# Faster Subgroup Checks for BLS12-381

Sean Bowe
sean@z.cash
Electric Coin Company

**Abstract**

Pairing-friendly elliptic curve constructions provide two elliptic curve groups which are both of prime order $q$ and usually each have a nontrivial cofactor $h$. Due to the way these curves are typically constructed, endomorphisms can be applied to perform fast cofactor multiplication. However, cofactor multiplication is sometimes insufficient for dealing with cofactors, such as with malleability attacks.

In this brief note, we describe efficient techniques for checking that points exist within the correct $q$-order subgroups of the BLS12-381 elliptic curve construction, which is the focus of standardization for pairing-based protocols. Instead of multiplying by $q$ and comparing the point with the identity, we use endomorphisms to eliminate the $q$-torsion while modifying (but not killing) the $h$-torsion components. The result can then be compared against the identity.

## 1 Introduction

Pairing-friendly elliptic curves have become a crucial component of many modern cryptographic protocols. These curves submit groups $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$, each of prime order $q$, such that an efficiently computable pairing function $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ exists where

$$e([a]G, [b]H) = T^{ab}$$

for all $a, b \in \mathbb{F}_q$ and some fixed $G \in \mathbb{G}_1$, $H \in \mathbb{G}_2$ and $T \in \mathbb{G}_T$. This is achieved by choosing an elliptic curve $E(\mathbb{F}_p)$ that contains a large prime $q$-order subgroup, such that $q|p^k - 1$ for a small "embedding degree" $k$. We take $\mathbb{G}_1$ to be this subgroup of $E(\mathbb{F}_p)$, and we take $\mathbb{G}_2$ to be the $q$-order subgroup of its degree $d$ twist $E'(\mathbb{F}_{p^e})$ where $k = de$. The pairing function $e$ is a map into the $q$-order multiplicative subgroup of $\mathbb{F}_{p^k}$.

BLS12-381 is a pairing-friendly curve in the Barreto-Lynn-Scott (BLS) family[1], with embedding degree 12. Due to a mixture of performance and security tradeoffs it has become an increasing focus of standardization efforts. As an example, recently Wahby and Boneh[8] proposed a set of constructions for efficiently hashing to $\mathbb{G}_1$ and $\mathbb{G}_2$ in BLS12-381, which is a necessary component of the BLS signature scheme.[2] We will be focusing on this curve, although some of our results may be generally applicable.

### 1.1 Addressing Cofactors

As with many pairing-friendly curves, for BLS12-381 the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ have nontrivial cofactors $h_1$ and $h_2$, respectively. This gives rise to small subgroup attacks. This can be addressed by multiplying points by the cofactor to eliminate the $h$-torsion components. However, it does not address all possible attacks; for example, points cannot be expected to be canonical representatives of subgroup elements, which has led to malleability attacks in existing protocols.[4]

Therefore, it is prudent for curve implementations to check that points really exist within $\mathbb{G}_1$ and $\mathbb{G}_2$ as they are being decoded. However, the naive approach requires multiplying the point by $q$ and comparing it against the identity to see that it is in the $q$-order subgroup. Due to the size of $q$ (approximately 255 bits) this is not ideal, especially in the case of $\mathbb{G}_2$ due to the expensive group arithmetic.

It has been shown that cofactor multiplication can be achieved very efficiently for some families of pairing-friendly curves through the use of endomorphisms.[7] Building on this, we show that endomorphisms can be used to efficiently kill the $q$-torsion components of a point while only modifying (but not killing) the $h$-torsion components of the point. If the point was actually in the correct $q$-order subgroup, the result should be the identity.

## 2 Preliminaries

Our focus is on the BLS12-381 elliptic curve construction. This curve is parameterized by $z = -2^{16} - 2^{48} - 2^{57} - 2^{60} - 2^{62} - 2^{63}$ such that

$$\begin{aligned} p &= (z-1)^2(z^4 - z^2 + 1)/3 + z \\ q &= z^4 - z^2 + 1 \end{aligned}$$

where $\mathbb{F}_p$ is our base field, and the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ are of prime order $q$. We construct extension fields by towering

$$\begin{aligned} \mathbb{F}_{p^2} &= \mathbb{F}_p(u)/x^2 + 1 \\ \mathbb{F}_{p^6} &= \mathbb{F}_{p^2}(v)/x^3 + u + 1 \\ \mathbb{F}_{p^{12}} &= \mathbb{F}_{p^6}(w)/x^2 + v \end{aligned}$$

so that we obtain $E(\mathbb{F}_p) : y^2 = x^3 + 4$ and its sextic twist $E'(\mathbb{F}_{p^2}) : y^2 = x^3 + 4(u+1)$. $\mathbb{G}_1$ is the $q$-order subgroup of $E(\mathbb{F}_p)$, and $\mathbb{G}_2$ is the $q$-order subgroup of $E'(\mathbb{F}_{p^2})$. Let $h_1$ be the cofactor of $\mathbb{G}_1$ and $h_2$ be the cofactor of $\mathbb{G}_2$. For reference, the cofactor $h_1$ is relatively small (close to 64-bits) but the cofactor $h_2$ is much larger, as is typically the case.

The choice of $z$ with small Hamming weight is made deliberately to improve the performance of the pairing function, but for similar reasons it can also be used to accelerate group arithmetic through the use of endomorphisms. Let $\pi_p$ be the $p$-power Frobenius on $E$, and let $\phi$ be the twisting isomorphism from $E$ to $E'$. Galbraith and Scott[6] introduced the "untwist-Frobenius-twist" endomorphism $\psi = \phi^{-1}\pi_p\phi$ such that

$$\psi^2(P) - [t]\psi(P) + [p]P = \mathcal{O}$$

holds for all points $P \in E'(\mathbb{F}_{p^2})$, where $t$ is the trace of Frobenius on $E$. They proposed leveraging this endomorphism to perform more efficient cofactor multiplication for $\mathbb{G}_2$, which is especially useful due to the large size of $h_2$.

Later, Scott et al.[7] found that the parameterization of many pairing-friendly curves (together with the endomorphism $\psi$) could allow for even more efficient cofactor multiplication. Fuentes et al.[5] used a reduction technique to obtain trivial expressions over $\psi$ that effectively perform cofactor multiplication, and these techniques were extended to BLS curves by Budroni and Pintore.[3]

It is worth noting that the cofactor multiplication technique of Budroni and Pintore uses that a scalar $a$ can be extracted such that we can interpret $\psi(P)$ as being a multiplication map $[a]P$ for all $P \in E'(\mathbb{F}_{p^2})$; however, this is not the case in BLS12-381 due to subgroups in $E'(\mathbb{F}_{p^2})$ of order $13^2$ and $23^2$. However, their technique still works for BLS12-381 as the polynomial in $\psi$ has roots in $GF(13^2)$ and $GF(23^2)$ that correspond with the roots of $x^2 - tx + p$.

# 3 Fast Subgroup Checks

The typical approach for checking that a point $P$ exists within the correct prime $q$-order subgroup is to check that $[q]P = \mathcal{O}$. We propose to use endomorphisms to multiply the $q$-torsion components of $P$ by $q$ while not killing any $h$-torsion components of $P$. Thus, if the original point was in the $q$-order subgroup, the result should be $\mathcal{O}$.

## 3.1 Checking Subgroups in $\mathbb{G}_2$

Our first result is a technique for efficiently checking that $P$ exists within $\mathbb{G}_2$ by applying the endomorphism $\psi$, through the following check

$$[z]\psi^3(P) - \psi^2(P) + P = \mathcal{O}$$

where $z$ is the parameter of the BLS12-381 elliptic curve construction. We obtain this result using the *LLL algorithm* as in Fuentes et al.[5] and Budroni and Pintore[3]. This can be computed using a single scalar multiplication by $z$ which is roughly a fourth of the size of $q$, and some other trivial group operations.

Again due to the subgroups of order $13^2$ and $23^2$ we must manually check that this procedure works for BLS12-381, and we have done so. Specifically, we have ensured that $zx^3 - x^2 + 1$ has no roots in $GF(13^2)$ and $GF(23^2)$.

It is notable that this check can be computed more efficiently than the cofactor multiplication of Budroni and Pintore[3], and so we posit that protocols using cofactor multiplication to avoid small subgroup attacks are better served by applying this check instead.

### 3.2 Checking Subgroups in $\mathbb{G}_1$

Next, we present a technique for checking that a point $P$ exists within $\mathbb{G}_1$. First, let us introduce the well-known endomorphism $\sigma : E \to E$ defined by $(x, y) \to (\beta x, y)$ for some $\beta \in \mathbb{F}_p$ of multiplicative order 3. Given a point $P \in E(\mathbb{F}_p)$ of order $n$, the endomorphism $\sigma$ acts as a multiplication map $[\lambda_n]P$ where $\lambda_n$ is a solution to $\lambda_n^2 + \lambda_n + 1 = 0 \pmod{n}$. We find that $\lambda_q = z^2 - 1$, which may be of independent interest.

Just as before, we use the *LLL algorithm* to find the subgroup check

$$[(z^2 - 1)/3](2\sigma(P) - P - \sigma^2(P)) - \sigma^2(P) = \mathcal{O}$$

which can be computed using only trivial group operations and a scalar multiplication by $(z^2 - 1)/3$, which is half the size of $q$ and has low Hamming weight. For each primitive subgroup of order $n$ (with the exception of $q$) we check that $\lambda_n$ is not a root of the polynomial $[(z^2 - 1)/3](2x - 1 - x^2) - x^2$ in $GF(n)$.

## 4 Acknowledgements

The authors thank Daira Hopwood and Riad S. Wahby for helpful discussion.

## References

[1] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. Cryptology ePrint Archive, Report 2002/088, 2002. `https://eprint.iacr.org/2002/088`.

[2] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '01, pages 514–532, Berlin, Heidelberg, 2001. Springer-Verlag.

[3] Alessandro Budroni and Federico Pintore. Efficient hash maps to g2 on bls curves. Cryptology ePrint Archive, Report 2017/419, 2017. https://eprint.iacr.org/2017/419.

[4] Henry de Valence. Why ristretto? pitfalls of a cofactor. https://ristretto.group/why_ristretto.html#pitfalls-of-a-cofactor.

[5] Laura Fuentes-Castañeda, Edward Knapp, and Francisco Rodríguez-Henríquez. Faster hashing to g2. In *Proceedings of the 18th International Conference on Selected Areas in Cryptography*, SAC'11, pages 412–430, Berlin, Heidelberg, 2012. Springer-Verlag.

[6] Steven D. Galbraith and Michael Scott. Exponentiation in pairing-friendly groups using homomorphisms. Cryptology ePrint Archive, Report 2008/117, 2008. https://eprint.iacr.org/2008/117.

[7] Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa. Fast hashing to g2 on pairing friendly curves. Cryptology ePrint Archive, Report 2008/530, 2008. https://eprint.iacr.org/2008/530.

[8] Riad S. Wahby and Dan Boneh. Fast and simple constant-time hashing to the bls12-381 elliptic curve. Cryptology ePrint Archive, Report 2019/403, 2019. https://eprint.iacr.org/2019/403.