Shen Dong

Email: sd2273@cornell.edu
Website: rabbitcabbage.github.io

EDUCATION

Cornell Univeristy *Sep 2025 - Present*
Ph.D. student in Computer Science
Advised by Prof. Nicholas Spooner

Shanghai Jiao Tong University (SJTU) *Sep 2021 - Jun 2025*
Bachelor of Engineering in Computer Science, member of ACM Class

RESEARCH EXPERIENCE

Coordinated Science Laboratory, UIUC
Supervised by Prof. Yupeng Zhang *Jul 2024 - Dec 2024*

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 - Aug 2025*

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.

PUBLICATION

FAIRZK: A Scalable System to Prove Machine Learning Fairness in Zero-Knowledge
T. Zhang, **S. Dong***, O. Deniz Koze*, Y. Shen, Y. Zhang*

- We develop efficient zero-knowledge proof protocols for common computations involved in measuring fairness of logistic regression and DNN with tighter bounds. Our prover time is improved by 3.1×–1789× depending on the size of the model and the dataset.
- I worked with co-authors to develop a new tighter bound, implemented spectral norms, aggregated statistics and our new bound in Zero-Knowledge Proofs, which are the most critical gadgets of the experiments, and conducted all experiments to compute fairness bound results from models in plaintext.
- Accepted by S&P 2025.

PREPRINT

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.
- I designed the main base OT protocol, implemented our new design and other protocols for comparison under emp-ot framework, and participated to most part of paper writing and revising.
- Preprint on eprint.

TEACHING EXPERIENCE

Teaching Assistant, Data Structures and Functional Programming, Cornell
CS3110 lectured by Prof. Dexter Kozen and Ayaka Yorihiro *Jan 2026 - May 2026*

Teaching Assistant, Introduction to Cryptography, Cornell
CS4830 lectured by Prof. Noah Stephens-Davidowitz *Sep 2025 - Dec 2026*

Teaching Assistant, Project RISC-V Tomasulo CPU of Computer Architecture, SJTU
CS2951 instructed by Prof. Alei Liang *Sep 2023 - Jan 2024*

Teaching Assistant, Principle and Practice of Computer Algorithms, SJTU
CS1952-1 guided by Prof. Yong Yu *Jun 2023 - Jul 2023*

Teaching Assistant, Data Structure, SJTU
CS1951 instructed by Prof. Huiyu Weng *Feb 2023 - Jun 2023*

PROJECTS

Post-Quantum Oblivious Transfers in emp-ot Framework [github]

Implementations in C/C++ of post-quantum oblivious transfers under emp-ot framework, including a new Naor-Pinkas-like 1-out-of-2 OT protocol and a new Simplest-like 1-out-of-2 OT protocol based on SABER, and Masny-Rindal 1-out-of-2 OT protocol based on SABER and CRYSTALs-Kyber.

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-worker) (∼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.

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, Computational Complexity and Quantum Computing.

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