CV of Thomas Yurek

+1 (219) 577-6345 | yurek2@illinois.edu | tomyurek.web.illinois.edu

About

I am a 6th year PhD student (I just defended my thesis!) who is broadly interested in building tools and techniques to advance the state of the art in privacy and decentralization technologies. I am a member of UIUC's Decentralized Systems Lab, which focuses on building and analyzing robust and secure peer-to-peer systems.

Education

Purdue University — West Lafayette, IN
Bachelor of Science in Honors Computer Engineering, Mathematics, and Statistics — *May 2017*

University of Illinois — Champaign, IL
PhD in Computer Science, Advised by Dr. Andrew Miller — *Expected May 2023*

Work Experience

Cryptographic Consultant — October 2022 - Present
Bolt Labs — *Baltimore, MD*

- Working with the team at Bolt Labs to bring the Threshold ECDSA library I open sourced from Meta up to production readiness

Research Scientist Intern — May - August 2022
Meta — *Menlo Park, CA*

- Worked on deploying a UC-secure Threshold ECDSA Signing system

Research Scientist Intern (part time) — October 2021 - May 2022
NTT Research — *Sunnyvale, CA*

- Worked on developing an optimally fault-tolerant asynchronous protocol for securely transferring secret shares between committees

PhD Software Engineering Intern — May - August 2021
Facebook — *Menlo Park, CA*

- Implemented a robust secret sharing library for internal use in privacy projects
- Assisted in the design and implementation of a privacy-preserving fuzzy matching system

Design Automation Engineer Intern — May - July 2015
Intel — *Hillsboro, OR*

- Architected and programmed an in-house framework to detect system failures and perform an appropriate action
- Developed primarily with Moose, an Object Oriented system for Perl

Design Engineering Intern — May - August 2014
Advanced Micro Devices — *Boxborough, MA*

- Learned how to analyze sequential digital circuits
- Wrote HSPICE control files to simulate different signal transitions
- Maintained Perl scripts to run these analyses and wrote scripts for data collection

Software Engineering Intern — June - December 2013
Rockwell Collins — *Cedar Rapids, IA*

- Debugged and tested software and hardware for RF communication
- Worked with Java, C#, and Python to develop and validate software
- Flew out to another company to answer questions about our product

Current Research

SGXonerated: Finding (and Partially Fixing) Privacy Flaws in TEE-based Smart Contract Platforms Without Breaking the TEE [Major Revision, PETS]

- An exploration of prevalent weaknesses in production SGX-on-Blockchain systems which can be exploited without knowing any unpatched SGX vulnerabilities
- By leveraging privacy leakage in transaction simulations, we demonstrate how attackers could extract MEV or even decrypt transaction amounts altogether

SGX.Fail: How Secrets Get eXtracted [Major Revision, IEEE S&P]

- An analysis of how a series of cascading failures causes practitioners to choose between application security and usability
- Case study includes a complete break of all of the privacy features of Secret Network

Comparing Programming Paradigms for Proof Systems [In Progress]

- A more systemic comparison of how different SNARK arithmetizations (specifically, R1CS and AIR both with and without RAM) affect the performance of different types of programs when all other variables (such as the FFT library and polynomial commitment scheme) are kept constant

Fully Robust Asynchronous Multiparty Computation with Linear Network Overhead [In Progress]

- Addresses a gap in prior work to allow for optimally fault-tolerant and efficient generation of multiplication triples

Previous Research

Long Live The Honey Badger: Robust Asynchronous DPSS and its Applications [Usenix Security]

- Design and implementation of the first optimally fault-tolerant asynchronous scheme to securely transfer secret shares between committees
- Includes a high-threshold DPSS algorithm, as well as an asymptotically-optimal batched algorithm

Practical Asynchronous Distributed Key Generation [IEEE S&P]

- The first asynchronous distributed key generation scheme practical enough to make an implementation worthwhile
- Matches best-known bandwidth for ADKG while providing a more generally useful output

hbACSS: How to Robustly Share Many Secrets [NDSS]

- Design and implementation of an efficient Asynchronous Complete Secret Sharing scheme for use in multiparty computation
- Achieves optimal asymptotic bandwidth for the first time. Matches computational performance of state of the art while using weaker assumptions and avoiding trusted setup

HoneyBadgerMPC and AsynchroMix: Practical Asynchronous MPC and its Application to Anonymous Communication [ACM CCS]

- Design and implementation of a one-round mixing scheme built upon fault-tolerant MPC
- Part of overall work to develop a robust multiparty computation framework

Reactive Redundancy for Data Destruction Protection (R2D2) [Computers & Security]

- Exploration of defenses against antiforensic techniques at the hypervisor level of a Virtual Machine
- Our solution involved creating snapshots of files just before they were overwritten by a malicious payload