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 - Present

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$_2$: 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.

TECHNICAL STRENGTHS

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

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 **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`

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`

LANGUAGE SKILLS

iBT-TOEFL (Reading: 30, Listening: 27, Writing: 27, Speaking: 27)

GRE (Verbal Reasoning: 162, Quantitative Reasoning: 168, Analytical Writing: 4)