Department of Computer Science
香港城市大學
City University of Hong Kong

COMPUTER SCIENCE COLLOQUIUM

Scalable Private Set Union: Faster and More Secure

SPEAKER **Prof Hong-Sheng Zhou**

Associate Professor
Virginia Commonwealth University
Richmond, Virginia
USA

DATE 15 June, 2023 (Thu)
TIME 10:30am – 11:30am
VENUE Y6405, CS Seminar Room, 6/F, Yellow Zone, Yeung Kin Man Academic Building, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon Tong, Hong Kong

ABSTRACT

A Private Set Union (PSU) protocol allows parties, each holding an input set, to jointly compute the union of the sets without revealing anything else. While it has found numerous applications in practice, not much research has been carried out so far, especially for large datasets.

In this talk, Prof Hong-Sheng Zhou will first present their recent result* in a USENIX Sec '22 paper: they take shuffling technique as a key to design PSU protocols for the first time. The result outperforms the state-of-the-art design by Kolesnikov et al. (ASIACRYPT 2019) in both efficiency and security; the unnecessary leakage in Kolesnikov et al.'s design can be avoided.

Prof Zhou will then present the result in an ongoing project: through a systematical investigation of PSU designs in literature to show that unnecessary information leakage occurs in all existing scalable PSU. Prof Zhou will then provide the first scalable PSU with best possible security in the semi-honest setting.

*(based on joint work with Yanxue Jia, Shi-Feng Sun, Jiajun Du and Dawu Gu, Shanghai Jiao Tong University)

BIOGRAPHY

Prof Hong-Sheng Zhou is an Associate Professor in the Computer Science Department at Virginia Commonwealth University. He was a postdoc at Maryland Cybersecurity Center under the direction of Prof Jonathan Katz. Before that, he received his PhD at the University of Connecticut with Prof Aggelos Kiayias as advisor.

Prof Zhou is interested in a wide range of topics in modern cryptography including Secure Multi-Party Computation, Blockchain Technologies, and Zero-Knowledge Proofs. He investigates cryptographic primitives and protocols in the complex environments aiming to achieve strong security guarantees including Composability, Leakage/Tampering/Subversion Resilience, Coercion Resilience, Fairness and Quantum Resilience. He has published a number of papers in top cryptography, security and distributed computing conferences, such as CRYPTO, EUROCRYPT, ASIACRYPT, ACM CCS, USENIX Security, and ACM PODC. Prof Zhou was a recipient of an NSF Computing Innovation Fellowship and a Google Faculty Research Award. His research has been funded by NSF and multiple industry research gifts.

All are welcome!

In case of questions, please contact Prof Cong WANG at congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at https://www.cs.cityu.edu.hk/events/cs-seminars/recent-cs-colloquiums .