Department of Computer Science, The University of Hong Kong

CS Seminar

Piano: Extremely Simple, Single-Server PIR with Sublinear Server Computation

Mingxun Zhou, PhD Candidate,
Computer Science Department,
Carnegie Mellon University

Date & Time:
June 30, 2023 (Friday)
2:00pm

Venue:
Rm 308, Chow Yei Ching Building, HKU

Abstract:

We construct a sublinear-time single-server pre-processing Private Information Retrieval (PIR) scheme with optimal client storage and server computation (up to poly-logarithmic factors), only relying on the assumption of the existence of One Way Functions (OWF). Our scheme achieves amortized sqrt(n) online server computation and client computation and sqrt(n) online communication per query, and requires roughly sqrt(n) client storage. Unlike prior single-server PIR schemes that rely on heavy cryptographic machinery such as Homomorphic Encryption, our scheme only utilizes lightweight cryptography such as PRFs, which is easily instantiated in practice. To our knowledge, this is the first practical implementation of a single-server sublinear-time PIR scheme. Compared to existing linear time single-server solutions, our schemes are faster by 10−300× and are comparable to the fastest two-server schemes. In particular, for a 100GB database of 1.6 billion entries, our experiments show that our scheme has less than 40ms online computation time on a single core.

Based on joint work with Andrew Park, Elaine Shi, Wenting Zheng.

About the Speaker:

Mingxun Zhou is a PhD student in the Computer Science Department at Carnegie Mellon University, advised by Elaine Shi and Giulia Fanti. His research focuses on privacy-preserving algorithm design, including differential private algorithms and cryptography. He also has research work on Blockchain technology, P2P network.

All are welcome!
For enquiries, please call 2859 2180 or email enquiry@cs.hku.hk
Department of Computer Science
The University of Hong Kong