A note on group membership tests for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on BLS pairing-friendly curves

Michael Scott

Cryptography Research Centre
Technical Innovation Institute
michael.scott@tii.ae

Abstract. Here we consider a method for quickly testing for group membership in the groups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ (all of prime order r) as they arise on a type-3 pairing-friendly curve. As is well known endomorphisms exist for each of these groups which allows for faster point multiplication for elements of order r. The endomorphism applies if an element is of order r. Here we show that, under relatively mild conditions, the endomorphism applies **if and only if** an element is of order r. This results in a faster method of confirming group membership. In particular we show that the conditions are met for the popular BLS family of curves.

1 Introduction

In the course of running a cryptographic protocol you receive an element in a cyclic group, whose prime order is a fixed system parameter. However cryptographic protocols are typically run in an untrusting environment. How can you be sure that the element you have been given is actually of the correct order? You should worry because it might benefit an attacker to provide an element of a different order, typically in a much smaller sub-groups. Your protocol depends for its security on executing in a large group, but now you find yourself unwittingly confined to a much smaller group, in which your "hard problem" is no longer hard. If you should continue to process such elements all bets are off concerning the security of your protocol.

In pairing-based protocols things are complicated by the fact that typically three groups are involved (on popular so-called type-3 pairing friendly curves [7]), usually referred to as $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$. If $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, then a pairing evaluates as $e(P,Q) \in \mathbb{G}_T$. While the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ consist of points on elliptic curves, the group $\mathbb{G}_T$ is embedded in a finite extension field. For more information on pairings and their role in cryptography, see [14]. All of the groups have the same prime order r, where r is typically at least 256-bits long, to provide a secure setting for cryptography. In each setting the number of plausible elements that could be presented will be hr for some co-factor h, different for each of the three groups. Typically in the pairing context $h_1 < r$, and $h_2 > r$ and $h_T \gg r$. In deciding on an optimal strategy for confirming that protocol inputs are of the correct order r we will need to take into account the

size of this cofactor. For more cogent arguments on the importance of dealing with co-factors, see section 1.1 of [10] "Pitfalls of a cofactor".

In fact that is not the only solution. We could choose our system parameters such that no small subgroups exist [13], [15], [2]. Now an attacker can only provide elements of a larger prime order. Being confined to a larger group is unlikely to cause a problem, so the attack fails. The hope is that group membership testing now becomes largely redundant, which absolves a careless implementor from having to worry about the group membership issue. However this is not an entirely satisfactory solution. The provided element is not of the correct order and the impact of, for example, inputting a supposed $\mathbb{G}_2$ point of the wrong order into a pairing may not yet be fully understood. Another downside of this approach is that it is unlikely to be an option for $\mathbb{G}_1$ where usually $h < r$, such that no larger subgroups can exist.

Going back to our original approach, two solutions currently exist. Assume that the number of points on the curve $\mathbb{G}_1$ is hr. The first idea is to multiply any incoming element by h to force it into the correct group. This is often referred to as "clearing the cofactor". If it were of the correct order, this simply moves the point to another point of order r. But this is not the original point, and that might introduce a complication for implementors. The second idea is to bite the bullet, and multiply the point by the full order r to confirm that this results in the group neutral element, in this case O the point-at-infinity. However this is going to be costly.

For elements in $\mathbb{G}_T$ only the second solution appears competitive, given the large size of h_T, even though exponentiation by h_T (a process often referred to as the "hard part of the final exponentiation" in pairing literature) has been highly optimized [11].

For $\mathbb{G}_2$ clearing the cofactor might still be an option using the fast method for cofactor elimination on BLS curves as described by Budroni and Pintore [6].

In their paper [2], talking about the group $\mathbb{G}_1$, Barreto et al contend that "Therefore, one must carry out either a scalar multiplication by r to check for the correct order or by the cofactor h to force points to have the right order."

Here we point to a third way, which provides the same assurance as multiplying the point by the group order, but at a fraction of the cost.

2 BLS-12 curves

The BLS-12 elliptic curve [3] consists of points with coordinates $x, y \in \mathbb{F}_p$ that satisfy

$$y^2 = x^3 + B$$

It is defined by a field modulus

$$p = (u-1)^2/3.(u^4 - u^2 + 1) + u$$

where $u = 1 \bmod 3$. The number of points on the curve is $hr = p + 1 - t$ and the pairing-friendly group of embedding degree 12 is of order r, where

$$r = u^4 - u^2 + 1$$

$$t = u + 1$$

There is a curve cofactor of

$$h = (u-1)^2/3$$

However as pointed out by Wahby and Boneh [17] the effective point cofactor is

$$h_1 = (u-1)$$

Each particular curve depends on the choice of u, which must be chosen such that p and r are prime. Curves are still plentiful under this constraint, so it is standard practise to pick a sparse u of low Hamming weight, as this brings advantages when calculating a pairing.

The group $\mathbb{G}_1$ consists of points of order r on an elliptic curve over the base field, that is on the curve $E(\mathbb{F}_p)$. The group $\mathbb{G}_2$ consists of points of order r on a sextic twist of the same curve $E'(\mathbb{F}_{p^2})$, defined over the quadratic extension field $\mathbb{F}_{p^2}$. The number of points on this curve is $h_2 r$, where h_2 is a much larger co-factor [12].

$$h_2 = (p^2 + p + 1 - (t^2 - \sqrt{3(4pt^2 - p^4)})/2)/r$$

Finally $\mathbb{G}_T$ consists of elements of order r in the extension field $\mathbb{F}_{p^{12}}$. The total number of elements in this extension field is

$$p^{12} - 1 = (p^6 - 1)(p^2 + 1)((p^4 - p^2 + 1)/r)r$$

Fortunately there is a quick "cyclotomic test" based on the p-power Frobenius to confirm that an element w is of an order that divides the cyclotomic factor $p^4 - p^2 + 1 = h_T.r$ [2].

$$w^{p^4 - p^2 + 1} = 1$$

This can be confirmed by checking that $w.w^{p^4} = w^{p^2}$. So the cofactor of concern here is

$$h_T = (p^4 - p^2 + 1)/r$$

3 The Endomorphisms

An elliptic curve is said to support an endomorphism if there is a quick method to determine a non-trivial known multiple of any point, without having to perform a point multiplication. The exploitation of an endomorphism to speed up general point multiplication on an elliptic curve was first suggested by Gallant, Lambert

and Vanstone [9], and is known as the GLV method. As applied to the group $\mathbb{G}_1$ here, it takes the form

$$\psi(P) = \lambda P$$

where ψ transforms the point from (x, y) to $(\beta.x, y)$, where β is a precomputed cube root of unity modulo p, and λ is a nontrivial cube root of unity modulo the order of the point, r. That is λ satisfies $\lambda^2+\lambda+1 = 0 \bmod r$. Noting the similarity between this expression and the r parameter as it occurs for a BLS-12 curve, we get the neat solution $\lambda = -u^2$. So for the BLS-12 curve the endomorphism is [8], [5]

$$\psi(P) = -u^2 P$$

Observe that any multiplication by $-u^2$ will be twice as quick as multiplication by r.

In the groups $\mathbb{G}_2$ and $\mathbb{G}_T$ Galbraith and Scott [8] extend the idea of [9] by pointing out that a p-power Frobenius endomorphism applies in these groups. The p-power Frobenius map as applied to an extension field that is home to a group like $\mathbb{G}_T$, arises as a consequence of a fast method to exponentiate to the power of p. See [8], [5] for details. On our BLS-12 curve we can see that this will be immediately useful, as for an element w of order r, given that $r|(p + 1 - t)$, $w^{p+1-t} = 0$ implies $w^p = w^{t-1} = w^u$. This time observe that exponentiation by u will be four times faster than exponentiation by r.

The p-power Frobenius map is also the basis for an endomorphism that applies in elliptic curve groups over extension fields like $\mathbb{G}_2$ [8]. In this case we get a fast way to calculate pQ, and for the BLS-12 curve we have $pQ = uQ$. Again, multiplication by u will be four times faster than multiplication by r.

These endomorphisms are normally used to speed up the group operation, be it point multiplication in elliptic curve groups, or exponentiation in finite extension field groups. Here we will be using them for an entirely different purpose, for confirming that group elements are indeed of the correct order r. Recall that if the total number of possible elements is hr for some cofactor h, only those of order r are members of the group. Let c be any non-trivial divisor of h. Then the other possibilites for an element are that it could be of an order c, or it could be of an order $c.r$. If these other possibilities can be excluded, we are assured that the element is of order r, and hence is a group member.

4 The $\mathbb{G}_2$ case

Consider a point Q which purports to be a member of $\mathbb{G}_2$. The cofactor in this case is h_2. Because the endomorphism should apply to Q, we can check that $pQ = uQ$, which costs little more than a point multiplication by a short, sparse u. This confirms that $(p - u)Q = (p + 1 - t)Q = O$. Therefore Q has an order dividing $p + 1 - t = hr$.

However we also know that Q is a point on $E'(\mathbb{F}_{p^2})$ and therefore has an order dividing $h_2 r$. Therefore Q is of an order dividing $\gcd(hr, h_2 r)$ or equivalently $\gcd(h_1 r, h_2 r)$. Hence Q is of order r under the condition $\gcd(h_1, h_2) = 1$, which is a test involving only the curve parameter u. Given that $h_1 = u - 1$ and the cofactor h_2 in this case is [2]

$$h_2 = (u^8 - 4u^7 + 5u^6 - 4u^4 + 6u^3 - 4u^2 - 4u + 13)/9$$

it is straightforward to use a tool like SageMath [16] to calculate the polynomial GCD, and hence confirm that this condition is true, and indeed that $h_2 \bmod h_1 = 1$ so that the condition is true for all candidate $u = 1 \bmod 3$. We note that the simple condition that $\gcd(h_1, h_2) = 1$ may not be true for other families of pairing friendly curves. But it does apply also to BLS-24 and BLS-48 curves.

5 The $\mathbb{G}_T$ case

A BLS-12 pairing evaluates as a element in the finite extension field $\mathbb{F}_{p^{12}}$. If this element is of order r then it is a member of $\mathbb{G}_T$. Consider an element w which purports to be a member of $\mathbb{G}_T$. Assume that the cyclotomic test (see above) has already been carried out to quickly eliminate a large class of non-members. Again we know that the endomorphism should hold for w, and we can check that $w^p = w^u$ at the cost of an exponentiation by u. This confirms that $w^{p-u} = w^{p+1-t} = 1$. Therefore w has an order dividing $h_1 r$. But it also has an order that divides $h_T r$. So again if $\gcd(h_1, h_T) = 1$ we know that w must be of order r. As before we find that $h_T \bmod h_1 = 1$, and so for BLS-12/24/48 curves this condition is always met.

6 The $\mathbb{G}_1$ case

In the case of $\mathbb{G}_1$ we take a different approach. The GLV endomorphism as it applies to a point $P = (x, y)$ on a BLS12 curve is

$$\psi(P) = (\beta x, y) = -u^2 P$$

where β is a cube root of unity modulo p. So the first thing to do is to check that the endomorphism is true for our candidate point P. If it is not, then we can confidently conclude that P is not of order r, and we are done. But we can go further and prove that if the endomorphism is true, then P must be of order r.

We offer proof by contradiction. Recall that $-u^2$ is a cube root of unity modulo the order. Therefore

$$-u^6 = 1 \bmod r$$

If the endomorphism were also true for a point of order $c.r$, where c is some divisor of h_1, then we would also have

$$-u^6 = 1 \bmod c.r$$

Which by the Chinese Remainder Theorem implies that

$$-u^6 = 1 \bmod c$$

However we know that for a BLS curve $c|h_1$ so $c|(u-1)$, therefore

$$u^6 = (u \bmod c)^6 = 1^6 = 1 \bmod c$$

which is a contradiction. Furthermore there is an "early out" optimization possible for points of an order c that divides $u-1$, as in that case $(u-1)P = O$ and $uP = P$. If in the course of calculating $-u^2P$ it is observed that this condition is met, then P is not of order r and we can exit immediately, reporting failure.

While this method is faster than point multiplication by the group order, it will be slower than processing an input by simply clearing the cofactor and multiplying it by h_1.

7 Discussion

Compared with the effort necessary to prove group membership by multiplying/exponentiating by r, these methods are $\times 2$ faster in $\mathbb{G}_1$, and $\times 4$ faster in $\mathbb{G}_2$ and $\mathbb{G}_T$ for BLS-12 curves. For BLS-24 and BLS-48 curves the advantage is the same in $\mathbb{G}_1$, and $\times 8$ and $\times 16$ respectively for the other two groups..

On prime order BN curves [4], which are often considered as competitive with BLS-12 curves, no testing at all is required for $\mathbb{G}_1$ membership testing, but the $\mathbb{G}_T$ case requires exponentiation to the power of $6u^2$ (see [15] section 8.2), for only a $\times 2$ advantage in $\mathbb{G}_T$ (and $\mathbb{G}_2$).

Indeed these new membership tests are so efficient it calls into question the requirement for BLS pairing-friendly curves to be $\mathbb{G}_T$ and $\mathbb{G}_2$ strong [15], [2], conditions which, certainly in combination, severely constrain our ability to find nice curves. Recall that being both $\mathbb{G}_2$ and $\mathbb{G}_T$ strong means that h_2 and h_T should be prime, such that no small subgroups exist. That group membership tests become redundant in these cases is only partially true. The $\mathbb{G}_1$ case still needs to be dealt with for BLS curves, and in the $\mathbb{G}_T$ case candidate elements still need to be pre-screened with a cyclotomic test.

But there is one very plausible scenario where the cost of subgroup membership testing becomes significant – that of pairing delegation [1]. Here any extra cost associated with a $\mathbb{G}_T$ membership check adds to the overall cost for a poorly endowed processor that has delegated the expensive pairing calculation to a more powerful (but untrusted) server. In this case it would still be advantageous for the curve to be $\mathbb{G}_T$ strong.

8 Conclusion

Before accepting an input to a pairing-based protocol (based on BLS curves) that purports to be a member of $\mathbb{G}_1$, $\mathbb{G}_2$ or $\mathbb{G}_T$, then the following is recommended.

- In the case of $\mathbb{G}_1$ and $\mathbb{G}_2$, check that the elliptic curve point is actually on the correct curve.
- In the case of $\mathbb{G}_1$ multiply it by the cofactor h_1. If it becomes the point-at-infinity, abort. Protocol designers should be aware that inputs in $\mathbb{G}_1$ will undergo such preprocessing.
- In the case of $\mathbb{G}_T$, subject the input to the "cyclotomic test", and abort on failure.
- In the cases of $\mathbb{G}_2$ and $\mathbb{G}_T$, subject the input to the appropriate endomorphism test as described above. But this may not be necessary if the curve is known to be $\mathbb{G}_2$ and/or $\mathbb{G}_T$ strong.

We note that in all cases the price for group membership assurance is at most that of a simple multiplication/exponentiation by the curve parameter u.

Acknowledgments

The author is grateful to Francisco Rodriguez-Henriquez, Steven Galbraith and Diego Aranha for providing valuable feed-back on earlier drafts of this work.

References

1. D. F. Aranha, E. Pagnin, and F. Rodriguez-Henriquez. LOVE a pairing. Cryptology ePrint Archive, Report 2021/1029, 2021. `http://eprint.iacr.org/2021/1029`.
2. P. S. L. M. Barreto, C. Costello, R. Misoczki, M. Naehrig, G. Pereira, and G. Zanon. Subgroup security in pairing-based cryptography. In *LATINCRYPT*, volume 9230 of *Lecture Notes in Computer Science*, pages 245–265. Springer-Verlag, 2015.
3. P.S.L.M. Barreto, B. Lynn, and M. Scott. Constructing elliptic curves with prescribed embedding degrees. In *Security in Communication Networks – SCN 2002*, volume 2576 of *Lecture Notes in Computer Science*, pages 257–267. Springer-Verlag, 2003.
4. P.S.L.M. Barreto and M. Naehrig. Pairing-friendly elliptic curves of prime order. In *Selected Areas in Cryptology – SAC 2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 319–331. Springer-Verlag, 2006.
5. J. Bos, C. Costello, and M. Naehrig. Exponentiating in pairing groups. Cryptology ePrint Archive, Report 2013/458, 2013. `http://eprint.iacr.org/2013/458`.
6. A. Budroni and F. Pintore. Efficient hash maps to G2 on bls curves. *Applicable Algebra in Engineering, Communication and Computing*, 2020. `https://eprint.iacr.org/2017/419.pdf`.
7. S. Galbraith, K. Paterson, and N. Smart. Pairings for cryptographers. *Discrete Applied Mathematics*, 156:3113–3121, 2008.

8. S. Galbraith and M. Scott. Exponentiation in pairing-friendly groups using homomorphisms. In *Pairing 2008*, volume 5209 of *Lecture Notes in Computer Science*, pages 211–224. Springer-Verlag, 2008.
9. R. Gallant, R. Lambert, and S. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphism. In *Crypto 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 190–200. Springer-Verlag, 2001.
10. M. Hamburg. Decaf: Eliminating cofactors through point compression. In *Crypto 2015*, volume 9215 of *Lecture Notes in Computer Science*, pages 705–723. Springer-Verlag, 2015.
11. D. Hayashida, K. Hayasaka, and T. Teruya. Efficient final exponentiation via cyclotomic structure for pairings over families of elliptic curves. Cryptology ePrint Archive, Report 2020/875, 2020. `http://eprint.iacr.org/2020/875`.
12. F. Hess, N. Smart, and F. Vercauteren. The eta pairing revisited. *IEEE Transactions on Information Theory*, 52:4595–4602, 2006.
13. C. H. Lim and P. J. Lee. A key recovery attack on discrete log-based schemes using a prime order subgroup. In *Crypto 1994*, volume 1294 of *Lecture Notes in Computer Science*, pages 249–263. Springer-Verlag, 1994.
14. N. El Mrabet and M. Joye, editors. *Guide to Pairing-Based Cryptography*. Chapman and Hall/CRC, 2016. `https://www.crcpress.com/Guide-to-Pairing-Based-Cryptography/El-Mrabet-Joye/p/book/9781498729505`.
15. M. Scott. Unbalancing pairing-based key exchange protocols. Cryptology ePrint Archive, Report 2013/688, 2013. `http://eprint.iacr.org/2013/688`.
16. The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.0.0)*, 2020. `https://www.sagemath.org`.
17. R. Wahby and D. Boneh. Fast and simple constant-time hashing to the BLS12-381 elliptic curve. Cryptology ePrint Archive, Report 2019/403, 2019. `http://eprint.iacr.org/2019/403`.