Project Abstract

The research explores lattice-based SNARKs and conducts an extensive evaluation of their security and usability aspects in the context of a blockchain. A comprehensive analysis of the advantages and drawbacks of substituting conventional SNARKs for lattice-based SNARKs is performed. Furthermore, a comparative assessment between lattice-based SNARKs and STARKs is undertaken, given that both cryptographic algorithms possess quantum-resistant properties.

Objectives

The objective of this research is to provide a thorough picture of zero-knowledge technologies, as well as to investigate the potential benefits that may arise from the integration of lattice-based SNARKs into the Ethereum ecosystem. In my opinion, it is of paramount importance to have a diverse selection of quantum-resistant cryptographic solutions in order to ensure the long-term security of Ethereum.

The success of this study may be gauged by the production of well-organized data and its consequential impact on future decisions regarding the selection of suitable cryptographic protocols for the underlying technology. Furthermore, the establishment of a solid foundational framework for future research endeavors is in itself a notable achievement.

Outcomes

This project will furnish essential insights into quantum-safe zero-knowledge proofs, which play a critical role in bulletproofing Ethereum’s security. Having safe and efficient ZK cryptography not only helps scaling Ethereum, but also enables the development of novel privacy-enhancing solutions to help implement the security of blockchain to everyday life. To ensure a solid basis for the development of these cryptographic techniques, rigorous and dependable research is indispensable.

Grant Scope

The research will include a comprehensive analysis of SNARKs, and their current implementations that rely on pre-quantum assumptions, which are expected not to be secure against quantum attackers in the medium- to long-term future. The properties of these SNARK constructions, currently mostly based on bilinear pairings, are compared to lattice-based SNARKs. Also, the usability on blockchains among these two and STARKs are to be evaluated as they represent a great proportion of scalability and privacy solutions in tomorrow’s Ethereum.

The expected output of the research is that lattice-based SNARKs are an option to be considered for the future, along with STARKs as both are believed to be post-quantum secure. In “Lattice-Based SNARKs: Publicly Verifiable, Preprocessing, and Recursively Composable” Albrecht et al. (2022) made significant progress on proposing the first lattice-based SNARK that simultaneously satisfied many of the desirable properties that an efficient post-quantum zero-knowledge algorithm requires. The research will also include examining the SNARK in question, possibly even enhancing it or reaching another proposal for a lattice-based construction.

Project Team

There will be one principle researcher and at least one supervisor specialized in the field working on this project:

- Aleksi Runola
    - Principle researcher
    - ~160 hours / month
        - Estimated timeline:
            - Researching the subject from July to September 2023
            - Writing the paper between September 2023 and April 2024
- Supervisor(s) to be assigned in a later stage
    - Specialized in cryptography
    - ~20-40 hours /month

Background

I’m a master’s student in University of Turku in the MDP in Information and Communications Technology program majoring in cyber security. I’m including an adequate amount of cryptography studies in my study plan, and really hope to contribute to the industry. My bachelor’s degree is in Computer Science, and I wrote my bachelor’s thesis on the scaling of Ethereum (link to the thesis, although it’s in Finnish: https://github.com/arunola/scaling-ethereum-thesis/blob/main/Ethereumin_skaalaaminen.pdf). This research would be my master’s thesis, thus providing me the academic support needed from my university.

For work, I’ve been doing software developing for a Finnish fiat/crypto ramp since 2018, and I have also contributed to some of the content we provide on our website. Most of the content can be found here: https://www.northcrypto.com. Majority of the blog posts etc. we write is on a very basic technological level in order to provide information for non-native crypto users.

I’m also a very avid Ethereum user and would love to contribute to the greater good of the Ethereum ecosystem.

Methodology

I plan to achieve my research objectives by examining all the latest research on SNARKs and lattice-based algorithms, evaluating the material available, and further refining the possibilities lattice-based solutions offer to SNARKs. As the subject is still on bit of a theoretical level, no scientific breakthrough can be promised, but I will do everything in my power to advance the research on the topic. All this research will obviously be supported by a supervisor from our well-respected university. In addition, I've also planned to contact and meet with some of the top professionals on the subject to gain even deeper knowledge and hopefully to reach a quantum leap on post-quantum cryptography.

Timeline

The extensive research on the subject could be started in July 2023, and the writing process (along with the continuous research) would start in September 2023. The structure and contents should be very clear by the end of 2023. First drafts of the finalized academic paper should be done in ~February/March 2024, and the paper would be published around May 2024.

I would be taking a study leave from work beginning from August 2023 to May 2024, meaning 9 months of full dedication for the project. Most of the funds would be to cover for the lost wages, and some for travelling expenses, as well as software and hardware costs.

Budget

- Principle Researchers Costs
  - $43 200
  - 160h/month x 9 months x $30/h
- Other Staff Costs
  - $0
  - Supervisors are paid for by the university
- Hardware Costs
  - $5000
  - Hardware for testing the SNARK implementations
- Software Costs
  - $1000
  - Basic software costs for IDEs, etc.
- Data Collection Costs
  - $1000
  - Estimation of money that will be spent on accessing research papers, usage of data collection tools etc.
- Indirect Costs

- $3000
- Travel costs to discuss with industry experts and possibly attend some conferences etc.

This totals to $53 200. Academic grants are taxable income in Finland, and the amounts are proportioned accordingly.