Cover letter

November 16, 2024

My name is Nan Cheng, a PhD student from the University of St. Gallen, conducting research under the supervision of Prof. Katerina Mitrokotsa. Prior to pursuing my PhD in Switzerland, I had spent six years working in the industry, primarily in software engineering, with some experience in administrative roles. My strong interest in cryptography led me to focus on this field since doing my Master's degree at Fudan University. At the Cybersecurity and Applied Cryptography Lab in St. Gallen, we research a wide range of topics, including functional encryption, private stream aggregation (PSA), private set union/intersection (PSU/PSI), and secure multiparty computation (MPC).

In my PhD research, I am motivated to identify and overcome practical efficiency bottlenecks, committed to exploring all means to achieve greater efficiency. Specifically, I have primarily worked independently on efficient multiparty computation (MPC) protocols for specific secure computation problems, focusing on reducing communication complexity and designing more efficient MPC schemes. This dedication has yielded promising results, resulting in several publications on the design and implementation of new MPC protocols. While my primary focus remains on MPC and its related area, I have broader interests in other areas too. Meanwhile, I am keeping up with the latest developments in zero-knowledge proofs (ZKP), having begun my exploration of this area this summer. This summer, I also attended the Privacy-Preserving Applied Cryptography Summer School organized by CISPA focusing on Anoymous credentials. Recently, I am visiting the Aarhus Crypto Group, where I am working with some collaborators to explore how to utilize pseudorandom correlated generation (PCG) to produce a wider variety of correlated randomness for MPC applications. We aim to generate daBits/edaBits with sublinear communication complexity. In addition to my research, I co-supervised a Master's thesis that outlined and compared various frameworks for secure inference evaluation using Function Secret Sharing.

My experience in software engineering has equipped me with a variety of skills, including proficiency in programming languages such as C/C++, Python, and Rust. Additionally, it has cultivated discipled programming habits, such as clear module design before coding, effective class and function abstraction, robust coding practices, and scalable interface design for future use. These experiences have also enhanced my patience with challenging problems, my logical approach to complex systems, and my adaptability to teamwork.

I have enjoyed my PhD journey so far, particularly the 'Eureka' moments that come with developing good ideas and the satisfaction of seeing my implementations surpass state-of-the-art solutions. However, I hope that by working with you, I can identify more interesting research problems in the blockchain world and contribute to them.