Statement of Purpose

Ganyuan Cao

1 Introduction

I am currently a graduate from Arizona State University. My major is Computer Science with a concentration on cybersecurity. Along with courses for my major at Department of Computing, I took the courses required for a certificate in cryptology at Department of Mathematics to build a strong mathematical background for cryptography. In addition to regular course work, I also participated in research in cybersecurity. Specifically, My research interest is in succinct computational Integrity &privacy(SCIP), and its application to blockchain and cryptocurrency. At Arizona State University, I achieved good academic standing and graduated with honor of Summa Cum Laude. To enrich my research experience, I joined Laboratory of Security Engineering for Future Computing(SEFCOM) as the undergraduate research assistant. I plan to continue my research as a Ph.D. or M.Sc. student for the reason that I would like to explore more advanced technology and knowledge deeply, systematically and with pertinence in the field that I am interested in during the research process. I also would like to contribute my work to academia and accelerate the research in cryptography and blockchain.

2 Technical Skills

At Arizona State University, I gained knowledge in computer science, computer security and cryptography.

In the field of computer science, I learned how to use different programming languages including C/C++ and Java proficiently. At the same time, I had a good grasp of Python through self-learning since I consider Python as a powerful tool for analysis, modeling, and simple object-oriented programming. I also obtained the knowledge of advanced algorithms including greedy algorithms and data structure including hash table, which are critical parts in the science of computer. In addition, I also explored the knowledge of theoretical computer science including Turing Machine and design of algorithms.

In the field of computer security, I had a good grasp of basic cryptography, access control, application security, system security, and digital forensics technique. During study for that knowledge, I can exploit flows of web applications and computer systems proficiently. I also did the forensics of a real-world phishing application.

To learn the knowledge of cryptography more deeply, I took the courses of theoretical cryptography at the Department of Mathematics. I fully learned how cryptosystems are carried out and the mathematical knowledge behind them including Number Theory, Abstract Algebra, and Elliptic Curve Cryptography. I also explored the more advanced cryptography topics including secure multiparty computation, homomorphic encryption, and zero-knowledge proof. I aimed to do research in those advanced cryptography topics in the future.

As a researcher, I am interested in research on succinct computational Integrity &privacy(SCIP), and its application to blockchain and cryptocurrency. SCIP and blockchain have a massive influence and applications on the society nowadays. To enrich my knowledge on the blockchain, I participate in the course of Blockchain and Cryptocurrency from Princeton University on the Coursera platform and gained the knowledge on blockchain, which plays a critical role in my research on blockchain.

3 Previous Academic Research

Blockchain and cryptocurrency technology is currently an advanced topic in the field of security in the distributed network. The original design of Bitcoin blockchain and Proof-of-Work(PoW) by ”Satoshi

Nakamoto" have shown some defects including increasing mining difficulty, less scalability, and lack of privacy due to the public ledger.

Up to now, I have conducted two research projects regarding the defects of the blockchain. The result of one project is a published paper "Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency" at IEEE Compsac 2018. The project aims to solve the problem of increasing mining difficulty. The key point of this paper is to introduce a "difficulty factor" to adjust the mining difficulty for different users according to the number of blocks they work out. As the co-author of this paper, I am mainly responsible for evaluating the performance of our protocol under different "difficulty factor", and complete the part of the introduction and preliminary which introduces the basic idea of our protocol and basic knowledge of bitcoin mining. The project is the first research project I participated in, I learned a lot about the process in conducting academic research and I was inspired a lot in different research aspects of blockchain technology while I read different papers about blockchain.

The other project was conducted solely. The result of this project is a poster "Estafette: A Parallelized Block Generation Protocol to increase the scalability of cryptocurrencies" at CryptoRally, Arizona State University. The project aims to solve the problem of scalability of Bitcoin blockchain via a parallelized block generation protocol. The key point of this poster is divided blocks into the parent block and child block. Child blocks are mined with partial previous hash and parent blocks are mined following the original Proof-of-Work. However, different targets are set for child blocks and parent blocks to ensure that one parent block and multiple child blocks are generated at the approximately same time. Unfortunately, this poster was not made to a full paper but I have the plan to refine the poster to a full paper in the future.

Currently, I am also carrying out a research with privacy in blockchain with a Post Doctoral Researcher. We aim to implement an efficient way to protect clients' privacy via zero-knowledge proof. Although Zerocash is a successful protocol to protect clients' privacy, it is still not efficient due to heavy computation. Zero-Knowledge proof is the best choice for us right now but we may adopt other cryptographic primitives to ensure higher efficiency and privacy.

4 Future Research

For my future research work, I would like to focus on designing efficient protocols to achieve Succinct Computational Integrity and Privacy (SCIP) and the application of SCIP on the public blockchain. Succinct Computational Integrity and Privacy is the concept that a prover computes a proof such that every other verifier can verify the proof without knowing the secret information of the prover in a succinct way. Protocols with SCIP enable good privacy in distributed network. Particularly, protocols with SCIP could solve the privacy and scalability issues of the current public blockchain. Users do not need to see the details of transactions when checking if a transaction is valid as they only need to verify the proof. Simultaneously, users can confirm the transaction if the proof is verified. Some research has been done to achieve SCIP in the distributed network including the famous Zcash which uses zk-SNARKS. Many cryptographic primitives are introduced in the protocols proposed to achieve SCIP. Nevertheless, they are usually computationally expensive to work out a proof. There is also research which tried to solve the problem by outsourcing computation to other workers to compute a proof and distributed Zero-knowledge proof such as DIZK. Designing efficient protocols to achieve SCIP on the public blockchain is my primary research direction in the future since I do conclude that it is necessary and revolutionary for the public blockchain.

In addition to SCIP on the public blockchain, I would also like to carry out research on other privacy-enhancing techniques on the public blockchain including distributed mixing schemes and manipulation of cryptographic primitives such as ring signature. Simultaneously, I would like to continue my research on mining difficulty, consensus protocol and scalability of the blockchain. Blockchain is the technology which could be adopted by different sectors for its good properties if the defects of blockchain could be reduced. Beyond the research on blockchain, I am also interested in the cryptographic protocols and design of new cryptographic primitives to provide security and privacy in the distributed network. As the ecosystem of the distributed network gets mature, it is critical to carry out research on the security and privacy of the distributed network to protect users' credentials and their privacy.