

HAOBIN (HIROKI) CHEN

(+86) 183 5825 6853 ◇ haobchen@iu.edu ◇ <https://hiroki-chen.github.io>

EDUCATION

Indiana University Bloomington, IN, USA

2023-2028(*Expected*)

Ph.D. in Computer Science

Nankai University, Tianjin, China

2019-2023

B.Eng. in Information Security, GPA: 3.68/4.0, Rank: 7/53

RESEARCH INTERESTS

Computer security; Data privacy; System security; Formal methods; Privacy-enhancing technologies

ACADEMIC EXPERIENCE

Proof of Being Forgotten: Rust-SGX based Enclave Verification Framework

May 2022 - Jun. 2023

Research Assistant Advised by: Prof. Xiaofeng Wang & Dr. Mingshen Sun

Remote Intern

Our goal is to offer an off-the-shelf solution for providing users that the enclave application is verified by Proof of Being Forgotten (PoBF). It refers to a kind of regulation enforcing that code dealing with secrets is verified so that secrets are completely consumed, and no secret is leaked to any unauthorized party.

- Implementing algorithms and allocators for cleaning secret residues in Intel SGX with Rust.
- Implementing type state transfer for secrets in the enclave.
- Learning Coq to formally verify the execution model.

Encrypted Database

Sept. 2020 - Jan. 2023

Research Assistant Advised by: Prof. Zheli Liu

Nankai University

Our goal is to construct a fully encrypted database that allows for efficient queries on ciphertext while providing strong security guarantees.

- Proposed novel encryption schemes for encrypted databases and implemented them in CryptDB.
- Collaborating with Huawei Inc. in making theoretical models practical and viable in real-world applications.
- Leveraging secure enclaves to reduce the overhead and improve the performance of encrypted databases.

Oblivious RAM and Databases Based on Secure Enclaves

Aug. 2021 - Aug. 2022

Research Assistant Advised by: Prof. Zheli Liu

Nankai University

Our goal is to design Oblivious RAM with the support of the Trusted Execution Environment (TEE) and provide protection against access pattern leakage for the databases.

- Implemented searchable symmetric encryption for a cloud file system called SEAL using PathORAM and oblivious data structures.
- Proposed novel notions of obliviousness called *program obliviousness* for TEE-based ORAMs.
- Designed novel and light-weighted recursive doubly Oblivious RAM based on Intel SGX.

INDUSTRIAL EXPERIENCE

Our goal is to integrate the state-of-the-art policy compliance data access and analysis framework into Teaclave and allow for verification of policy enforcement.

PUBLICATIONS

- Hongbo Chen, **Haobin Hiroki Chen**, Mingshen Sun, Kang Li, Zhaofeng Chen, Xiaofeng Wang. A Verified Confidential Computing as a Service Framework for Privacy Preservation. In *USENIX Security 2023*.
- **Haobin Chen** and Siyi Lv. Revisiting Frequency-Smoothing Encryption: New Security Definitions and Efficient Constructions. Submitted to *Cybersecurity*.

SKILLS

Typesetting Document	Latex, Markdown
Programming	Rust (Proficient), C/C++ (Proficient), Makefile, CMake, Coq, Shell, Java, Python, PHP, Bash

HONORS AND AWARDS

- 2021 The 3rd prize at the **National College Student Information Security Contest**, Shandong University (Highest undergraduate contest for information security, < 8%)
- 2021 **Nankai Excellent Community Immersion Project** (< 10%)
- 2021, 2022 **Nankai Academically Excellent Student Scholarship** (Awarded to undergraduate students with excellent academic performance, < 5%)
- 2021, 2022 **Nankai Innovation Award of Technology and Research Scholarship** (Awarded to undergraduate students with outstanding research potential, < 3%)
- 2022 **Nankai Outstanding Innovation Project** (Awarded to undergraduate students who participated in outstanding research projects. < 15%)
- 2023 **Nankai Distinguished Bachelor Thesis Award** (< 3%)

TALKS

- 1 **Introduction to Zerocoin: An Anonymous and ZKP-Based E-Cash from Bitcoin**
Presented at course CSSE0014 *Security Protocols and Their Design*
- 2 **How Does the Compiler Work: A Brief Introduction to the LLVM Framework**
Presented at course COSC0017 *Compilers Design*
- 3 **Introduction to the Encrypted Databases**
Presented at course UPEC0990 *Database and Its Applications*
- 4 **The Linux Kernel Fuzzing**
Presented at course CSSE0004 *Software Security*

PROJECTS

- 1 FH-CryptDB (with ~ 6,000 lines of C++ code).
Link: https://github.com/hiroki-chen/FH_cryptDB

- 2 SSE-SEAL: An implementation of the paper *Demertzis et al. SEAL: Attack Mitigation for Encrypted Databases via Adjustable Leakage* (with $\sim 3,000$ lines of C++ code).
Link: <https://github.com/hiroki-chen/SSE-SEAL>
- 3 SO₂: A recursive doubly oblivious RAM bootstrapping on SGX. (with $\sim 4,000$ lines of C++ code).
Link: <https://github.com/hiroki-chen/SGXOram>
- 4 Inference attacks against encrypted databases.
Link: <https://github.com/hiroki-chen/FrequencyAttack>
- 5 A compiler for SysY (a C-like language).
Link: <https://github.com/hiroki-chen/NKUCompiler>
- 6 Oblivious-RAM: Reference Implementation for Different ORAM algorithms.
Link: <https://github.com/hiroki-chen/Oblivious-RAM>
- 7 NeoOS: An Unix-Like Kernel in Rust.
Link: <https://github.com/hiroki-chen/NeoOS>