北京大学前沿计算研究中心
Center on Frontiers of Computing Studies, Peking University

密码学课题组
学术报告

New Ways to Garble Arithmetic Circuits

Hanjun Li

PhD student
University of Washington

Host：刘天任 助理教授
2023年5月23日 星期二 16:00
静园五院204

Abstract

The beautiful work of Applebaum, Ishai, and Kushilevitz [FOCS'11] initiated the study of arithmetic variants of Yao's garbled circuits, where the circuits consist of Add, Mult, gates instead of logical XOR, AND gates. The wire values are elements in some ring R, with bit-length $|R|$. To measure efficiency, we define the rate of a garbling scheme as the maximal ratio between the size of the garbled circuit $|\hat{C}|$,and the cost of writing the computation in the clear $|C|*|R|$. In AIK's paper, they construct a scheme for arithmetic circuits over bounded integers under the LWE assumption, with rate $O(K_{LWE})$.

In this talk, I'll present two schemes:

- One for bounded integers, as in AIK, under the DCR assumption with rate O(1) for large domains.
- One for $\mathcal{Z}_P$ elements for any modulus p, under either LWE or DCR.

In our paper, we also have a variant of the first scheme supporting circuits that are augmented with Boolean computation (e.g., truncation of an integer value, and comparison between two values), while keeping the constant rate when garbling the arithmetic part.

Biography

Hanjun Li is a third year PhD student at University of Washington advised by Rachel (Huijia) Lin and Stefano Tessaro. His research interests lie in cryptography. Before coming to UW, he obtained his master's degree from Carnegie Mellon University, advised by Vipul Goyal.

http: //cfcs.pku.edu.cn/