λ HAOBIN (HIROKI) CHEN λ

+1 (812) 325-6706 ⋄ haobchen@iu.edu ⋄ https://hiroki-chen.github.io

EDUCATION

Indiana University Bloomington, IN, USA *2023-2028(Expected)*
Ph.D. student in Computer Science, Advisor: XiaoFeng Wang

Nankai University, Tianjin, China *2019-2023*
B.Eng. in Information Security

RESEARCH INTERESTS

Computer security & privacy; System security; Formal verification & PL; Privacy-enhancing technologies

ACADEMIC EXPERIENCE

Center for Distributed Confidential Computing (CDCC) Aug. 2023 -
Research Assistant Advised by Prof. XiaoFeng Wang *Indiana University Bloomington*

Center for Distributed Confidential Computing (CDCC) is an academic project aiming to lay the technical foundations for scalable data-in-use protection on cloud and edge systems. It is a multi-institution project sponsored by the Secure and Trustworthy Cyberspace Frontiers Program of the National Science Foundation.

- Using Coq to verify security-critical systems
- Designing cutting-edge hardware-assisted (e.g., CPU and GPU TEEs) technologies for data protection.
- Optimizing and accelerating secure systems for better runtime performance.

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*

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.
- Learning and implementing differential privacy techniques to anonymize the user's sensitive data.

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

Privacy Innovation Lab, TikTok Inc. May 2024 - Aug. 2024
Research Intern mentored by Dr. Mingshen Sun *San Jose, CA*

TBD.

GSoC: Apache Teaclave (incubating) and Privacy Policy Enforcement Jun. 2023 - Nov. 2023
Mentored by Dr. Mingshen Sun *Remote*

Our goal is to offer a state-of-the-art data analysis solution to solve privacy regulatory problems such as data privacy policy enforcement with the support of TEEs. We also aim to formally verify the framework so that it can be trusted and used with more confidence.

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 *Proceedings of the 32nd USENIX Security Symposium* (**Sec'23**), August, 2023.

SKILLS

Typesetting Document	Latex, Markdown
Programming	Rust (Proficient), C/C++ (Proficient), Python, Java
FP & Verification	Coq (Proficient), OCaml (Intermediate), Haskell

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** ($< 3\%$)

2023 **The 3rd Prize and Regional Outstanding Award at the National Contest for OS Design and Implementation**
(as mentor for the team, $< 2\%$)

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 $\sim$ 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 SO_2: 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`

8 Proof of Being Forgotten.
Link: `https://github.com/ya0guang/pobf`