Chenhao Bao

https://bchyes.github.io/| M: +(86) 158 6806 0965 | bch123@sjtu.edu.cn

EDUCATION

Shanghai Jiao Tong University **Shanghai, China**

Bachelor of Engineering in Computer Science and Technology Aug. 2021 – Jun. 2025(expected)

- Member of ACM Honors Class, which is an elite CS program for top 5% talented students
- **GPA:** 3.94 / 4.3, **rank:** 8 / 33
- **Relevant Coursework:** Algebraic Structures(95), Honor Mathematical Analysis(99), Graph Theory and Combinatorics(96), Programming(95), Honor Linear Algebra(93), Scientific Computation(95), Design and Analysis of Modern Algorithms(94), Probability(97), Optimization Methods(A+), Topics in Modern Algorithms(99), Computational Complexity(95), Quantum Computation(A-), Blockchain technologies(96), Information Theory(99).

EXPERIENCE

Brown University **Providence, RI, USA**

Student Intern in Cryptography, advised by Prof. Peihan Miao Jul. 2024 – Present

- Conducting research in applied cryptography with a specific interest in enhancing the speed of facial recognition processes while ensuring privacy protection.

Shanghai Jiao Tong University **Shanghai, China**

Undergraduate Researcher in Cryptography, advised by Prof. Shengli Liu Jun. 2023 – Present

- Engaged in a discussion group of Secure Multi-party Computation (MPC) protocols, based on *A Pragmatic Introduction to Secure Multi-Party Computation*.
- Participated in a discussion group focused on lattice-based cryptography, based on the lecture note of *CS 395T: Topics in Cryptography*.
- Developed a generic two-factor authenticated key exchange scheme that enhances security by achieving zero-knowledge properties and implemented quantum-resistant security.

RESEARCHING EXPERIENCE

Biometric-Based Two-Factor Authentication and Key Generation

Member Oct. 2023 – Sept. 2024

- Studied aPAKE, digital signatures, and secure sketch in detail, and improved upon previous single-factor schemes based on aPAKE to design the current generic two-factor scheme.
- Defined an enhanced security model that satisfies not only authentication and indistinguishability but also zero-knowledge properties, ensuring that public data, stored database information, and transcripts do not leak any sensitive biometric information.
- Implemented quantum-resistant instantiations for each component, achieving a quantum-secure scheme, and analyzed the scheme's efficiency based on these instantiations.
- The work is now submitted to ACNS.

Implementation and comparison of gas tracing algorithms for dual robots in confined space

Member Mar. 2023 – Feb. 2024

- Conducted a thorough investigation of existing algorithms, performing efficiency testing and comparisons within real-world simulation environments.
- Developed and proposed an improved hybrid approach combining Whale Optimization Algorithm and E. coil Optimization Algorithm specifically for dual-vehicle scenarios.

WORKING EXPERIENCE

Design and Analysis of Modern Algorithms **Shanghai, China**
Teaching Assitant guided by Prof. Yuhao Zhang Sept. 2023 – Feb. 2024

- Helped students understand algorithm architecture and guided them in analyzing efficiency using theoretical approaches, while grading assignments and providing constructive feedback to enhance their problem-solving skills.

Algebraic Structures **Shanghai, China**
Teaching Assitant guided by Prof. Shengli Liu Mar. 2023 – Jun. 2023

- Assisted students in understanding fundamental concepts of algebraic structures, such as groups, rings, and fields, and supported the professor in creating and reviewing final exam questions to ensure comprehensive assessment of key course topics.

Academic Center **Shanghai, China**
Member Sept. 2022 – Jan. 2023

- Organized and coordinated events, including lectures and discussion panels, fostering an environment for intellectual exchange and collaboration.

COURSE PROJECTS

RISC-V CPU **Shanghai, China**
Self-Contributor [repo] Sept. 2022 – Feb. 2023

- FPGA circuit implementation of RISC-V CPU of Tomasulo out-of-order-execution algorithm, written in iVerilog.

Mx* Complier **Shanghai, China**
Self-Contributor [repo] Sept. 2022 – Feb. 2023

- Engineered a compiler that compiles a C-and-Java-like language Mx* to LLVM Intermediate Representation and RISC-V assembly, written in Java.

Train Ticket Management System **Shanghai, China**
Co-Contributor [repo] May 2022 – Jul. 2022

- Designed a train ticket system with multi-user support and privilege management. I implemented the backend and built a B+ tree storage. All used C++ STL data structures are from scratch (including map, and queue).

Bookstore Management System **Shanghai, China**
Self-Contributor [repo] Dec. 2021 – Jan. 2022

- Developed a Bookstore Management System utilizing block-linked lists to efficiently maintain user and book information and implemented various functionalities to support a wide range of bookstore operations.

SKILLS, LANGUAGES & AWARDS

Awards:

- **Zhiyuan Honors Scholarship** 2021, 2022, 2023 (Top 2% in Shanghai Jiao Tong University)
- **SJTU Merit Scholarship** - C level 2022, 2023
- **National High School Mathematics League Second Prize** 2020

Languages: Native in Chinese; Fluent in English (TOEFL: 107); Basic in Japanese
Technical Skills: C++/Python/Java/Go/Verilog/Matlab/LaTeX/Markdown