Faster Point Multiplication on Elliptic Curves with Efficient Endomorphisms," in *Advances in Cryptology — CRYPTO 2001*, J. Kilian, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pp. 190–200.

[19] S. D. Galbraith, X. Lin, and M. Scott, "Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves," in *Advances in Cryptology - EUROCRYPT 2009*, A. Joux, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 518–535.

[20] Z. Hu, P. Longa, and M. Xu, "Implementing the 4-dimensional GLV Method on GLS Elliptic Curves with j-invariant 0," *Designs, Codes and Cryptography*, vol. 63, no. 3, pp. 331–343, 2012.

[21] A. Joux and C. Pierrot, "The Special Number Field Sieve in $\mathbb{F}_{p^n}$," in *Pairing-Based Cryptography – Pairing 2013*, Z. Cao and F. Zhang, Eds. Cham: Springer International Publishing, 2014, pp. 45–61.

[22] T. Kim and R. Barbulescu, "Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case," in *Advances in Cryptology – CRYPTO 2016*, M. Robshaw and J. Katz, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 543–571.

[23] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system. I. The user language," *J. Symbolic Comput.*, vol. 24, no. 3-4, pp. 235–265, 1997, computational algebra and number theory (London, 1993).

[24] D. Freeman, M. Scott, and E. Teske, "A Taxonomy of Pairing-Friendly Elliptic Curves," *Journal of Cryptology*, vol. 23, no. 2, pp. 224–280, 2010.

[25] A. Guillevic, "A Short-List of Pairing-Friendly Curves Resistant to Special TNFS at the 128-Bit Security Level," in *Public-Key Cryptography – PKC 2020*, A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, Eds. Cham: Springer International Publishing, 2020, pp. 535–564.

[26] E. Brickell and J. Li, "Enhanced Privacy ID: A Direct Anonymous Attestation Scheme with Enhanced Revocation Capabilities," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 3, pp. 345–360, 2012.

[27] E. Brickell, J. Camenisch, and L. Chen, "Direct Anonymous Attestation," in *Proceedings of the 11th ACM Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery, 2004, pp. 132–145.

[28] L. Fuentes-Castañeda, E. Knapp, and F. Rodríguez-Henríquez, "Faster Hashing to $\mathbb{G}_2$," in *Selected Areas in Cryptography*, A. Miri and S. Vaudenay, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 412–430.

[29] A. Miyaji, M. Nakabayashi, and S. Takano, "Characterization of Elliptic Curve Traces Under FR-Reduction," in *Information Security and Cryptology — ICISC 2000*, D. Won, Ed. Springer Berlin Heidelberg, 2001.

[30] D. Freeman, "Constructing Pairing-Friendly Elliptic Curves with Embedding Degree 10," in *Algorithmic Number Theory*, F. Hess, S. Pauli, and M. Pohst, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 452–465.

[31] F. Vercauteren, "Optimal Pairings," *IEEE Transactions on Information Theory*, vol. 56, no. 1, pp. 455–461, 2009.

[32] C.-A. Zhao, F. Zhang, and J. Huang, "A note on the Ate pairing," *International Journal of Information Security*, vol. 7, no. 6, pp. 379–382, 2008.

[33] A. Guillevic, S. Masson, and E. Thomé, "Cocks-Pinch Curves of Embedding Degrees Five to Eight and Optimal Ate Pairing Computation," *Designs, Codes and Cryptography*, vol. 88, no. 6, pp. 1047–1081, 2020.

[34] R. Granger and M. Scott, "Faster squaring in the cyclotomic subgroup of sixth degree extensions," in *Public Key Cryptography – PKC 2010*, P. Q. Nguyen and D. Pointcheval, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 209–223.

[35] K. Karabina, "Squaring in Cyclotomic Subgroups," *Mathematics of Computation*, vol. 82, no. 281, 2012.

[36] X. Zhang and D. Lin, "Analysis of Optimum Pairing Products at High Security Levels," in *Progress in Cryptology - INDOCRYPT 2012*, S. Galbraith and M. Nandi, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 412–430.

APPENDIX A

Algorithm 1 Find a target vector C for $\mathbb{G}_2$ testing

Input: curve parameters t, p, r, k and an integer max

Output: Vector C

1: $B := RMatrixSpace(Integers(), \varphi(k), \varphi(k))!0$;

2: $B[1][1] := r$;

3: **for** i := 2 **to** $\varphi(k)$ **do**

4: $B[i][1] = -p^{i-1}$;$B[i][i] := 1$;

5: **end for**

6: $L := LatticeWithBasis(B)$;

7: $C := ShortestVector(B)$;

8: $min := Norm(C)$;

9: $P < x, m, n >:= PolynomialRing(Integers(), 3)$;

10: $R := quo < P|x^2 - mx + n >$;

11: $b := R!(c_0 + c_1 x + \cdots + c_{\varphi(k-1)} x^{\varphi(k-1)})$;

12: $b := Evaluate(b, [2, t])$;

13: $b := Evaluate(b, [3, p])$;

14: $[b_1, b_0] := Coefficients(b)$;

15: **if** $gcd(b_0^2 + b_0 b_1 t + b_1^2 p, \#E'(\mathbb{F}_{p^e}))$ eq r **then**

16: **break**;

17: **else**

18: $V := ShortVectorsProcess(L, min, max)$;

19: **repeat**

20: $C := NextVector(V)$;

21: $b := R!(c_0 + c_1 x + \cdots + c_{\varphi k-1} x^{\varphi k-1})$;

22: $b := Evaluate(b, [2, t])$;

23: $b := Evaluate(b, [3, p])$;

24: $[b_1, b_0] := Coefficients(b)$;

25: **until** $gcd(b_0^2 + b_0 b_1 t + b_1^2 p, \#E'(\mathbb{F}_{p^e}))$ eq r;

26: **end if**

27: **return** C

Algorithm 2 Find parameters a_0 and a_1 for $\mathbb{G}_1$ testing

Input: curve parameter r, GLV scalar λ, CM discriminant D and an integer max

Output: a_0 and a_1

1: $B := RMatrixSpace(Integers(), 2, 2)![r, 0, -\lambda, 1]$;

2: $L := LatticeWithBasis(B)$;

3: $A := ShortestVector(B)$; //$[a_0, a_1] := A$

$min := Norm(A)$;
if $\gcd(a_0^2 - (-D \mod 2)a_0a_1 + a_1^2, \#E(\mathbb{F}_p))$ eq r **then**
    break;
else
    $V := ShortVectorsProcess(L, min, max)$;
    repeat
        $A := NextVector(V)$;
    until $\gcd(a_0^2 - (-D \mod 2)a_0a_1 + a_1^2, \#E(\mathbb{F}_p))$ eq r;
return a_0, a_1

Algorithm 3 Find a target vector C for $\mathbb{G}_T$ testing

Input: elliptic curve parameters p, r, k and an integer max

Output: Vector C

$B := RMatrixSpace(Integers(), \varphi(k), \varphi(k))!0$;
$B[1][1] := r$;
for i := 2 **to** $\varphi(k)$ **do**
    $B[i][1] = -p^{i-1}$;$B[i][i] := 1$;
end for
$L := LatticeWithBasis(B)$;
$C := ShortestVector(B)$;
$min := Norm(C)$;
if $gcd\big(c_0 + c_1 \cdot p + \cdots + c_{\varphi(k)-1} \cdot p^{\varphi(k)-1}, \Phi_k(p)\big)$ eq r **then**
    break;
else
    $V := ShortVectorsProcess(L, min, max)$;
    repeat
        $C := NextVector(V)$;
    until $gcd(c_0 + c_1 \cdot p + \cdots + c_{\varphi(k)-1} \cdot p^{\varphi(k)-1}, \Phi_k(p))$ eq r;
end if
return C