

Shen Dong

Email: shen-dong@sjtu.edu.cn, ds111@illinois.edu

<https://github.com/RabbitCabbage>

EDUCATION

Shanghai Jiao Tong University (SJTU)

2021 - 2025 (*Expected*)

Bachelor of Engineering in Computer Science

Member of ACM Class, an elite CS program for the top 5% talented students. GPA: 3.8/4.3.

RESEARCH EXPERIENCE

Coordinated Science Laboratory, UIUC

Supervised by [Prof. Yupeng Zhang](#)

Jul 2024 - Now

Working on zk-friendly hash functions and developing new efficient and scalable zero-knowledge proof protocols with applications in machine learning fairness.

Lattice Cryptography and System Security Laboratory, SJTU

Supervised by [Prof. Yu Yu](#)

Sep 2023 - Now

Exploring topics of post-quantum cryptography including code-based cryptography and lattice-based cryptography, and other fields in cryptology like Multi-Party Computation and Zero-Knowledge Proofs.

TEACHING EXPERIENCE

Teaching Assistant of Computer Architecture, SJTU

instructed by [Prof. Alei Liang](#)

Sep 2023 - Jan 2024

Teaching Assistant of Principle and Practice of Computer Algorithms Course, SJTU

guided by [Prof. Yong Yu](#)

Jun 2023 - Jul 2023

Teaching Assistant of Data Structure Course, SJTU

instructed by [Prof. Huiyu Weng](#)

Feb 2023 - Jun 2023

OTHER EXPERIENCE

The 2024 Cryptography Summer Camp, Shanghai

held by [Shanghai Qi Zhi Institute](#)

Jul 2024

participated in the summer camp, which is a 1-week program for top students interested in Cryptography, attended in lectures and discussions on different fields of Cryptography.

2023 SJTU-THU-PKU Computer Science Summer School, Shanghai

held by [Zhiyuan College, SJTU](#)

Jul 2023

participated in the summer school, which is a 2-week program for top CS students in China, attended in lectures and discussions by winners of Turing award and professors from University of Illinois at Urbana-Champaign, Northwestern University, Chinese University of Hong Kong, etc.

PREPRINTS

A Simple Post-Quantum Oblivious Transfer Protocol from Mod-LWR

S. Dong, H. Cui, K. Zhang, K. Yang, Y. Yu

- We construct a simple, efficient OT protocol based on Saber, a Mod-LWR-based key exchange protocol. Our implementation outperforms the state-of-the-art Kyber-based post-quantum OT protocol by Masny and Rindal (CCS'19) in terms of both computation and communication costs.
- [Preprint on eprint](#), toy trial still being refined.

PROJECTS

Java-and-C-like Language Compiler (~32K lines in Java) [\[github\]](#)

A basic compiler implemented, which can convert codes of program written by a Java-and-C-like language to an AST. It enables semantic check, transformation to LLVM IR, and eventually transformation to RISC-V assembly. Some optimization is still on the way.

RISC-V CPU of Tomasulo Architecture (~1.3K lines in Verilog) [\[github\]](#)

An out-of-order CPU including I-cache, a 2-bit saturating counter branch predictor, and a write buffer implemented to improve the performance. The CPU could run successfully on an FPGA board.

Train Ticket Booking System (co-woker) (~26K lines, backend in C++) [\[github\]](#)

A project co-worked with classmate aims to provide a train ticket booking system. B plus tree was implemented to work as backend to store numerous train data. Front end was consist of html, providing beautiful UI which once worked on a server.

Database Management System BusTub of CMU (private) [\[github\]](#)

BusTub is a relational database management system built at Carnegie Mellon University for the Introduction to Database Systems (15-445/645) course, which supports basic SQL and comes with an interactive shell. Concurrency control for distributed systems is completed.

HONORS AND AWARDS

Zhiyuan Honorary Scholarship, Award for top 5% students *2021, 2022, 2023, 2024(expected)*

SKILLS AND SELECTED COURSES

Programming Languages: C/C++ , Python , Java and RISC-V assembly and Verilog.

Math: Calculus, Linear Algebra, Abstract Algebra, Algorithms, Mathematical logic, Probability Theory, Graph and Combinatorics, Data Mining, Computation Complexity and Quantum Computing.

English: TOEFL 105(R30, L24, W27, S24), GRE 324(V150, Q170, W4).

Selected Courses: Topics in Advanced Algorithms (CS3936): 98/100, Computational Complexity Theory (CS3954):95/100, Modern Cryptography (NIS3352): 94/100, Cryptography in Blockchain(CS2914): 95/100, Model Checking (CS3959): 97/100, Quantum Computing (CS3960): A, Data Mining (CS2912): 97/100, Mathematical Analysis (MATH1607): 97/100, Design of Computer System (CS2913): 95/100.