CT Advanced Computing Center (CACC) Security Seminar Series 2024

Speaker: Yossi Gilad
Date: October 23, 2024
Time: 11- 12:30pm
Location: ITE 336
Meeting Link : https://uconn-cmr.webex.com/uconn-cmr/j.php?MTID=m4d36ddf4d36edd727aa04331cdb7d7f6

Meeting number (access code): 2633 368 4613

Meeting password: MqmJMizs533

Distributed PIR: Scaling Private Messaging via the Users’ Machines

This work presents a new architecture for metadata-private messaging that counters scalability challenges by offloading most computations to the clients. At the core of our design is a distributed private information retrieval (PIR) protocol, where the responder delegates its work to alleviate PIR's computational bottleneck and catches misbehaving delegates by efficiently verifying their results. We introduce DPIR, a messaging system that uses distributed PIR to let a server storing messages delegate the work to the system's clients, such that each client contributes proportional processing to the number of messages it reads. The server removes clients returning invalid results, which DPIR leverages to integrate an incentive mechanism for honest client behavior by conditioning messaging through DPIR on correctly processing PIR requests from other users. The result is a metadata-private messaging system that asymptotically improves scalability over prior work with the same threat model. We show through experiments on a prototype implementation that DPIR concretely improves performance by 3.25× and 4.31× over prior work and that the performance gap grows with the user base size.