Thesis Portfolio

IMPLEMENTING PRIVACY-PRESERVING IDENTITY VERIFICATION WITH ZK-SNARKS: A TECHNICAL EXAMINATION OF ZERO-KNOWLEDGE PROOFS AND THE LEO PROGRAMMING LANGUAGE

(Technical Report)

PRIVACY AND TRUST IN THE AGE OF DEEP FAKES: A SOCIOTECHNICAL EXPLORATION OF ZERO-KNOWLEDGE PROOFS ON THE ALEO BLOCKCHAIN

(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Youssef Cherrat

Spring, 2025

Department of Computer Science

Sociotechnical Synthesis

Implementing privacy-preserving methods within decentralized systems represents a crucial advancement in the broader scope of digital security and identity verification. My technical project and STS research are both intricately linked through their exploration of zero-knowledge proofs (ZKPs), particularly zk-SNARKs, within blockchain technologies. The relevance of Science, Technology, and Society (STS) to engineering practice is underscored by this interplay, as it highlights the ethical and social implications of deploying advanced cryptographic solutions in fields requiring rigorous standards for data privacy and user trust.

In my STS research, I examined the potential of zero-knowledge proofs, specifically leveraging the Leo programming language and the Aleo blockchain, to establish a secure and privacy-centric identity verification system. This system allows individuals to confirm essential identity attributes, such as age or credential validity, without exposing personal data. My research highlighted how traditional verification methods expose users to privacy risks by distributing sensitive information across multiple parties, thus increasing vulnerability to breaches. Through implementing a prototype identity verification protocol, my findings demonstrated significant improvements in maintaining confidentiality and reducing risks associated with data breaches. Evaluations revealed that the Aleo blockchain effectively stores minimal verification proofs, achieving rapid verification speeds and robust defense mechanisms against various security threats.

The technical portion of my project produced a working prototype utilizing zk-SNARKs embedded within blockchain protocols to enhance secure data transfer. This prototype emphasizes zk-SNARKs' ability to maintain user confidentiality while ensuring transparency through cryptographic verification. Specifically, the system was designed to tackle two primary

challenges: computational efficiency and scalability. My implementation utilized recursive zk-SNARKs to aggregate multiple proofs into compact forms, significantly improving processing efficiency. Additionally, a multi-party computation (MPC) approach was adopted for the trusted setup phase, ensuring decentralized and secure generation of cryptographic parameters. Preliminary results underscored that zk-SNARKs substantially improved the efficiency of secure data handling, particularly in high-volume transaction environments such as finance and healthcare.

Through undertaking both my technical project and STS research, I gained profound insights into the ethical dimensions and real-world implications of integrating advanced cryptographic methods within decentralized systems. The ethical considerations inherent in managing sensitive user data underscore the importance of implementing privacy by design. My projects collectively emphasized the balance between technological capabilities and ethical responsibilities, highlighting that robust cryptographic privacy solutions must be paired with transparency, user comprehension, and responsible organizational governance. This dual exploration has significantly deepened my understanding of the critical role that engineers and technologists play in safeguarding digital trust and privacy in an increasingly interconnected world.

Acknowledgments: I express my sincere gratitude to Professor Aaron Bloomfield for his invaluable guidance and support throughout my independent study. His expertise significantly enriched my understanding of zero-knowledge cryptography and blockchain technology, enabling me to navigate technical challenges and deepen my exploration of this critical field.

Portfolio Table of Contents