

# HAOBIN CHEN

(+86) 183 5825 6853 ◇ haobin\_chen@mail.nankai.edu.cn ◇ <https://hiroki-chen.github.io/>

## EDUCATION

---

**Nankai University, Tianjin, China**

2019-2023(Expected)

B.Sc in Information Security

Overall GPA: 3.68/4.0(87.78%, Top 10%)

### Core Courses

Data Structures (4.0/4.0), Java Programming Language (4.0/4.0), High-Level Programming Language (C++, 4.0/4.0), Operating System (4.0/4.0), Computer Organisation and Design (4.0/4.0), Database System (4.0/4.0), Cryptography (4.0/4.0), Security Protocols and Their Design (4.0/4.0), IoT Security (4.0/4.0)

## RESEARCH INTERESTS

---

Computer Security; Data Privacy; Applied Cryptography; Security Protocols

## EXPERIENCE

---

### Encrypted Database

September 2020 - Present

Research Assistant Advised by: Prof. Zheli Liu

Nankai University & Huawei Inc.

Our goal is to construct a fully encrypted database that allows for efficiency query 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

August 2021 - August 2022

Research Assistant Advised by: Prof. Zheli Liu

Nankai University

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

- Implemented searchable symmetric encryption for 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.

**Paper in progress: SO<sub>2</sub>: An SGX-Based Doubly Oblivious RAM with Small Client Storage.**

---

### Intelligent Service Platform for Residential Communities

March 2021 - Dec 2021

Advised by: Prof. Peng Nie

Donghui Dongrui Community, Tianjin, China

Our goal is to solve the real-world problems faced by communities consisting of senior residents.

- Developing an online platform that provides residents with one-stop services to make their lives more convenient.
- Focusing on deploying the encrypted database as the data storage and secure encryption schemes to ensure data privacy for sensitive information.

---

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

August 2022 - Present

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 enclave.
- Learning Coq to formally verify the execution model.

## TECHNICAL STRENGTHS

---

<b>Website</b>	HTML5, CSS, JavaScript, and Bootstrap
<b>Typesetting Document</b>	Latex, Markdown
<b>Programming</b>	C/C++ (Proficient), Makefile, CMake, Coq, Shell, Java, Python, PHP, Bash
<b>Frameworks</b>	Google Remote Procedure Call (gRPC), Intel Software Guard eXtension (SGX), Yii2, SpringBoot, Yara, Yacc & Bison
<b>Platforms</b>	Linux Programming (proficient) and shell commanding
<b>Softwares</b>	Git, IDA Pro, OllyDbg, WinDbg, LLVM

## HONORS AND AWARDS

---

- 2021 The 3<sup>rd</sup> 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 **Nankai Academically Excellent Student Scholarship** (Awarded to undergraduate students with excellent academic performance, < 5%)
- 2021 **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%)

## 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](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<sub>2</sub>: 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>