Families of SNARK-friendly 2-chains of elliptic curves

Youssef El Housni[1,2,3] and Aurore Guillevic[4,5]

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

Abstract

A SNARK [9,10,5,1] is a cryptographic primitive that enables a prover to prove to a verifier the knowledge of a satisfying witness to a non-deterministic (NP) statement by producing a proof π such that the size of π and the cost to verify it are both sub-linear in the size of the witness. If π does not reveal anything about the witness we refer to the cryptographic primitive as a zero-knowledge (zk) SNARK. Today, the most succinct SNARKs require pairing-friendly elliptic curves and trusted setup assumptions as in Groth'16 [6] but in return admit small, constant-size proofs with a constant-time verification. However, the trusted setup is specific to the NP statement to prove. Hence, Groth'16 is not suitable in applications that need to prove many different statements. Fortunately, SNARKs with a universal or transparent setup are an active area of research and recent polynomial-commitment-based constructions allow very efficient constructions. The most efficient universal constructions such as PlonK [4] and Marlin [3] are based on the KZG polynomial commitment [8], which also requires a pairing-friendly elliptic curve. Both type of constructions are succinct and thus suitable for recursive SNARKs, that is proofs verifying the correctness of other proofs. However, to do so efficiently, one need not only a single pairing-friendly elliptic curve but a chain of pairing-friendly elliptic curves. An efficient 2-chain was proposed in Zexe [2], composed of BLS12-377 and CP6-782 curves.

Last year at JC2 and in [7], we introduced a 2-chain of curves made of the previous BLS12-377 and a new BW6-761 curve, a Brezing-Weng curve of embedding degree 6 defined over a 761-bit prime field, which we demonstrated to be orders of magnitude faster than CP6-782. In this work, we first are interested in families of 2-chains in which the BW6-761 curve would fall. We present a family of BW6 curves from any BLS12 curve and derive generic formulas, in terms of the BLS12 curve seed u, and integer parameters h_t, h_y. We extend this work to a 2-chain family of BW6 curves from BLS24 curves. To achieve higher levels of security in the target finite field of the outer curves, we compare a larger field characteristic thanks to larger parameters h_t, h_y, to the larger embedding degrees

8 and 12 obtained with Cocks-Pinch curves. Finally, we argue that the BLS12 and BLS24 based families are respectively tailored for Groth'16 and KZG-based SNARKs recursive proof composition, and we present a short list of curves with an optimized implementation along with benchmarks.

References

1. Bitansky, N., Canetti, R., Chiesa, A., Tromer, E.: From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In: Goldwasser, S. (ed.) ITCS 2012. pp. 326–349. ACM (Jan 2012). https://doi.org/10.1145/2090236.2090263
2. Bowe, S., Chiesa, A., Green, M., Miers, I., Mishra, P., Wu, H.: ZEXE: Enabling decentralized private computation. In: 2020 IEEE Symposium on Security and Privacy. pp. 947–964. IEEE Computer Society Press (May 2020). https://doi.org/10.1109/SP40000.2020.00050
3. Chiesa, A., Hu, Y., Maller, M., Mishra, P., Vesely, N., Ward, N.P.: Marlin: Preprocessing zkSNARKs with universal and updatable SRS. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part I. LNCS, vol. 12105, pp. 738–768. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45721-1_26
4. Gabizon, A., Williamson, Z.J., Ciobotaru, O.: PLONK: Permutations over lagrange-bases for oecumenical noninteractive arguments of knowledge. ePrint 2019/953
5. Gentry, C., Wichs, D.: Separating succinct non-interactive arguments from all falsifiable assumptions. In: Fortnow, L., Vadhan, S.P. (eds.) 43rd ACM STOC. pp. 99–108. ACM Press (Jun 2011). https://doi.org/10.1145/1993636.1993651
6. Groth, J.: On the size of pairing-based non-interactive arguments. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 305–326. Springer, Heidelberg (May 2016). https://doi.org/10.1007/978-3-662-49896-5_11
7. Housni, Y.E., Guillevic, A.: Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition. In: Krenn, S., Shulman, H., Vaudenay, S. (eds.) CANS 20. LNCS, vol. 12579, pp. 259–279. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-65411-5_13
8. Kate, A., Zaverucha, G.M., Goldberg, I.: Constant-size commitments to polynomials and their applications. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 177–194. Springer, Heidelberg (Dec 2010). https://doi.org/10.1007/978-3-642-17373-8_11
9. Kilian, J.: A note on efficient zero-knowledge proofs and arguments (extended abstract). In: 24th ACM STOC. pp. 723–732. ACM Press (May 1992). https://doi.org/10.1145/129712.129782
10. Micali, S.: CS proofs (extended abstracts). In: 35th FOCS. pp. 436–453. IEEE Computer Society Press (Nov 1994). https://doi.org/10.1109/SFCS.1994.365746