Co-factor clearing and subgroup membership testing on pairing-friendly curves

Youssef El Housni, Aurore Guillevic, Thomas Piellard

Co-factor clearing and subgroup membership testing on pairing-friendly curves*

Youssef El Housni[1,2,3][0000−0003−2873−3479],
Aurore Guillevic[4,5][0000−0002−0824−7273], and
Thomas Piellard[1]

[1] ConsenSys, gnark
youssef.elhousni@consensys.net
thomas.piellard@consensys.net
[2] LIX, CNRS, École Polytechnique, Institut Polytechnique de Paris
[3] Inria
[4] Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
[5] Aarhus University, Aarhus, Denmark
aurore.guillevic@inria.fr

Abstract. An important cryptographic operation on elliptic curves is hashing to a point on the curve. When the curve is not of prime order, the point is multiplied by the cofactor so that the result has a prime order. This is important to avoid small subgroup attacks for example. A second important operation, in the composite-order case, is testing whether a point belongs to the subgroup of prime order. A pairing is a bilinear map $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ where $\mathbb{G}_1$ and $\mathbb{G}_2$ are distinct subgroups of prime order r of an elliptic curve, and $\mathbb{G}_T$ is a multiplicative subgroup of the same prime order r of a finite field extension. Pairing-friendly curves are rarely of prime order. We investigate cofactor clearing and subgroup membership testing on these composite-order curves. First, we generalize a result on faster cofactor clearing for BLS curves to other pairing-friendly families of a polynomial form from the taxonomy of Freeman, Scott and Teske. Second, we investigate subgroup membership testing for $\mathbb{G}_1$ and $\mathbb{G}_2$. We fix a proof argument for the $\mathbb{G}_2$ case that appeared in a preprint by Scott in late 2021 and has recently been implemented in different cryptographic libraries. We then generalize the result to both $\mathbb{G}_1$ and $\mathbb{G}_2$ and apply it to different pairing-friendly families of curves. This gives a simple and shared framework to prove membership tests for both cryptographic subgroups.

1 Introduction

A pairing is a bilinear map from two groups $\mathbb{G}_1, \mathbb{G}_2$ into a target group $\mathbb{G}_T$ and is available on dedicated pairing-friendly elliptic curves. $\mathbb{G}_1$ corresponds to

* preprint version available on ePrint at https://eprint.iacr.org/2022/352 and HAL at https://hal.inria.fr/hal-03608264, SageMath verification script at https://gitlab.inria.fr/zk-curves/cofactor.

a subgroup of prime order r of the elliptic curve over a prime field $\mathbb{F}_q$, $\mathbb{G}_2$ is a distinct subgroup of points of order r, usually over some extension $\mathbb{F}_{q^k}$, and $\mathbb{G}_T$ is the target group in a finite field $\mathbb{F}_{q^k}$, where k is the embedding degree.

The choices of pairing-friendly curves of prime order over $\mathbb{F}_q$ are limited to the MNT curves (Miyaji, Nakabayashi, Takano) of embedding degree 3, 4, or 6, Freeman curves of embedding degree 10, and Barreto–Naehrig curves of embedding degree 12. Because of the new NFS variant of Kim and Barbulescu, Gaudry, and Kleinjung (TNFS), the discrete logarithm problem in extension fields $\mathrm{GF}(q^k)$ is not as hard as expected, and key sizes and pairing-friendly curve recommendations are now updated. In this new list of pairing-friendly curves, BN curves are no longer the best choice in any circumstances. The widely deployed curve is now the BLS12-381 curve: a Barreto–Lynn–Scott curve of embedding degree 12, with a subgroup of 255-bit prime order, defined over a 381-bit prime field. The parameters of this curve have a polynomial form, and in particular, the cofactor has a square term: $c_1(x) = (x-1)^2/3$ were x is the seed $-(2^{63} + 2^{62} + 2^{60} + 2^{57} + 2^{48} + 2^{16})$.

One important cryptographic operation is to hash from a (random) string to a point on the elliptic curve. This operation has two steps: first mapping a string to a point $P(x, y)$ on the curve, then multiplying the point by the cofactor so that it falls into the cryptographic subgroup. For the first step, there is the efficient Elligator function for curves with j-invariant not 0 nor 1728 and having a point of order 4. For other curves including BLS curves of j-invariant 0, Wahby and Boneh propose an efficient map in [14]. Because the BLS12-381 curve is not of prime order, the point is multiplied by the cofactor c_1 to ensure the hash function to map into the cryptographic subgroup of 255-bit prime order. Wahby and Boneh wrote in [14] that it is sufficient to multiply by $(x-1)$, instead of the cofactor $(x-1)^2/3$. They observed that for any prime factor ℓ of $(x-1)$, the BLS12-381 curve has no point of order ℓ^2. Finally in [8] the authors show that for all BLS curves, the curve cofactor contains the square form $(x-1)^2/3$ and it is enough to multiply by $(x-1)$ to clear this factor, instead of $(x-1)^2/3$, thanks to a theorem of Schoof [11].

Other pairing-friendly curves are investigated to replace the BN curves, and at CANS'2020, Clarisse, Duquesne and Sanders revisited Brezing-Weng curves and showed that curves of embedding degree 13 and 19 are competitive for fast operations on the curve (in the first group $\mathbb{G}_1$). Again, a fast multiplication by the curve cofactor is important to provide a fast hashing to the curve.

Another important operation is to test whether a given point belongs to the right subgroup of order r, i.e. $\mathbb{G}_1$ or $\mathbb{G}_2$. This is a crucial operation to avoid small subgroups attacks. In late 2021, Scott in the preprint [12] investigated subgroup membership testing in $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ for BLS12 curves and discussed the generalization of the results to other BLS curves. Given a point on a curve $E(\mathbb{F}_q)$ or on a degree-d twisted curve E' defined over an extension of degree k/d, the question is whether the point is of prime order r. This test can be done much faster if an efficient endomorphism is available, which is usually the case for pairing-friendly curves. Budrato and Pintore showed that computing a general formula of the eigenvalue modulo the cofactor is not always well-defined at all primes [6].

Contributions. In this paper, we first apply El Housni and Guillevic technique [8] for cofactor clearing to other pairing-friendly constructions listed in the taxonomy paper of Freeman, Scott and Teske [9]. We show that it applies to many polynomial families: all curves of the constructions numbered 6.2 to 6.7, except for the cases $k \equiv 2, 3 \bmod 6$ of Construction 6.6 that generalizes the BLS curves. We provide a SageMath verification script at

`https://gitlab.inria.fr/zk-curves/cofactor`

Next, we fix a proof argument in the paper [12] for $\mathbb{G}_2$ membership test and generalize the result. This gives a simple and shared framework to prove both $\mathbb{G}_1$ and $\mathbb{G}_2$ membership tests.

Organization of the paper. Section 2 provides preliminaries on pairing-friendly curves and associated subgroups and endomorphisms. In Section 3, we investigate the cofactor clearing technique for different polynomial constructions in [9]. In Section 4, we revisit some previously known results on subgroup membership and propose a simple criterion for these tests. We conclude in Section 5.

2 Preliminaries

Let E be an elliptic curve $y^2 = x^3 + ax + b$ defined over a field $\mathbb{F}_q$, where q is a prime or a prime power. Let π_q be the Frobenius endomorphism:

$$\begin{aligned} \pi_q : E(\overline{\mathbb{F}_q}) &\to E(\overline{\mathbb{F}_q}) \\ (x, y) &\mapsto (x^q, y^q) \quad (\text{and } \mathcal{O} \mapsto \mathcal{O}) \ . \end{aligned}$$

Its minimal polynomial is $X^2 - tX + q$ where t is called the *trace*. Let r be a prime divisor of the curve order $\#E(\mathbb{F}_q) = q + 1 - t = c_1 r$. The r-torsion subgroup of E is denoted $E[r] \coloneqq \{P \in E(\overline{\mathbb{F}_q}), [r]P = \mathcal{O}\}$ and has two subgroups of order r (eigenspaces of π_q in $E[r]$) that are useful for pairing applications. We define the two groups $\mathbb{G}_1 = E[r] \cap \ker(\pi_q - [1])$, and $\mathbb{G}_2 = E[r] \cap \ker(\pi_q - [q])$. The group $\mathbb{G}_2$ is defined over $\mathbb{F}_{q^k}$, where the embedding degree k is the smallest integer $k \in \mathbb{N}^*$ such that $r \mid q^k - 1$. A pairing e is a bilinear map $\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ where $\mathbb{G}_T$ is the *target* group of r-th roots of unity in $\mathbb{F}_{q^k}$.

It is also important to recall some results with respect to the complex multiplication (CM) discriminant $-D$. When $D = 3$ (resp. $D = 4$), the curve has CM by $\mathbb{Q}(\sqrt{-3})$ (resp. $\mathbb{Q}(\sqrt{-1})$) so that twists of degrees 3 and 6 exist (resp. 4). When E has d-th order twists for some $d \mid k$, then $\mathbb{G}_2$ is isomorphic to $E'[r](\mathbb{F}_{q^{k/d}})$ for some twist E'. Otherwise, in the general case, E admits a single twist (up to isomorphism) and it is of degree 2. We denote c_2 the $\mathbb{G}_2$ cofactor, *i.e* $\#E'(\mathbb{F}_{q^{k/d}}) = c_2 r$.

When $D = 3$, the curve has a j-invariant 0 and is of the form $y^2 = x^3 + b$ ($a = 0$). In this case, an efficient endomorphism ϕ exist on $\mathbb{G}_1$. Given β a cube root of unity in $\mathbb{F}_q$,

$$\begin{aligned}\phi : E(\mathbb{F}_q)[r] &\to E(\mathbb{F}_q)[r] \\ (x, y) &\mapsto (\beta x, y) \quad (\text{and}\, \mathcal{O} \mapsto \mathcal{O}) \ .\end{aligned}$$

ϕ has a minimal polynomial $X^2 + X + 1$ and an eigenvalue λ satisfying $\lambda^2 + \lambda + 1 \equiv 0 \mod r$. When $D = 1$, the curve has j-invariant 1728 and is of the form $y^2 = x^3 + ax$ ($b = 0$). In this case an efficient endomorphism σ exist on $\mathbb{G}_1$. Given $i \in \mathbb{F}_q$ such that $i^2 = -1$,

$$\begin{aligned}\sigma : E(\mathbb{F}_q)[r] &\to E(\mathbb{F}_q)[r] \\ (x, y) &\mapsto (-x, iy) \quad (\text{and}\, \mathcal{O} \mapsto \mathcal{O}) \ .\end{aligned}$$

On $\mathbb{G}_2$, an efficient endomorphism is ψ the "untwist-Frobenius-twist" introduced in [10]. ψ has a minimal polynomial $X^2 - tX + q$ and is defined by

$$\begin{aligned}\psi : E'[r](\mathbb{F}_{q^{k/d}}) &\to E'[r](\mathbb{F}_{q^{k/d}}) \\ (x, y) &\mapsto \xi^{-1} \circ \pi_q \circ \xi(x, y) \quad (\text{and}\, \mathcal{O} \mapsto \mathcal{O}) \ .\end{aligned}$$

where ξ is the twisting isomorphism from E' to E. When $D = 3$, there are actually two sextic twists, one with $q + 1 - (-3f + t)/2$ points on it, the other with $q + 1 - (3f + t)/2$, where $f = \sqrt{(4q - t^2)/3}$. Only one of these is the "right" twist, i.e. has an order divisible by r. Let ν be a quadratic and cubic non-residue in $\mathbb{F}_{q^{k/d}}$ and $X^6 - \nu$ an irreducible polynomial, the "right" twist is either $y^2 = x^3 + b/\nu$ (D-type twist) or $y^2 = x^3 + b\nu$ (M-type twist). For the D-type, $\xi : E' \to E : (x, y) \mapsto (\nu^{1/3} x, \nu^{1/2} y)$ and ψ becomes

$$\psi : (x, y) \mapsto (\nu^{(q-1)/3} x^q, \nu^{(q-1)/2} y^q) \quad (\text{and}\, \mathcal{O} \mapsto \mathcal{O}) \ .$$

For the M-type, $\xi : E' \to E : (x, y) \mapsto (\nu^{2/3} x/\nu, \nu^{1/2} y/\nu)$ and ψ becomes

$$\psi : (x, y) \mapsto (\nu^{(-q+1)/3} x^q, \nu^{(-q+1)/2} y^q) \quad (\text{and}\, \mathcal{O} \mapsto \mathcal{O}) \ .$$

For other d-twisting ξ formulae, see [13].

Most of pairing-friendly curves fall into polynomial families, *i.e.* the curves parameters are expressed as polynomials $q(x), r(x)$ and $t(x)$. These polynomials are then evaluated in a "seed" u to derive a given curve (cf. Sec. 3).

3 Polynomial families of pairing-friendly curves, and faster co-factor clearing

3.1 Faster co-factor clearing

We recall the result on cofactor clearing from [8]. Let $\mathrm{End}_{\mathbb{F}_q}(E)$ denote the ring of $\mathbb{F}_q$-endomorphisms of E, let $\mathcal{O}$ denotes a complex quadratic order of the ring of integers of a complex quadratic number field, and $\mathcal{O}(\Delta)$ denotes the complex quadratic order of discriminant Δ.

Theorem 1 ([11, Proposition 3.7]). *Let E be an elliptic curve over $\mathbb{F}_q$ and $n \in \mathbb{Z}_{\geq 1}$ with $q \nmid n$. Let π_q denote the Frobenius endomorphism of E of trace t. Then,*

$$E[n] \subset E(\mathbb{F}_q) \iff \begin{cases} n^2 \mid \#E(\mathbb{F}_q), \\ n \mid q-1 \text{ and} \\ \pi_q \in \mathbb{Z} \text{ or } \mathcal{O}\big(\frac{t^2-4q}{n^2}\big) \subset \mathrm{End}_{\mathbb{F}_q}(E). \end{cases}$$

We will apply this theorem to the polynomial families of the taxonomy paper of Freeman, Scott and Teske [9]. The families are designed for specific discriminants $D = 1$ for constructions 6.2, 6.3 and 6.4, $D = 3$ for construction 6.6 and some of the KSS families, $D = 2$ for construction 6.7. First we identify a common cofactor within the family which has a square factor, then we compute its gcd with $q(x) - 1$ and $y(x)$. We summarize our results in the following tables and provide a SageMath verification script at `https://gitlab.inria.fr/zk-curves/cofactor`.

3.2 Construction 6.6

The family of pairing-friendly BLS curves appeared in [2]. A BLS curve can have an embedding degree k multiple of 3 but not 18. Common examples are $k = 9, 12, 15, 24, 27, 48$. A generalization was given in [9] and named Construction 6.6. Let k be a positive integer with $k \leq 1000$ and $18 \nmid k$. Construction 6.6 is given in Table 1. Then (t, r, q) parameterizes a complete family of pairing-friendly curves with embedding degree k and discriminant 3. Next, in Table 2, we compute the cofactor polynomial $c_1(x)$ for Construction 6.6 family. We recall that $y(x)$ satisfies the Complex Multiplication equation $4q(x) = t(x)^2 + Dy(x)^2$. To prove the results of Table 2, we will need Lemmas 1, 2, 3, and 4.

Table 1. Construction 6.6 from [9, §6], formulas for $k = 9, 15 \bmod 18$ from ePrint.

k	$r(x)$	$t(x)$	$y(x)$	$q(x)$	$x \bmod 3$
$1 \bmod 6$	$\Phi_{6k}(x)$	$-x^{k+1} + x + 1$	$(-x^{k+1} + 2x^k - x - 1)/3$	$(x+1)^2(x^{2k} - x^k + 1)/3 - x^{2k+1}$	2
$2 \bmod 6$	$\Phi_{3k}(x)$	$x^{k/2+1} - x + 1$	$(x^{k/2+1} + 2x^{k/2} + x - 1)/3$	$(x-1)^2(x^k - x^{k/2} + 1)/3 + x^{k+1}$	1
$3 \bmod 18$	$\Phi_{2k}(x)$	$x^{k/3+1} + 1$	$(-x^{k/3+1} + 2x^{k/3} + 2x - 1)/3$	$(x^2 - x + 1)^2(x^{2k/3} - x^{k/3} + 1)/3 + x^{k/3+1}$	2
$9, 15 \bmod 18$	$\Phi_{2k}(x)$	$-x^{k/3+1} + x + 1$	$(-x^{k/3+1} + 2x^{k/3} - x - 1)/3$	$(x+1)^2(x^{2k/3} - x^{k/3} + 1)/3 - x^{2k/3+1}$	2
$4 \bmod 6$	$\Phi_{3k}(x)$	$x^3 + 1$	$(x^3 - 1)(2x^{k/2} - 1)/3$	$(x^3 - 1)^2(x^k - x^{k/2} + 1)/3 + x^3$	1
$5 \bmod 6$	$\Phi_{6k}(x)$	$x^{k+1} + 1$	$(-x^{k+1} + 2x^k + 2x - 1)/3$	$(x^2 - x + 1)(x^{2k} - x^k + 1)/3 + x^{k+1}$	2
$0 \bmod 6$	$\Phi_k(x)$	$x + 1$	$(x-1)(2x^{k/6} - 1)/3)$	$(x-1)^2(x^{k/3} - x^{k/6} + 1)/3 + x$	1

Lemma 1. *Over the field of rationals $\mathbb{Q}$, $\Phi_d(x)$ denotes the d-th cyclotomic polynomial, and for all the distinct divisors d of n including 1 and n,*

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x) \ . \qquad (1)$$

Lemma 2. *For any odd $k \geq 1$ not multiple of 3 ($k \equiv 1, 5 \bmod 6$), we have*

$$x^2 - x + 1 \mid x^{2k} - x^k + 1 \ . \tag{2}$$

Proof (of Lemma 2). By Lemma 1, $x^{6k}-1$ is a multiple of $\Phi_1 = x-1$, $\Phi_2 = x+1$, $\Phi_3 = x^2+x+1$ and $\Phi_6 = x^2-x+1$. Since

$$x^{6k} - 1 = (x^{3k}-1)(x^{3k}+1) = (x^k-1)(x^{2k}+x^k+1)(x^k+1)(x^{2k}-x^k+1)$$

and $\Phi_1\Phi_3 \mid x^{3k}-1$ but $\Phi_6 \nmid x^{3k}-1$ because k is odd, nor x^k+1 because k is not multiple of 3, then $\Phi_6 = x^2-x+1$ should divide the other term $x^{2k}-x^k+1$.

Lemma 3. *For any odd $k \geq 1$ such that ($k \equiv 1 \bmod 6$), we have*

$$x^2 - x + 1 \mid x^{k+1} - x + 1 \quad \text{ and } \quad x^2 - x + 1 \mid x^{k+1} - 2x^k + x + 1 \ . \tag{3}$$

Proof (of Lemma 3). Let $\omega, \overline{\omega} \in \mathbb{C}$ be the two primitive 6-th roots of unity that are the two roots of x^2-x+1. Since $k \equiv 1 \bmod 6$ and $\omega^6 = \overline{\omega}^6 = 1$, then $\omega^k = \omega$, $\overline{\omega}^k = \overline{\omega}$, $\omega^{k+1} = \omega^2$ and $\overline{\omega}^{k+1} = \overline{\omega}^2$. Then $\omega^{k+1} - \omega + 1 = \omega^2 - \omega + 1 = 0$ and $\overline{\omega}^{k+1} - \overline{\omega} + 1 = \overline{\omega}^2 - \overline{\omega} + 1 = 0$. Hence $\omega, \overline{\omega}$ are roots of $x^{k+1}-x+1$ and x^2-x+1 divides $x^{k+1}-x+1$. Similarly, $\omega^{k+1} - 2\omega^k + \omega + 1 = \omega^2 - 2\omega + \omega + 1 = 0$ and the same holds for $\overline{\omega}$. We conclude that x^2-x+1 divides $x^{k+1}-2x^k+x+1$.

Lemma 4. *For any odd $k \geq 1$ such that ($k \equiv 5 \bmod 6$), we have*

$$x^2 - x + 1 \mid x^{k+1} - 2x^k - 2x + 1 \ . \tag{4}$$

Proof (of Lemma 4). Let $\omega, \overline{\omega} \in \mathbb{C}$ be the two primitive 6-th roots of unity that are the two roots of x^2-x+1. Similarly as in the proof of Lemma 3, since $k \equiv 5 \bmod 6$ and $\omega^3 = -1$, $\omega^6 = 1$, then $\omega^{k+1} = 1$, $\omega^k = \omega^5 = -\omega^2$. Then $\omega^{k+1} - 2\omega^k - 2\omega + 1 = 1 - 2(-\omega^2) - 2\omega + 1 = 2\omega^2 - 2\omega + 2 = 0$. The same holds for $\overline{\omega}$, and we conclude that x^2-x+1 divides $x^{k+1}-2x^k-2x+1$.

Proof (of Table 2). For $k = 1 \bmod 6$, one computes

$$\begin{aligned} q(x) + 1 - t(x) =& (x+1)^2(x^{2k}-x^k+1)/3 - x^{2k+1} + 1 - (-x^{k+1}+x+1) \\ =& (x+1)^2(x^{2k}-x^k+1)/3 - x(x^{2k}-x^k+1) \\ =& (x^{2k}-x^k+1)(x^2-x+1)/3 \ . \end{aligned}$$

Table 2. Cofactors of Construction 6.6 families

k	$q(x)+1-t(x)$	$c_0(x)$	$\gcd(c_0(x), q(x)-1)$	$\gcd(c_0(x), y(x))$
$1 \bmod 6$	$(x^{2k}-x^k+1)(x^2-x+1)/3$	$(x^2-x+1)^2/3$	x^2-x+1	$(x^2-x+1)/3$
$2 \bmod 6$	$(x^k-x^{k/2}+1)(x^2+x+1)/3$	$(x^2+x+1)/3$	1	1
$3 \bmod 18$	$(x^{2k/3}-x^{k/3}+1)(x^2-x+1)^2/3$	$(x^2-x+1)^2/3$	1	1
$9 \bmod 18$	$(x^{2k/3}-x^{k/3}+1)(x^2-x+1)/3$	$(x^2-x+1)/3$	1	1
$15 \bmod 18$	$(x^{2k/3}-x^{k/3}+1)(x^2-x+1)/3$	$(x^2-x+1)^2/3$	1	1
$4 \bmod 6$	$(x^k-x^{k/2}+1)(x^3-1)^2/3$	$(x^3-1)^2/3$	x^3-1	$(x^3-1)/3$
$5 \bmod 6$	$(x^{2k}-x^k+1)(x^2-x+1)/3$	$(x^2-x+1)^2/3$	x^2-x+1	$(x^2-x+1)/3$
$0 \bmod 6$	$(x^{k/3}-x^{k/6}+1)(x-1)^2/3$	$(x-1)^2/3$	$x-1$	$(x-1)/3$

By Lemma 2, (x^2-x+1) divides $x^{2k}-x^k+1$ since $k \equiv 1 \bmod 6$. Note that for $x \equiv 2 \bmod 3$, $x^2-x+1 \equiv 0 \bmod 3$. Hence the cofactor is a multiple of $c_0(x) = (x^2-x+1)^2/3$. Next, one computes

$$\begin{aligned} q(x)-1 = & \underbrace{(x+1)^2}_{=(x^2-x+1)+3x} (x^{2k}-x^k+1)/3 - x^{2k+1} - 1 \\ =&(x^2-x+1)(x^{2k}-x^k+1)/3 + x(x^{2k}-x^k+1) - x^{2k+1} - 1 \\ =&(x^2-x+1)(x^{2k}-x^k+1)/3 - (x^{k+1}-x+1) \end{aligned}$$

and by Lemma 3, x^2-x+1 divides $x^{k+1}-x+1$. We computed the derivative of $q(x)-1$ and checked that none of $\omega, \overline{\omega}$ is a zero of the derivative. Finally, x^2-x+1 divides $q(x)-1$ with multiplicity one. To conclude, Lemma 3 ensures that (x^2-x+1) divides $y(x)$, and we checked that the derivative of $y(x)$ does not vanish at a primitive sixth root of unity, hence x^2-x+1 divides $y(x)$ with multiplicity one.

For $k = 2 \bmod 6$, one computes

$$\begin{aligned} q(x)+1-t(x) =&(x-1)^2(x^k-x^{k/2}+1)/3 + x^{k+1} + 1 - (x^{k/2+1}-x+1) \\ =&(x^2-2x+1)(x^k-x^{k/2}+1)/3 + x(x^k-(x^{k/2}+1) \\ =&(x^k-x^{k/2}+1)(x^2+x+1)/3 \end{aligned}$$

Note that k is even. Lemma 2 will apply for $k' = k/2$ to be odd, that is $k \equiv 2 \bmod 12$. Nevertheless the cofactor $c_0(x)$ will not be a square. We checked that none of the primitive cubic and sextic roots of unity are roots of $q(x)-1$ nor $y(x)$, hence the gcd of $c_0(x)$ and $q(x)-1$, resp. $y(x)$, is 1.

For $k = 3 \bmod 18$, it is straightforward to get $q(x)+1-t(x) = (x^2-x+1)^2(x^{2k/3}-x^{k/3}+1)/3$, the cofactor $c_0(x) = (x^2-x+1)^2/3$ is a square as for $k = 1 \bmod 6$. For $k = 9, 15 \bmod 18$, we compute

$$\begin{aligned} q(x)+1-t(x) =&(x+1)^2(x^{2k/3}-x^{k/3}+1)/3 - x^{2k/3+1} + 1 - (-x^{k/3+1}+x+1) \\ =&(x^2+2x+1)(x^{2k/3}-x^{k/3}+1)/3 - x(x^{2k/3}-x^{k/3}+1) \\ =&(x^2-x+1)(x^{2k/3}-x^{k/3}+1)/3 \end{aligned}$$

For $k = 9 \bmod 18$, $k/3$ is a multiple of 3 and x^2-x+1 does not divide $(x^{2k/3}-x^{k/3}+1)$, while for $k = 15 \bmod 18$, $k/3$ is co-prime to 6, and $(x^{2k/3}-x^{k/3}+1)$ is a multiple of (x^2-x+1) by Lemma 2. For $k \equiv 3, 9, 15 \bmod 18$, we checked that neither $q(x)-1$ nor $y(x)$ have a common factor with $c_0(x)$, and no faster co-factor clearing is available.

For $k \equiv 4, 0 \bmod 6$, the calculus is similar to the case $k \equiv 1 \bmod 6$, and for $k \equiv 5 \bmod 6$, we use Lemma 4 to conclude about $y(x)$.

For the cases $k \equiv 2 \mod 6$ and $k \equiv 9 \mod 18$, $c_1(x)$ has no square factor and thus the cofactor clearing is already optimised. For $k \equiv 3, 15 \bmod 18$, the cofactor is a square but Theorem 1 does not apply. For all remaining cases, $c_1(x) = n(x)^2/3$ for some polynomial factor $n(x)/3$ that satisfies Theorem 1.

Hence, it is sufficient to multiply by $n(x)$ to clear the cofactor on Construction 6.6 curves. We summarize our results in Theorem 2.

Theorem 2. *For $k \equiv 1, 5 \bmod 6$, the curve cofactor has a factor $c_0(x) = (x^2 - x + 1)^2/3$, whose structure is $\mathbb{Z}/(x^2 - x + 1)/3\mathbb{Z} \times \mathbb{Z}/(x^2 - x + 1)\mathbb{Z}$, and it is enough to multiply by $n(x) = (x^2 - x + 1)$ to clear the co-factor $c_0(x)$.*

For $k \equiv 4 \bmod 6$, the curve cofactor has a factor $c_0(x) = (x^3 - 1)^2/3$, whose structure is $\mathbb{Z}/(x^3-1)/3\mathbb{Z} \times \mathbb{Z}/(x^3-1)\mathbb{Z}$, and it is enough to multiply by $n(x) = (x^3 - 1)$ to clear the co-factor $c_0(x)$.

For $k \equiv 0 \bmod 6$, the curve cofactor has a factor $c_0(x) = (x - 1)^2/3$, whose structure is $\mathbb{Z}/(x - 1)/3\mathbb{Z} \times \mathbb{Z}/(x - 1)\mathbb{Z}$, and it is enough to multiply by $n(x) = (x - 1)$ to clear the co-factor $c_0(x)$.

Proof (of Th. 2). From Table 2, $k = 1, 5 \bmod 6$ has $n(x) = (x^2 - x + 1)/3$, $k = 4 \bmod 6$ has $n(x) = (x^3 - 1)/3$, $k = 0 \bmod 6$ has $n(x) = (x - 1)/3$ where $n(x)$ satisfies the conditions of Th. 1. The n-torsion is $\mathbb{F}_q$-rational, that is $E[n] \subset E(\mathbb{F}_q)$ and has structure $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ over $\mathbb{F}_q$. Taking into account the co-factor 3, the structure of the subgroup of order $c_0(x) = 3n^2(x)$ is $\mathbb{Z}/3n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ and multiplying by $3n(x)$ clears the cofactor.

Example. In [7], Clarisse, Duquesne and Sanders introduced two new pairing-friendly curves with optimal $\mathbb{G}_1$, the curves BW13-P310 with seed $u = -\texttt{0x8b0}$ and BW19-P286 with seed $v = -\texttt{0x91}$. They fall in Construction 6.6 with $k = 1 \bmod 6$. Our faster co-factor clearing method applies.

For BW13-P310, the prime subgroup order is $r = \Phi_{6\cdot 13}(u) = (u^{26} - u^{13} + 1)/(u^2-u+1)$. The cofactor is $(u^2-u+1)^2/3$, where (u^2-u+1) divides $q(u)-1$ and $(u^2 - u + 1)/3$ divides $y(u)$. It is enough to multiply by $(u^2 - u + 1)$ to clear the cofactor.

For BW19-P286, the prime subgroup order is $r = \Phi_{6\cdot 19}(v) = (v^{38} - v^{19} + 1)/(v^2-v+1)$. The cofactor is $(v^2-v+1)^2/3$, where (v^2-v+1) divides $q(v)-1$ and $(v^2 - v + 1)/3$ divides $y(v)$. It is enough to multiply by $(v^2 - v + 1)$ to clear the cofactor.

3.3 Constructions 6.2, 6.3, 6.4, and 6.5 with $D = 1$

The constructions with numbers 6.2 to 6.5 have discriminant $D = 1$, we report the polynomial forms of the parameters in Table 3. The cofactor $c_1(x)$ in $q(x) + 1 - t(x) = r(x)c_1(x)$ has always a factor $c_0(x)$ that we report in Table 4, with special cases for $k = 2$ and $k = 4$. For $q(x)$ to be an integer, $x \equiv 1 \bmod 2$ is required, except for 6.5 where x is required to be even.

Lemma 5. *For any odd $k \geq 1$ we have*

$$x^2 + 1 \mid x^{2k} + 1 \ . \tag{5}$$

Explicitly,

$$x^{2k} + 1 = (x^2 + 1)(1 - x^2 + x^4 - \ldots + \ldots - x^{2k-4} + x^{2k-2}) \ . \tag{6}$$

Table 3. Constructions 6.2, 6.3, 6.4, and 6.5 from [9, §6]

	k	$r(x)$	$t(x)$	$y(x)$	$q(x)$
6.2	1 mod 2	$\Phi_{4k}(x)$	$-x^2+1$	$x^k(x^2+1)$	$(x^{2k+4}+2x^{2k+2}+x^{2k}+x^4-2x^2+1)/4$
6.3	2 mod 4	$\Phi_{2k}(x)$	x^2+1	$x^{k/2}(x^2-1)$	$(x^{k+4}-2x^{k+2}+x^k+x^4+2x^2+1)/4$
6.4	4 mod 8	$\Phi_k(x)$	$x+1$	$x^{k/4}(x-1)$	$(x^{k/2+2}-2x^{k/2+1}+x^{k/2}+x^2+2x+1)/4$
6.5	$k=10$	$\Phi_{20}(x)$	$-x^6+x^4-x^2+2$	$x^3(x^2-1)$	$(x^{12}-x^{10}+x^8-5x^6+5x^4-4x^2+4)/4$

Table 4. Cofactors of Constructions 6.2, 6.3, 6.4, and 6.5. Note that $x \equiv 1 \bmod 2$ except for 6.5 where $x \equiv 0 \bmod 2$.

	k	$c_0(x)$	$\gcd(c_0(x), q(x)-1)$	$\gcd(c_0(x), y(x))$
6.2	1 mod 2	$(x^2+1)^3/4$	x^2+1	x^2+1
6.3	$k=2$	$(x^2-1)^2/2$	x^2-1	x^2-1
6.3	2 mod 4, $k>2$	$(x^2-1)^2(x^2+1)/4$	x^2-1	x^2-1
6.4	$k=4$	$(x-1)^2/2$	$x-1$	$x-1$
6.4	4 mod 8, $k>4$	$(x-1)^2(x^2+1)/4$	$x-1$	$x-1$
6.5	$k=10$	$x^4/4$	x^2	x^3

Proof. By Lemma 1, $x^{4k}-1$ is a multiple of $\Phi_1 = x-1$, $\Phi_2 = x+1$ and $\Phi_4 = x^2+1$. Since $x^{4k}-1 = (x^{2k}-1)(x^{2k}+1)$ and $\Phi_1\Phi_2 \mid x^{2k}-1$ but $\Phi_4 \nmid x^{2k}-1$ because k is odd, then $\Phi_4 = x^2+1$ should divide the other term $x^{2k}+1$.

Proof (of Table 4). All families of constructions 6.2 to 6.5 have j-invariant 1728, an a point of order 2 (their order is even).

In Construction 6.2 one has k odd. One gets $q(x)+1-t(x) = (x^2+1)^2(x^{2k}+1)/4$, and by Lemma 5, x^2+1 is a factor of $x^{2k}+1$, hence $c_0(x) = (x^2+1)^3/4$ which is even, divides $q(x)+1-t(x)$. The factorization of $q(x)-1$ is

$$\begin{aligned}
q(x)-1 =&(x^{2k}(x^2+1)^2+(x^2-1)^2)/4-1\\
=&((x^4+2x^2+1)x^{2k}+(x^4-2x^2+1)-4)/4\\
=&((x^4-1)x^{2k}+(2x^2+2)x^{2k}+(x^4-1)-2x^2-2)/4\\
=&((x^4-1)(x^{2k}+1)+2(x^2+1)(x^{2k}-1))/4\\
=&(x^4-1)(x^{2k}+1+2a(x))/4 \text{ where}\\
a(x) =&(x^{2k}-1)/(x^2-1) = 1+x^2+x^4+\ldots+x^{2k-2} = \sum_{i=0}^{k-1} x^{2i}
\end{aligned}$$

and by Lemma 1, $x^{2k}-1$ is a multiple of $x^2-1 = \Phi_1\Phi_2$, and $(x^4-1)/2$ divides $q(x)-1$. More precisely, because x is odd, $4 \mid q(x)-1$, and

$$q(x)-1 = 2\underbrace{(x^2+1)}_{\text{even}}\underbrace{(x^2-1)/4}_{\in\mathbb{Z}}\underbrace{(x^{2k}+1+2a(x))/2}_{\in\mathbb{Z}}\ .$$

As a consequence, x^2+1 divides $q(x)-1$. Finally, $y(x) = x^k(x^2+1)$ is a multiple of x^2+1.

We isolate the case $k = 2$ in Construction 6.3, with parameters $r(x) = \Phi_4(x) = x^2+1$ (even), $t(x) = x^2+1$, $y(x) = x(x^2-1)$, $q(x) = (x^6-x^4+3x^2+1)/4$, $q(x)+1-t(x) = (x^2+1)(x^2-1)^2/4$. We set $r(x) = (x^2+1)/2$ and $c_1(x) = (x^2-1)^2/2$, $q(x)-1 = (x^2-1)(x^4+3)/4$ where $(x^4+3)/4$ is an integer. For larger $k = 2 \bmod 4$, one has

$$\begin{aligned}
q(x)+1-t(x) =&(x^{k+4} - 2x^{k+2} + x^k + x^4 + 2x^2 + 1)/4 + 1 - (x^2+1) \\
=&(x^k(x^2-1)^2 + (x^2+1)^2 - 4x^2)/4 \\
=&(x^k+1)(x^2-1)^2/4
\end{aligned}$$

and since k is even, by Lemma 5, x^2+1 divides x^k+1, hence $c_0(x) = (x^2+1)(x^2-1)^2/4$ divides the curve order. We compute $q(x)-1$ and factor it:

$$\begin{aligned}
q(x)-1 =&(x^k(x^2-1)^2 + (x^2+1)^2)/4 - 1 \\
=&(x^k(x^2-1)^2 + (x^2-1)^2 + 4x^2 - 4)/4 \\
=&(x^2-1)(x^k \underbrace{(x^2-1)}_{\text{mult. of 4}} + \underbrace{x^2-1}_{\text{mult. of 4}} + 4)/4
\end{aligned}$$

which proves that x^2-1 divides $q(x)-1$. Because $y(x) = x^{k/2}(x^2-1)$, it is obvious that x^2-1 divides $y(x)$.

With Construction 6.4, $k = 4 \bmod 8$. First $k = 4$ is a special case where the curve order is $q(x)+1-t(x) = (x-1)^2(x^2+1)/4$, the cofactor is $c_0(x) = (x-1)^2/2$, $r(x) = (x^2+1)/2$, $q(x)-1 = (x^2-1)(x^2-2x+3)/4$ factors as $q(x)-1 = (x-1)(x+1)/2(x^2-2x+3)/2$, and $y(x) = x(x-1)$.

For larger k, we compute, with $q(x) = (x^{k/2}(x-1)^2 + (x+1)^2)/4$,

$$\begin{aligned}
q(x)+1-t(x) =&(x^{k/2}(x-1)^2 + (x+1)^2)/4 + 1 - (x+1) \\
=&(x^{k/2}(x-1)^2 + x^2 + 2x + 1 - 4x)/4 \\
=&(x^{k/2}(x-1)^2 + (x-1)^2)/4 \\
=&(x-1)^2(x^{k/2}+1)/4
\end{aligned}$$

and because $k \equiv 4 \bmod 8$, $k/2$ is even and by Lemma 5, x^2+1 divides $x^{k/2}+1$, hence $c_0(x) = (x-1)^2(x^2+1)/4$ divides the curve order. Now we compute $q(x)-1$ and obtain the factorisation

$$\begin{aligned}
q(x)-1 =&(x^{k/2}(x-1)^2 + (x+1)^2)/4 - 1 \\
=&(x^{k/2}(x-1)^2 + x^2 - 2x + 1 + 4x - 4)/4 \\
=&(x^{k/2}(x-1)^2 + (x-1)^2 + 4(x-1))/4 \\
=&(x-1)(x^{k/2}(x-1) + (x-1) + 4)/4 \\
=&(x-1)(\underbrace{(x^{k/2}+1)(x-1)}_{\text{mult. of 4}} + 4)/4
\end{aligned}$$

hence $x-1$ divides $q(x)-1$. Finally $y(x) = x^{k/4}(x-1)$ and $(x-1)$ divides $y(x)$.

For construction 6.5, x is even this time, the curve order is $q(x)+1-t(x) = x^4/4(x^8-x^6+x^4-x^2+1)$, $y(x) = x^3(x^2-1)$, $q(x)-1 = x^2(x^{10}-x^8+x^6-5x^4+5x^2-4)/4$ were the factor $(x^{10}-x^8+x^6-5x^4+5x^2-4)/4$ is an integer whenever x is even.

From Table 4 and Theorem 1, we obtain Theorem 3.

Theorem 3. *For construction 6.2, the curve cofactor has a factor $c_0(x) = (x^2+1)^3/4$, whose structure is $\mathbb{Z}/(x^2+1)/2\mathbb{Z} \times \mathbb{Z}/(x^2+1)^2/2\mathbb{Z}$, and it is enough to multiply by $n(x) = (x^2+1)^2/2$ to clear the co-factor $c_0(x)$.*

For construction 6.3, the curve cofactor has a factor $c_0(x) = (x^2-1)^2(x^2+1)/4$, whose structure is $\mathbb{Z}/(x^2-1)/2\mathbb{Z}\times\mathbb{Z}/((x^2-1)(x^2+1)/2\mathbb{Z}$, and it is enough to multiply by $n(x) = (x^2-1)(x^2+1)/2$ to clear the co-factor $c_0(x)$.

For construction 6.4, the curve cofactor has a factor $c_0(x) = (x-1)^2(x^2+1)/4$, whose structure is $\mathbb{Z}/(x-1)/2\mathbb{Z} \times \mathbb{Z}/(x-1)(x^2+1)/2\mathbb{Z}$, and it is enough to multiply by $n(x) = (x-1)(x^2+1)/2$ to clear the co-factor $c_0(x)$.

For construction 6.5, the curve order has cofactor $c_0(x) = x^4/4$, whose structure is $\mathbb{Z}/x^2/2\mathbb{Z}\times\mathbb{Z}/x^2/2\mathbb{Z}$, and it is enough to multiply by $n(x) = x^2/2$ to clear the cofactor.

3.4 Construction 6.7 with $D = 2$

Construction 6.7 in [9] has discriminant $D = 2$. We report the polynomial forms of the parameters in Table 5. The cofactor $c_1(x)$ in $q(x)+1-t(x) = r(x)c_1(x)$ has always a factor $c_0(x)$ that we report in Table 6. For $q(x)$ to be an integer, $x \equiv 1 \bmod 2$ is required, and $x \equiv 1 \bmod 4$ for $k \equiv 0 \bmod 24$.

Table 5. Construction 6.7 from [9, §6].

6.7, $k = 0 \bmod 3$, $\ell = \mathrm{lcm}(8,k)$
$r(x) = \Phi_\ell(x)$
$t(x) = x^{\ell/k}+1$
$y(x) = (1-x^{\ell/k})(x^{5\ell/24}+x^{\ell/8}-x^{\ell/24})/2$
$q(x) = (2(x^{\ell/k}+1)^2+(1-x^{\ell/k})^2(x^{5\ell/24}+x^{\ell/8}-x^{\ell/24})^2)/8$

Table 6. Cofactor of Construction 6.7. Note that $x \equiv 1 \bmod 2$, except for $k \equiv 0 \bmod 24$, where $x \equiv 1 \bmod 4$.

	k	$c_0(x)$	$\gcd(c_0(x), q(x)-1)$	$\gcd(c_0(x), y(x))$
6.7	0 mod 3	$(x^{\ell/k}-1)^2/8$	$(x^{\ell/k}-1)/2$	$(x^{\ell/k}-1)/2$

Proof (of Table 6). We compute

$$\begin{aligned}q(x)+1-t(x) =&(2(x^{\ell/k}+1)^2+(1-x^{\ell/k})^2(x^{5\ell/24}+x^{\ell/8}-x^{\ell/24})^2)/8+1-(x^{\ell/k}+1)\\ =&(2(x^{\ell/k}+1)^2-8x^{\ell/k}+(1-x^{\ell/k})^2(x^{\ell/24}(x^{4\ell/24}+x^{2\ell/24}-1))^2)/8\\ =&(2(x^{\ell/k}-1)^2+(x^{\ell/k}-1)^2x^{\ell/12}(x^{\ell/6}+x^{\ell/12}-1)^2)/8\\ =&(x^{\ell/k}-1)^2(x^{\ell/12}(x^{\ell/6}+x^{\ell/12}-1)^2+2)/8\end{aligned}$$

and for $q(x)-1$ we obtain

$$\begin{aligned}q(x)-1 =&(2(x^{\ell/k}+1)^2-8+(x^{\ell/k}-1)^2(x^{\ell/12}(x^{\ell/6}+x^{\ell/12}-1)^2))/8\\ q(x)-1 =&(2(x^{\ell/k}-1)^2+8x^{\ell/k}-8+(x^{\ell/k}-1)^2(x^{\ell/12}(x^{\ell/6}+x^{\ell/12}-1)^2))/8\\ q(x)-1 =&(x^{\ell/k}-1)(8+(x^{\ell/k}-1)(2+x^{\ell/12}(x^{\ell/6}+x^{\ell/12}-1)^2)/8\end{aligned}$$

It is straightforward to see that $(x^{\ell/k}-1)/2$ divides $y(x)$.

From Table 6 and Theorem 1, we obtain Theorem 4.

Theorem 4. *For construction 6.7, let* $\ell = \mathrm{lcm}(k, 8)$. *The curve cofactor has a factor* $c_0(x) = (x^{\ell/k}-1)^2/8$, *whose structure is* $\mathbb{Z}/(x^{\ell/k}-1)/4\mathbb{Z}\times\mathbb{Z}/(x^{\ell/k}-1)/2\mathbb{Z}$, *and it is enough to multiply by* $n(x) = (x^{\ell/k}-1)/2$ *to clear the co-factor* $c_0(x)$.

3.5 Other constructions

We also investigated the KSS curves named Constructions 6.11, 6.12, 6.13, 6.14, 6.15 in [9], and the KSS-54 curve of 2018, but none of the cofactors is a square, and the gcd of the cofactor and $q(x)-1$, resp. $y(x)$, is equal to 1. Hence our faster co-factor clearing does not apply.

4 Subgroup membership testing

For completeness, we first state the previously known membership tests for $\mathbb{G}_1$ [12,5] and $\mathbb{G}_T$ [12,8,1] for BLS curves. Next, we show that the proof argument for the $\mathbb{G}_2$ test in [12] is incomplete and provide a fix and a generalization.

For the sequel, we recall that the curves of interest have a j-invariant 0 and are equipped with efficient endomorphisms ϕ on $\mathbb{G}_1$ and ψ on $\mathbb{G}_2$ (see Sec. 2).

4.1 $\mathbb{G}_1$ and $\mathbb{G}_T$ membership

Given a point $P \in E(\mathbb{F}_q)$, Scott [12, §6] proves by contradiction that for BLS12 curves it is sufficient to verify that $\phi(P) = -u^2P$ where $-u^2$ is the eigenvalue λ of ϕ. A similar test was already proposed in a preprint by Bowe [5, §3.2] for the BLS12-381: $((u^2-1)/3)(2\phi'(P)-P-\phi'^2(P))-\phi'^2(P) = \mathcal{O}$ (where ϕ' here is ϕ^2). This boils down to exactly $\phi(P) = -u^2P$ using $\phi^2(P)+\phi(P)+P = \mathcal{O}$ and $\lambda^2+\lambda+1 \equiv 0 \mod r$ ($u^4 \equiv u^2-1 \mod r$). However, the proof uses a tautological reasoning, as reproached by Scott [12, footnote p. 6], because it replaces λP by $\phi(P)$ where P is a point yet to be proven of order r.

For $w \in \mathbb{G}_T$ membership test, Scott [12] hinted that it is sufficient on BLS12 curves to verify that $w^{q^4-q^2+1} = 1$ (cyclotomic subgroup test) and that $w^q = w^u$. This was based on a personal communication with the authors of [8] who proved the proposition for any pairing- friendly curve. They also implemented this test for some BLS12 and BLS24 curves in [4] prior to Scott's pre-print. The same test also appears in [1] without a proof.

4.2 $\mathbb{G}_2$ membership

Following [12, Section 4], let $E(\mathbb{F}_q)$ be an elliptic curve of j-invariant 0 and embedding degree $k = 12$. Let E' be the sextic twist of E defined over $\mathbb{F}_{q^{k/d}} = \mathbb{F}_{q^2}$, and ψ the "untwist-Frobenius-twist" endomorphism with the minimal polynomial

$$\chi(X) = X^2 - tX + q \tag{7}$$

Let $Q \in E'(\mathbb{F}_{q^2})$. We have $\gcd(q + 1 - t, \#E'(\mathbb{F}_{q^2})) = r$. To check if Q is in $E'(\mathbb{F}_{q^2})[r]$, it is therefore sufficient to verify that

$$[q + 1 - t]Q = \mathcal{O}$$

Since $[q] = -\psi^2 + [t] \circ \psi$ from Eq. (7), the test to perform becomes

$$\psi \circ ([t]Q - \psi(Q)) + Q - [t]Q = 0 \ . \tag{8}$$

It is an efficient test since ψ is fast to evaluate and $[t]Q$ can be computed once and cheaper than $[r]Q$. For BLS12 curves $t = u + 1$ and the test to perform becomes in [12, Section 4] the quadratic equation

$$\psi(uQ) + \psi(Q) - \psi^2(Q) = uQ$$

So far, the only used fact is $\chi(\psi) = 0$, which is true everywhere. So the reasoning is correct and we have

$$\psi(uQ) + \psi(Q) - \psi^2(Q) = uQ \implies Q \in E'(\mathbb{F}_{q^2})[r]$$

However the preprint [12, Section 4] goes further and writes that the quadratic equation has only two solutions, $\psi(Q) = Q$ and $\psi(Q) = uQ$. Since ψ does not act trivially on $E'(\mathbb{F}_{q^2})$ the conclusion is

$$\psi(Q) = uQ \implies Q \in E'(\mathbb{F}_{q^2})[r] \tag{9}$$

The issue The previous property is, by luck, true as we will show later (Sec. 4.3). However, the overall reasoning is flawed, because it circles back to the fact that ψ acts as the multiplication by u on $\mathbb{G}_2$, while we are trying to prove that Q is in $\mathbb{G}_2$. This is the same kind of tautological reasoning reproached in the footnote of Scott's preprint [12]. This reasoning implicitly supposes ψ acts as the multiplication by u only on $E'(\mathbb{F}_{q^2})[r]$, and therefore that this action characterizes $E'(\mathbb{F}_{q^2})[r]$. However, $E'(\mathbb{F}_{q^2})[r]$ might not be the only subgroup of $E'(\mathbb{F}_{q^2})$ on which ψ has the eigenvalue u. Indeed, if a prime number ℓ divides the cofactor c_2 and $\chi(u) = 0 \bmod \ell$, it is possible that, on $E'(\mathbb{F}_{q^2})[\ell]$, ψ acts as the multiplication by u, for instance if $E'(\mathbb{F}_{q^2})[\ell]$ contains the eigenspace associated to u. So the implication (9) is true, provided that no such prime exists.

The solution The implication (9) becomes true if we know that there is no other subgroup of $E'(\mathbb{F}_{q^2})$ on which ψ acts as the multiplication by u. To make sure of this, it is enough to check that $\chi(u) \neq 0 \bmod \ell_i$ for all primes ℓ_i dividing c_2. If that is the case, we know that ψ acts as the multiplication by u only on $E'(\mathbb{F}_{q^2})[r]$. Using the Chinese Remainder Theorem it gives the following criterion:

Proposition 1 *If ψ acts as the multiplication by u on $E'(\mathbb{F}_{q^2})[r]$ and $\gcd(\chi(u), c_2) = 1$ then*

$$\psi(Q) = [u]Q \implies Q \in E'(\mathbb{F}_{q^2})[r] \ .$$

Note that checking the gcd of the polynomials $\chi(\lambda(X))$ and $c_2(X)$ is not sufficient and one needs to check the gcd of the integers, that are evaluations of the polynomials at u. In fact, $\gcd(\chi(\lambda(X)), c_2(X)) = 1$ in $\mathbb{Q}[X]$ only means that there is a relation $A\chi(\lambda) + Bc_2 = 1$ where $A, B \in \mathbb{Q}[X]$. The seeds u are chosen so that $\chi(\lambda(u)), c_2(u)$ are integers, but it might not be the case for $A(u)$ and $B(u)$. If d is the common denominator of the coefficients of A and B, we can only say that for a given seed u, $\gcd(\chi(u), c_2(u)) \mid d$. Therefore, we have to take care of the "exceptional seeds" u such that $\gcd(\chi(u), c_2(u))$ is a proper divisor of d.

4.3 A generalisation of $\mathbb{G}_1$ and $\mathbb{G}_2$ membership tests

Proposition 1 can be generalized to both $\mathbb{G}_1$ and $\mathbb{G}_2$ groups for any polynomial-based family of elliptic curves. Let $\tilde{E}(\mathbb{F}_{\tilde{q}})$ be a family of elliptic curves (i.e. it can be $E(\mathbb{F}_q)$ or $E'(\mathbb{F}_{q^{k/d}})$ for instance). Let $\mathbb{G}$ be a cryptographic group of $\tilde{E}$ of order r equipped with an efficient endomorphism $\tilde{\phi}$. It has a minimal polynomial $\tilde{\chi}$ and an eigenvalue $\tilde{\lambda}$. Let c be the cofactor of $\mathbb{G}$. Proposition 1 becomes then

Proposition 2 *If $\tilde{\phi}$ acts as the multiplication by $\tilde{\lambda}$ on $\tilde{E}(\mathbb{F}_{\tilde{q}})[r]$ and $\gcd(\tilde{\chi}(\tilde{\lambda}), c) = 1$ then*

$$\tilde{\phi}(Q) = [\tilde{\lambda}]Q \implies Q \in \tilde{E}(\mathbb{F}_{\tilde{q}})[r] \ .$$

Examples

Example 1 (BN[3]). Let $E(\mathbb{F}_{q(x)})$ define the BN pairing-friendly family. It is parameterized by

$$\begin{aligned} q(x) &= 36x^4 + 36x^3 + 24x^2 + 6x + 1 \\ r(x) &= 36x^4 + 36x^3 + 18x^2 + 6x + 1 \\ t(x) &= 6x^2 + 1 \end{aligned}$$

and $E(\mathbb{F}_{q(x)})$ has a prime order so $c_1 = 1$. The cofactor on the sextic twist $E'(\mathbb{F}_{q^2})$ is $c = c_2$

$$\begin{aligned} c_2(x) &= q(x) - 1 + t(x) \\ &= 36x^4 + 36x^3 + 30x^2 + 6x + 1 \ . \end{aligned}$$

On $\mathbb{G} = \mathbb{G}_2 = E'(\mathbb{F}_{q^2})[r]$, $\tilde{\phi} = \psi$ (the “untwist-Frobenius-twist”) has a minimal polynomial $\tilde{\chi} = \chi$ and an eigenvalue $\tilde{\lambda} = \lambda$

$$\begin{aligned} \chi &= X^2 - tX + q \\ \lambda &= 6X^2 \ . \end{aligned}$$

We have $\gcd(c_2, \chi(\lambda)) = \gcd(c_2(X), \chi(6X^2)) = 1$, and running the extended Euclidean algorithm we find a relation $Ac_2 + B\chi(\lambda) = 1$ where $A, B \in \mathbb{Q}[X]$. The common denominator of the coefficients of A and B is $d = 2$. We now look at the congruence relations the seed u should satisfy so that $\chi(\lambda(u))$ and $c_2(u)$ are both divisible by 2: those will be the exceptional seeds, under which the implication (9) could be false. Since c_2 is always odd there is no exceptional seeds and we obtain:

Proposition 3 *For the BN family, if $Q \in E'(\mathbb{F}_{q^2})$,*

$$\psi(Q) = [u]Q \implies Q \in E'(\mathbb{F}_{q^2})[r] \ .$$

Example 2 (BLS12[2]). The BLS12 parameters are:

$$\begin{aligned} q(x) &= (x-1)^2/3 \cdot r(x) + x \\ r(x) &= x^4 - x^2 + 1 \\ t(x) &= x + 1 \ . \end{aligned}$$

On $\mathbb{G} = \mathbb{G}_1 = E(\mathbb{F}_p)[r]$, the endomorphism $\tilde{\phi} = \phi$ has minimal polynomial $\tilde{\chi} = \chi$ and eigenvalue $\tilde{\lambda} = \lambda$ as follows:

$$\begin{aligned} \chi &= X^2 + X + 1 \\ \lambda &= -X^2 \ . \end{aligned}$$

We have $c = c_1 = (X-1)^2/3$. Running the extended Euclidean algorithm on c_1 and $\chi(\lambda)$, we find a relation $Ac_1 + B\chi(\lambda) = 1$ in $\mathbb{Q}[X]$. In fact, here A and B are in $\mathbb{Z}[X]$, so there are no exceptional cases: for any acceptable seed u, $\gcd(c_1(u), \chi(\lambda(u))) = 1$, so we retrieve the result from Scott's paper [12]:

Proposition 4 *For the BLS12 family, if $Q \in E(\mathbb{F}_p)$,*

$$\phi(Q) = [-u^2]Q \implies Q \in E(\mathbb{F}_p)[r] \ .$$

On $\mathbb{G} = \mathbb{G}_2 = E'(\mathbb{F}_{q^2})[r]$, $\tilde{\phi} = \psi$ (the "untwist-Frobenius-twist") has a minimal polynomial $\tilde{\chi} = \chi$ and an eigenvalue $\tilde{\lambda}$, where

$$\begin{aligned} \chi &= X^2 - tX + q \\ \lambda &= X \ . \end{aligned}$$

The $\mathbb{G}_2$ cofactor is $c = c_2$

$$c_2(x) = (x^8 - 4x^7 + 5x^6 - 4x^4 + 6x^3 - 4x^2 - 4x + 13)/9 \ .$$

We have $\gcd(c_2, \chi(\lambda)) = 1$ and running the extended Euclidean algorithm we find a relation $Ac_2 + B\chi(\lambda) = 1$ where $A, B \in \mathbb{Q}[X]$. The common denominator of the coefficients of A and B is $3 \cdot 181$. We look at what congruence properties the seed u should have so that $\chi(\lambda(u))$ and $c_2(u)$ are both divisible by 181 or 3 to rule out the exceptional cases (as before, with those seeds, the implication (9) could be false). We find that there is no seed u such that $3 \mid c_2(u)$. Furthermore, the seeds u such that $181 \mid \chi(\lambda(u))$ and $181 \mid c_2(u)$ are such that $u \equiv 7 \bmod 181$ and in that case, $181 \mid r(u)$. Therefore there are no exceptional cases as long as r is prime, and we obtain:

Proposition 5 *For the BLS12 family, if $r = r(u)$ is prime and $Q \in E'(\mathbb{F}_{q^2})$,*

$$\psi(Q) = [u]Q \implies Q \in E'(\mathbb{F}_{q^2})[r] \ .$$

Example 3 (BLS24[2]). The BLS24 family is parameterized by

$$\begin{aligned} q(x) &= (x-1)^2/3 \cdot r(x) + x \\ r(x) &= x^8 - x^4 + 1 \\ t(x) &= x + 1 \ . \end{aligned}$$

On $\mathbb{G} = \mathbb{G}_1 = E(\mathbb{F}_p)[r]$, the endomorphism $\tilde{\phi} = \phi$ has minimal polynomial $\tilde{\chi} = \chi$ and eigenvalue $\tilde{\lambda} = \lambda$, where

$$\begin{aligned} \chi &= X^2 + X + 1 \\ \lambda &= -X^4 \ . \end{aligned}$$

We have $c = c_1 = (X-1)^2/3$. Running the extended Euclidean algorithm on c_1 and $\chi(\lambda)$, we find a relation $Ac_1 + B\chi(\lambda) = 1$ in $\mathbb{Q}[X]$. As for BLS12, A and B are in $\mathbb{Z}[X]$, so there are no exceptional cases, and we have

Proposition 6 *For the BLS24 family, if $Q \in E(\mathbb{F}_p)$,*

$$\phi(Q) = [-u^4]Q \implies Q \in E(\mathbb{F}_p)[r] \ .$$

On $\mathbb{G} = \mathbb{G}_2 = E'(\mathbb{F}_{q^4})[r]$, $\tilde{\phi} = \psi$, the "untwist-Frobenius-twist" has a minimal polynomial $\tilde{\chi} = \chi$ and an eigenvalue $\tilde{\lambda} = \lambda$, where

$$\chi = X^2 - tX + q$$
$$\lambda = X \ .$$

The cofactor on the sextic twist $E'(\mathbb{F}_{q^4})$ is $c = c_2$

$$\begin{aligned} c_2(x) =&(x^{32} - 8x^{31} + 28x^{30} - 56x^{29} + 67x^{28} - 32x^{27} - 56x^{26} + 160x^{25} - 203x^{24} + 132x^{23} \\ &+ 12x^{22} - 132x^{21} + 170x^{20} - 124x^{19} + 44x^{18} - 4x^{17} + 2x^{16} + 20x^{15} - 46x^{14} + 20x^{13} \\ &+ 5x^{12} + 24x^{11} - 42x^{10} + 48x^9 - 101x^8 + 100x^7 + 70x^6 - 128x^5 + 70x^4 - 56x^3 \\ &- 44x^2 + 40x + 100)/81 \ . \end{aligned}$$

We have $\gcd(c_2, \chi(\lambda)) = 1$. Running the extended Euclidean algorithm on c_2 and $\chi(\lambda)$, we find a relation $Ac_2 + B\chi(\lambda) = 1$ where the common denominator of the coefficients of A and B is $3^5 \times 1038721$. As before, we find that there is no seed u such that $3 \mid c_2(u)$. Moreover, the seeds u such that $1038721 \mid c_2(u)$ and $1038721 \mid \chi(\lambda)$ are such that $u = 162316 \bmod 1038721$. In this case $1038721 \mid r(u)$ and hence there are no exceptional cases. We obtain:

Proposition 7 *For the BLS24 family, if $r = r(u)$ is prime and $Q \in E'(\mathbb{F}_{q^4})$, then*

$$\psi(Q) = [u]Q \implies Q \in E'(\mathbb{F}_{q^4})[r] \ .$$

5 Conclusion

Cofactor clearing and subgroup membership tests are two important operations in many pairing-based protocols. In this work, we generalized and proved a technique for cofactor clearing to many pairing-friendly constructions. We gave a simple criterion to prove both $\mathbb{G}_1$ and $\mathbb{G}_2$ membership tests after fixing an incomplete proof of a $\mathbb{G}_2$ test that was recently widely deployed in cryptographic libraries. These operations are now provably fast for different pairing-friendly curves which consequently speeds up many cryptographic protocols. This also gives more flexibility to find curves with nice properties at the expense of composite cofactors.

References

1. Aranha, D.F., Pagnin, E., Rodríguez-Henríquez, F.: LOVE a pairing. In: Longa, P., Ràfols, C. (eds.) LATINCRYPT 2021. LNCS, vol. 12912, pp. 320–340. Springer (2021). https://doi.org/10.1007/978-3-030-88238-9_16
2. Barreto, P.S.L.M., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: Cimato, S., Galdi, C., Persiano, G. (eds.) SCN 02. LNCS, vol. 2576, pp. 257–267. Springer, Heidelberg (Sep 2003). https://doi.org/10.1007/3-540-36413-7_19

3. Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer, Heidelberg (Aug 2006). https://doi.org/10.1007/11693383_22
4. Botrel, G., Piellard, T., Housni, Y.E., Tabaie, A., Kubjas, I.: Consensys/gnark-crypto (Feb 2022). https://doi.org/10.5281/zenodo.6092968, `https://doi.org/10.5281/zenodo.6092968`
5. Bowe, S.: Faster subgroup checks for BLS12-381. Cryptology ePrint Archive, Report 2019/814 (2019), `https://eprint.iacr.org/2019/814`
6. Budroni, A., Pintore, F.: Efficient hash maps to $\mathbb{G}_2$ on bls curves. ePrint `2017/419`
7. Clarisse, R., Duquesne, S., Sanders, O.: Curves with fast computations in the first pairing group. In: Krenn, S., Shulman, H., Vaudenay, S. (eds.) CANS 20. LNCS, vol. 12579, pp. 280–298. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-65411-5_14
8. El Housni, Y., Guillevic, A.: Families of SNARK-friendly 2-chains of elliptic curves. In: Dunkelman, O., Dziembowski, S. (eds.) Eurocrypt'2022. LNCS, Springer (2022), to appear, ePrint `2021/1359`
9. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. Journal of Cryptology **23**(2), 224–280 (Apr 2010). https://doi.org/10.1007/s00145-009-9048-z
10. Galbraith, S.D., Scott, M.: Exponentiation in pairing-friendly groups using homomorphisms. In: Galbraith, S.D., Paterson, K.G. (eds.) PAIRING 2008. LNCS, vol. 5209, pp. 211–224. Springer, Heidelberg (Sep 2008). https://doi.org/10.1007/978-3-540-85538-5_15
11. Schoof, R.: Nonsingular plane cubic curves over finite fields. Journal of Combinatorial Theory, Series A **46**(2), 183–211 (1987). https://doi.org/10.1016/0097-3165(87)90003-3
12. Scott, M.: A note on group membership tests for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on BLS pairing-friendly curves. ePrint `2021/1130`
13. Scott, M.: A note on twists for pairing friendly curves (2009), `http://indigo.ie/~mscott/twists.pdf`
14. Wahby, R.S., Boneh, D.: Fast and simple constant-time hashing to the BLS12-381 elliptic curve. IACR TCHES **2019**(4), 154–179 (2019). https://doi.org/10.13154/tches.v2019.i4.154-179