Call for Proposals: Analysis of Pluto-Eris

IOG

1 Executive Summary

Input Output Global (IOG), the powerhouse behind the Cardano blockchain and ecosystem, is interested in a thorough cryptographic security and efficiency analysis of Pluto-Eris [plu], a hybrid cycle of curves.

The deadline for submitting results is December 31, 2023. The deadline for proposal submission is September 10, 2023. Final proposals should include details related to the effort required and the costs that IOG will cover for the selected provider. All other details will be negotiated as per the details herein.

All communications to be directed to Vanishree Rao at vanishree.rao@iohk.io and Markulf Kohlweiss at markulf.kohlweiss@iohk.io.

2 Introduction

IOG is interested in a through analysis of Pluto-Eris, a hybrid cycle of curves. In this call for proposals, we specify the high-level motivation and the projected impact of this work, the feature and security properties of the curves and the format and acceptance criteria of work delivery.

2.1 The Motivation

IOG has incubated a protocol that aims to build a zero-knowledge proof system supporting recursion, aka proofs of proofs, based on Halo2 [hal]. Halo2 is currently based on the pasta cycle of curves with neither of the two curves being pairing friendly. This prevents the usage of efficient (succinctly verifiable) polynomial commitment schemes, such as the KZG scheme [KZG10a], that need pairing-friendly curves. This has motivated the search for a cycle of curves where at least one of the curves is pairing friendly.

An efficient hybrid cycle of curves will be a significant contribution to the blockchain space that utilizes zero-knowledge proofs. This is because, it can help Halo2, one of the most widely used zero-knowledge proof systems, to achieve constant verification complexity (w.r.t. the circuit size). A non-constant verification complexity is one of the biggest pain points in various applications, including bridges and zk rollups [bar, VOm+].

The outcome of this work is aimed to affect the critical core part of the protocol.

3 Requirements on the Hybrid Cycle of Curves

This section specifies the properties that need to be satisfied by Pluto-Eris.

Note that Pluto is the pairing-friendly curve and Eris is not. A formal definition of a hybrid cycle of curves can be found in Appendix A. We will present the security and feature requirements below.

3.1 Security Requirements

Security level. The Pollard Rho security level for Eris needs be at least 128 bits. The STNFS cost must estimate the security level of the Pluto to be at least 128 bits.

Twist security. Both curves must have a twist security of at least 128 bits.

Sampling process. The curves need to be sampled deterministicaly through a script using the feature requirements and security requirements mentioned in this document; any other constraint in the script needs to be approved by IOG.

SafeCurves. Whilst all Safecurves [saf] criteria are highly desirable, it might not be possible to satisfy some of them. In that case, it is required to provide a best-possible alternative with the same overall functionality. Such exceptions will also need to be approved by IOG.

We describe some possible deviations in the following, further deviations need a formal approval from IOG to be acceptable.

- Elligator 2. If Elligator 2 [BHKL13] cannot be used, indistinguishability must be efficiently achievable through Elligator Squared [Tib14].
- Ladder support. Ladder support needn't be satisfied.
- Embedding degree. The embedding degree criterion is not required for the pairing-friendly curve.
- Completeness. Complete formulas are desirable. An investigation of efficient scalar multiplication and multi-scalar multiplication (natively and inside proofs) is acceptable.

3.2 Feature Requirements

2-adicity. Both curves must have a 2-adicity of at least 32.

j-invariant. Both curves must have j-invariant $= 0$.

Hash to curve. It is highly desirable to have efficient hash to curve algorithms, such as the "simplified SWU" method [BCI+10] or extensions such as [WB19].

Low Hamming weight for the BN parameter u. If the BN parameter u has low Hamming weight, the pairing computation can be efficient. Hence, it is desirable that the pairing-friendly curve has a low Hamming weight BN parameter.

4 Deliverables

The deliverables consist of:

1. An independently written script to deterministically sample Pluto-Eris and provide documentation for it.
2. A detailed report containing a thorough security and feature analysis, addressing every requirement mentioned above. It should also contrast Pluto-Eris with the pasta curves [pas].
3. Proof of concept implementation in Rust using the Arkworks [ark] library of all group operations including $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ and pairing operations for the pairing friendly curve, curve operations for E_1 and E_2 and hash to curve for both the curves. The implementation should include unit tests and performance tests with sufficient test vectors.
4. The proposal must include a bid and a description of the team executing the proposal.

4.1 Acceptance Criteria

1. The sampling script should enforce all the feature and security requirements, unless the provider obtains a clear exception approval from IOG.
2. The report should detail the performance and security analysis.
3. The code needs to be properly documented.

5 Timeline

- Deadline for proposal submission: September 10, 2023 at 11:59PM EST
- Deadline for project completion: December 31, 2023 at 11:59PM EST

Appendix

A Definition of Hybrid Cycle of Curves

We use the definition of *2-cycles of elliptic curves* from [AHG22, Definition 1], and combine this with the existence of a pairing on one of the two curves. Specifically:

Definition 1 *A **hybrid cycle of curves** is a pair of elliptic curves $E_1/\mathbb{F}_{p_1}$ & $E_2/\mathbb{F}_{p_2}$, such that:*

- $\#(E_1/\mathbb{F}_{p_1}) = p_2$ *and* $\#(E_2/\mathbb{F}_{p_2}) = p_1$
- $E_1/\mathbb{F}_{p_1}$ *is pairing friendly.*

Other definitions may be found in [BSCTV17], or [EH22, Chapter 4.3].

We follow the conventions of [GPS06]. We refer to $E_2/\mathbb{F}_{p_2}$ as $\mathbb{G}$ and to $E_1/\mathbb{F}_{p_1}$ as $\mathbb{G}_1$. For $\mathbb{G}_1$ to be pairing friendly, there needs to exist another source group $\mathbb{G}_2$ and a target group $\mathbb{G}_T$ as well as an efficient, non-degenerate pairing operation $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$.

Such curves are particularly useful for compact recursive proofs, relying on polynomial commitments using the Inner Product Argument [BCC+16] over $\mathbb{G}_1$ and $\mathbb{G}$ for unbounded recursion, and using the pairing on $\mathbb{G}_1$ and $\mathbb{G}_2$ for a [KZG10b]-based polynomial commitment for compression.

References

[AHG22] Diego F. Aranha, Youssef El Housni, and Aurore Guillevic. A survey of elliptic curves for proof systems. Cryptology ePrint Archive, Paper 2022/586, 2022. https://eprint.iacr.org/2022/586.

[ark] Arkworks: An ecosystem for developing and programming with zksnarks. https://github.com/arkworks-rs. Accessed: 2023-06-12.

[bar] barrywhitehat. Roll up: Scale ethereum with snarks. https://github.com/barryWhiteHat/roll-up/. Accessed: 2023-06-20.

[BCC+16] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, and Christophe Petit. Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 327–357. Springer, 2016.

[BCI+10] Eric Brier, Jean-Sébastien Coron, Thomas Icart, David Madore, Hugues Randriam, and Mehdi Tibouchi. Efficient indifferentiable hashing into ordinary elliptic curves. In *Advances in Cryptology–CRYPTO 2010: 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings 30*, pages 237–254. Springer, 2010.

[BHKL13] Daniel J Bernstein, Mike Hamburg, Anna Krasnova, and Tanja Lange. Elligator: elliptic-curve points indistinguishable from uniform random strings. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 967–980, 2013.

[BSCTV17] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Scalable zero knowledge via cycles of elliptic curves. *Algorithmica*, 79:1102–1160, 2017.

[EH22] Youssef El Housni. *The arithmetic of pairing-based proof systems.* Theses, Institut Polytechnique de Paris, November 2022.

[GPS06] S. D. Galbraith, K. G. Paterson, and N. P. Smart. Pairings for cryptographers. Cryptology ePrint Archive, Paper 2006/165, 2006. https://eprint.iacr.org/2006/165.

[hal] The halo2 book. https://zcash.github.io/halo2/. Accessed: 2023-06-18.

[KZG10a] Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg. Constant-size commitments to polynomials and their applications. In *Advances in Cryptology - ASIACRYPT 2010*, 2010.

[KZG10b] Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg. Constant-size commitments to polynomials and their applications. In Masayuki Abe, editor, *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*, volume 6477 of *Lecture Notes in Computer Science*, pages 177–194. Springer, 2010.

[pas] pasta curves. https://github.com/zcash/pasta_curves. Accessed: 2023-06-12.

[plu] Pluto/eris supporting evidence. https://github.com/daira/pluto-eris. Accessed: 2023-06-12.

[saf] Safecurves: choosing safe curves for elliptic-curve cryptography. https://safecurves.cr.yp.to. Accessed: 2023-06-12.

[Tib14] Mehdi Tibouchi. Elligator squared: Uniform points on elliptic curves of prime order as uniform random strings. In *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, pages 139–156. Springer, 2014.

[VOm$^+$] Vis Virial, Mesquita Oliveira, minimalsm, Dimitris Apostolou, Manik Jain, Corwin Smith, Paul Wackerow, Ray Zhu, Shelley Olivia, Emmanuel Awosika, Sam Richards, Luozhu Zhang, Joseph Cook, Sora Nature, and Hursit Tarcan. Zero-knowledge rollups. https://ethereum.org/en/developers/docs/scaling/zk-rollups/. Accessed: 2023-06-20.

[WB19] Riad S. Wahby and Dan Boneh. Fast and simple constant-time hashing to the bls12-381 elliptic curve. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(4):154–179, Aug. 2019.