Journal & Proceedings of the Royal Society of New South Wales, vol. 155, part 2, 2022, p. 229. ISSN 0035-9173/22/020229-02

Thesis abstract

Contributions to blockchain-based security protocols

Yannan Li

Abstract of a thesis for a Doctorate of Philosophy submitted to The University of Wollongong, Wollongong, Australia

Blockchain is a prominent technology that revolutionises the way to do business and security, becoming a key advance worldwide. Dr Yannan Li's thesis focused on the design of blockchain-based secure applications. Specifically, she provided solutions in four essential scenarios: 1) regulation in blockchain-based cryptocurrencies, 2) blockchain-based decentralised e-voting, 3) contractual equivocation in blockchain; and 4) privacy protection in the stateless blockchain. Dr Li's thesis employs various advanced cryptographic techniques, including cryptographic commitments, zero-knowledge proofs, signatures of knowledge, verifiable encryption, cryptographic accumulators, and verifiable secret sharing, to design secure protocols and provide security proofs accordingly. All the protocols were implemented and the performance was provided to show the practicality of the proposal. Specifically, the four contributions of the thesis are listed as follows: First, Dr Li proposed Traceable Monero, to balance the anonymity and traceability in the system. As a result, the anonymity of an honest user is guaranteed, while a malicious user is subjective to be traced and identified for further penalty. The research outcomes have been published in IEEE Transaction on Dependable and Secure Computing (TDSC), a top journal in cybersecurity with CORE Rank A and IEEE Network, with impact factor 10.294. Second, Dr Li proposed a secure blockchain-based self-tallying voting system. No central party is required to tally the ballots and results can be calculated publicly while the privacy of all the ballots can be guaranteed. Besides, it satisfies fairness among all the users. This research outcome was published in IEEE TDSC, a top journal in cybersecurity with CORE Rank A. Third, Dr Li provided solutions for contractual equivocation in blockchain, which supports user-defined fine-grained policy-based equivocation. Dr Li presented a generic construction together with formal security proof. This paper was published in ACM ASIACCS, a top conference in cybersecurity with CORE Rank A. Fourth, Dr Li proposed mercurial subvector commitments and applied the new tool in stateless blockchain to capture privacy guarantee. A formal system and security models are provided, together with concrete construction. This research outcome was published in ACISP2021, a reputable conference in cybersecurity and this paper won the Best Paper Award. The research contributions of Yannan Li's PhD thesis is outstanding and the thesis is well-organised, as highlighted by the two external assessors whose expertise are in this research field. The thesis received the examiners' commendation for an outstanding dissertation and the Best Thesis Award in the Faculty of EIS, UOW.

In summary, Yannan's contributions to the research field as demonstrated in her PhD thesis have been outstanding, enabling further research in this area and will contribute to the blockchain industry. This thesis will attract further work in the area of blockchain, and its adoption in practice.

Dr Yannan Li
School of Computing and Information Technology
University of Wollongong

E-mail: yannan@uow.edu.au

URL: https://ro.uow.edu.au/theses1/1068/