Xiuyu **Ye**

PhD. Student · Cryptography · Security

☎ (+1) 765-407-0642 | ✉ ye151@purdue.edu | ⌂ https://darahye.github.io/

Education

Purdue University
West Lafayette, IN

B.S. in Computer Science, Mathematics and Statistics *Aug. 2015 - May. 2020*

- With concentration in System Programming, Security, Computer graphic and visualization, Foundations of Computer Science

Purdue University
West Lafayette, IN

PhD. in Computer Science *Aug. 2020 - present*

- Specializing in Leakage Resilient Cryptography, Information theoretic cryptography

Experience

Research and Publications in Leakage Resilient Cryptography

Main Area of Research *Aug. 2021 - present*

- Studies leakage resilience of secret sharing scheme under the local leakage model and characterizes the unintended information revelation about the secret by obtaining independent leakage from each secret share. Investigates the distinguishing advantage between the distribution of secret shares under physical-bit local leakages.

Graduate Teaching Assistant: Cryptography

CS355, CS555 (graduate) *Aug. 2021 - May. 2023*

- Assisted in constructing assignments and exams, guiding students in understanding mathematical foundations of cryptography and various cryptographic concepts in private and public key cryptography, secret sharing schemes, PRG/PRF, OWF, MAC, digital signatures, secure multiparty computation, etc.

Graduate Teaching Assistant: System Programming

CS252, CS503(OS) *Aug. 2020 - May. 2021*

- Provided mentorship to students in writing large class projects like malloc, bash shell, http severs, and web applications.
- Created long term class projects in XINU regarding process management and synchronization, virtual memory and file system.

Software Development Engineer

Aptiv Technology Partners, LLC *May. 2018 - Aug. 2018*

- Used $C\#$ to develop a terminal that translates the signal transmitted from the car engine simulator to physically meaningful car specifications.

Publications

Security of Shamir's Secret-sharing against Physical Bit Leakage: Secure Evaluation Places
Draft

Hemanta Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and **Xiuyu Ye**

-

Leakage-resilient Linear Secret-sharing against arbitrary Bounded-size Leakage Family
TCC 2022

Hemanta Maji, Hai Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, **Xiuyu Ye**, and Albert Yu

Tight Estimate of the Local Leakage Resilience of the Additive Secret-sharing Scheme and its Consequences
ITC 2022

Hemanta Maji, Hai Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, **Xiuyu Ye**, and Albert Yu

Presentation

Midwest Crypto Day 2023

UIUC

PRESENTATION ON IMPROVING THE SECURITY OF SHAMIR'S SECRET-SHARING *April. 2023*

- Present the explicit algorithm to characterize modulus and evaluation places that make Shamir's secret-sharing scheme robust to physical bit leakage attack.

Related Courseworks

Advanced Cryptology

CS655 *Jan. 2023 - May. 2023*

- Studied Concrete Security Analysis, Idealized Models, Preprocessing Attacks and Lower Bounds, Proofs of Space, Proofs of Sequential Work, Memory Tight Reductions, Memory Hard Functions, Oblivious RAM, Obfuscation, Functional Secret Sharing, Quantum Random Oracle Model and Compressed Oracles, Fully Homomorphic Encryption