Daniel Noble

I am a cryptography researcher. My research focuses on developing MPC protocols with the goal of real-world deployment. My dissertation topic was efficient memory access in MPC using Distributed ORAM (DORAM).

Experience

University of Pennsylvania, PhD Student. *Philadelphia, PA, USA*. May 2018 – May 2024
Research Assistant. *Philadelphia, PA, USA.* Oct 2017 – Apr 2018
Advised by Brett Hemenway Falk. In collaboration with Hastings and Zdancewic (IEEE S&P 2019), we investigated and evaluated frameworks (compilers) for secure multiparty computation. From this, I realized real-world general MPC deployment would require efficient protocols for accessing memory at secret-shared locations, a problem called Distributed Oblivious RAM (DORAM). We designed a new, efficient DORAM protocol (SCN 2022). While proving the protocol secure, I noticed a flaw in several other ORAM/DORAM protocols, resulting in the Alibi attack (Eurocrypt 2021). We then collaborated with Ostrovsky, Shtepel and Zhang (TCC 2023) to create a DORAM variant that was secure against malicious adversaries, and I took the lead in proving this protocol secure in the UC model. Most recently, we used the silent dot-product technique to build a DORAM with sub-logarithmic communication overhead. Falk and I have also worked on Proactive Secret Sharing (with Rabin, TCC 2023), applying MPC to differentially-private statistics (with Roth, Haeberlin, SOSP 2019) and Private-Set Intersection (with Ostrovsky, WPES 2019).
I was also a teaching assistant for Falk's Blockchain course and Rabin's seminar on Advanced Cryptography.

Silence Laboratories, Cryptography Consultant. *Singapore (remote)*. April 2023 – present.
Develop and evaluate cryptographic protocols for business-tailored MPC libraries. Participate in meetings with clients to clarify design requirements and provide technical guidance. Advise on protocol implementation. Primarily, I have developed application-appropriate protocols for consensus and weighted dynamic threshold signatures. I also gave a presentation at DeCompute 2023 on the necessity of professional ethics for the MPC industry.

Diversifi Technologies Ltd, Advisor. *Tel Aviv, Israel (remote).* March – May 2022.
Advised on technical design and whitepaper for decentralized exchange and associated distributed network.

Intuidex, Inc, Software Developer. *Bethlehem, PA, USA*. July 2015 – July 2017.
Full stack developer at data-analytic start-up Intuidex. Implemented new features in enterprise software product. Fixed defects. Established version control process for product database changes. Joined customer calls to provide technical insight and clarify design requirements. Supervised new developer. Installed product on customer sites. Initiated internal training demos to improve internal communication. Stack: Java, EJB, MySql, Mercurial.

Education

University of Pennsylvania, Ph.D., Computer and Information Science. *Philadelphia, PA.* May 2024

Yale University, B.S., Computer Science. *New Haven, CT.* May 2015

Research Publications (selected)

MetaDORAM: Breaking the Log-Overhead Information Theoretic Barrier. In submission. *Daniel Noble, Brett Hemenway Falk, Rafail Ostrovsky.*

DORAM revisited: Maliciously secure RAM-MPC with logarithmic overhead. TCC 2023. [Talk]. *Brett Falk, Daniel Noble, Rafail Ostrovsky, Matan Shtepel, Jacob Zhang.*

Proactive Secret Sharing with Constant Communication. TCC 2023. [Talk] *Brett Falk, Daniel Noble, Tal Rabin.*

Alibi: A Flaw in Cuckoo-Hashing Based Hierarchical ORAM Schemes and a Solution. EUROCRYPT 2021. [Talk] *Brett Hemenway Falk, Daniel Noble, Rafail Ostrovsky.*

SoK: General Purpose Compilers for Secure Multi-Party Computation. IEEE S&P (OAKLAND) 2019. *Marcella Hastings, Brett Hemenway, Daniel Noble, Steve Zdancewic.*