Survey of ZK-SNARK

Yuncong Zhang

May 15, 2020

Abstract

1 Introduction

Zero-Knowledge Succinct Noninteractive ARgument of Knowledge (zkSNARK) enables verifying the correctness of an NP statement without revealing any information about the witness, with complexity lower than direct verification. The concept of zero-knowledge proof originated from Goldwasser, Micali, and Rackoff [GMR89]. Following this work, and the ground-breaking proposal of PCP by Babai et al. [BFLS91], Kilian [Kil92] created the first *succinct interactive argument* by compiling a PCP via cryptographic commitment, where the notation of "argument" means the proof system has only computational soundness. After that, Micali [Mic00] obtained a succinct non-interactive argument by applying the Fiat-Shamir [FS86] transformation to Kilian's protocol. Since then, a decade of research has produced a tremendous and ever-increasing number of zkSNARK implementations. Currently, zkSNARK is still undergoing active research, both for theoretical interests [NY90] and for its practical applications, especially in Blockchain [BCG$^+$14].

However, the rapid development of zkSNARK exhibits considerable challenges for researchers to keep up with the state-of-the-art of this field. The ZKProof Community recently initiated the standardization of zero-knowledge proofs and has presented a reference document [DB19]. Despite being comprehensive, this document is more of an exhaustive reference of concepts than a systematic review of the literature. Other surveys including those by Nitulescu [Nit19], Walfish [WB15] et al. are also valuable for understanding the crucial concepts and research status of zkSNARKs. However, they each focus on a limited number of lines of progress. Nitulescu [Nit19] describes the early history of zero-knowledge proofs and provides a detailed technical explanation of QAP/LIP-based implementations of zkSNARKs. Walfish [WB15] illustrates the ideas behind implementations including Pinocchio [PHGR13], Thaler [Tha13], Buffet [WSR+15], TinyRAM [BCG+13, BCTV14], et al. Both works focus on the circuit-oriented designs and neglect those works that are more friendly with random access machines (RAMs) [BCG+13, BCGV16, BBHR18]. A comprehensive survey of literature in zkSNARKs can serve as an anchor of knowledge in this field of research, provide an overview of the most significant ideas behind current implementations, and inspire new perspectives to understand zkSNARKs.

In this paper, we present a survey that provides an overview of the current status of research of zkSNARKs. First, we discuss the concepts that are necessary to understand the literature in this research field. Secondly, we recall the history of zkSNARKs and examine the motivations and insights behind each major contribution. Finally, we propose a framework for classifying and evaluating the zkSNARK implementations, in terms of efficiency, functionality, expressiveness, infrastructure, building blocks, security assumptions, et al.

2 Preliminaries

2.1 Notations

Elliptic curves.

2.2 Cryptographic Building Blocks

Pairing.

3 Interactive Proofs

3.1 Probabilistic Checkable Proofs

4 Pairing-based ZK-SNARKs

The construction of ZK-SNARK in this line of work originates from a series of works by Groth, Ostrovsky and Sahai [Gro06, GOS06a, GOS06b], which proposed constructions of NIZK based on bilinear groups. The state-of-the-art construction of ZK-SNARK is proposed by Groth in 2016 [Gro16], which will hereby be referred to as Groth16.

4.1 Quadratic Arithmetic Problems

4.2 PCPs for QAP

4.3 QAP-based NIZKs Without PCP

5 PCP-based ZK-SNARKs

References

[BBHR18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. *IACR Cryptol. ePrint Arch.*, 2018:46, 2018.

[BCG+13] Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. Snarks for C: verifying program executions succinctly and in zero knowledge. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 90–108. Springer, 2013.

[BCG+14] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014*, pages 459–474. IEEE Computer Society, 2014.

[BCGV16] Eli Ben-Sasson, Alessandro Chiesa, Ariel Gabizon, and Madars Virza. Quasi-linear size zero knowledge from linear-algebraic pcps. In Eyal Kushilevitz and Tal Malkin, editors, *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part II*, volume 9563 of *Lecture Notes in Computer Science*, pages 33–64. Springer, 2016.

[BCTV14] Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza. Succinct non-interactive zero knowledge for a von neumann architecture. In Kevin Fu and Jaeyeon Jung, editors, *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014*, pages 781–796. USENIX Association, 2014.

[BFLS91] László Babai, Lance Fortnow, Leonid A Levin, and Mario Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the* *twenty-third annual ACM symposium on Theory of computing*, pages 21–32, 1991.

[DB19] E. Tromer. D. Benarroch, L. T. A. N. Brandao. Zkproof community reference, 2019. `https://zkproof.org`.

[FS86] Amos Fiat and Adi Shamir. How to prove yourself: Practical solutions to identification and signature problems. In Andrew M. Odlyzko, editor, *Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer, 1986. `https://doi.org/10.1007/3-540-47721-7\_12`.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on computing*, 18(1):186–208, 1989.

[GOS06a] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for nizk. In *Annual International Cryptology Conference*, pages 97–111. Springer, 2006.

[GOS06b] Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero knowledge for np. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 339–358. Springer, 2006.

[Gro06] Jens Groth. Simulation-sound nizk proofs for a practical language and constant size group signatures. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 444–459. Springer, 2006.

[Gro16] Jens Groth. On the size of pairing-based non-interactive arguments. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 305–326. Springer, 2016.

[Kil92] Joe Kilian. A note on efficient zero-knowledge proofs and arguments. In *Proceedings of the twenty-fourth annual ACM symposium on Theory of computing*, pages 723–732, 1992.

[Mic00] Silvio Micali. Computationally sound proofs. *SIAM Journal on Computing*, 30(4):1253–1298, 2000.

[Nit19] Anca Nitulescu. A gentle introduction to snarks. 2019.

[NY90] Moni Naor and Moti Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In Harriet Ortiz, editor, *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing, May 13-17, 1990, Baltimore, Maryland, USA*, pages 427–437. ACM, 1990. `https://doi.org/10.1145/100216.100273`.

[PHGR13] Bryan Parno, Jon Howell, Craig Gentry, and Mariana Raykova. Pinocchio: Nearly practical verifiable computation. In *2013 IEEE Symposium on Security and Privacy, SP 2013, Berkeley, CA, USA, May 19-22, 2013*, pages 238–252. IEEE Computer Society, 2013.

[Tha13] Justin Thaler. Time-optimal interactive proofs for circuit evaluation. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 71–89. Springer, 2013.

[WB15] Michael Walfish and Andrew J. Blumberg. Verifying computations without reexecuting them. *Commun. ACM*, 58(2):74–84, 2015.

[WSR+15] Riad S. Wahby, Srinath T. V. Setty, Zuocheng Ren, Andrew J. Blumberg, and Michael Walfish. Efficient RAM and control flow in verifiable outsourced computation. In *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015.* The Internet Society, 2015.