CV of Thomas J. Yurek

1212 Boxwood Drive / Munster, IN 46321 / yurek2@illinois.edu / +1 (219) 577-6345

I am a PhD student who is broadly interested in privacy and applied cryptography. I am a member of UIUC's Decentralized Systems Lab, which focuses on building and analyzing robust and secure peer-to-peer systems. My recent research activity has been related to asynchronous, byzantine fault-tolerant multiparty computation.

Education

University of Illinois, Champaign IL, USA — May 2023
PhD Student under Dr. Andrew Miller

Purdue University, West Lafayette, IN, USA — May 2017
Bachelor of Science in Honors Computer Engineering, Mathematics, and Statistics
Minor in Global Engineering Studies

Work Experience

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

- 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

Thundercore, Sunnyvale CA, USA — May 2019 - July 2019
Research Intern

- Developed new cryptographic protocol for random number generation in a trustless blockchain setting

Intel, Portland, OR, USA — May 2015 - July 2015
Design Automation Engineer Intern

- 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

Advanced Micro Devices, Boston, MA, USA — May 2014 - August 2014
Design Engineering Intern

- 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

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

- 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

hbACSS [In Submission, NDSS]

- Design and implementation of an efficient Asynchronous Verifiable 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

Previous Research Projects

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]
Prof. Saurabh Bagchi, Purdue University

- Did research looking at 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

Cryptanalysis of a Hardware VPN Device
Prof. Nadia Heninger, University of Pennsylvania

- Analysis of faulty random number generation in some VPN devices and how it can be used to decrypt encrypted connections
- Gained proficiency with mathematical libraries commonly used for cryptography

Laser Fault Injection Against AES-NI
Prof. Christof Paar, Ruhr-Universität Bochum

- Implementation a theorized side-channel attack against AES-NI using a laser that can only target groups of transistors due to optical limitations
- Learned to use laser equipment and programmable nanopositioning technology

Continuous Analysis of Many CAMeras (CAM^2)
Prof. Yung-Hsiang Lu, Purdue University

- Processed information from tens of thousands of livestreaming cameras around the world to make predictions for weather, traffic, the environment, and more
- Implemented a system to gather and display weather data associated with webcameras
- Implemented a scalable server to store and quickly retrieve large quantities of data