Shen Dong

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

EDUCATION

Cornell Univeristy *Starting Aug 2025*
PhD student in Computer Science

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

RESEARCH INTERESTS

My exploration spans theoretical foundations, protocol design, and practical cryptography implementations, focusing on **post-quantum primitives and efficient zero-knowledge proofs (ZKP)**. I hope to explore more facets of cryptography, which drives my pursuit of a PhD degree in the future.

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 - 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.

PREPRINTS

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.

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.

OTHER EXPERIENCE

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

Maintained and coordinated a homework project of RISC-V Tomasulo CPU, taught supplementary classes about the mentioned project, reviewed codes, answered questions and organized discussions.

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

Spearheaded a project homework of tomasulo simulator, answered questions and organized discussions, reviewed students' code by testing and QA.

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

Taught basic algorithm class, designed and assigned several algorithm problems as homework, checked and revised questions for weekly algorithm competition, assigned coding projects of data structures and reviewed students' code, revised and graded exams.

PROJECTS

LPN Estimator (co-worker) [website]

A tool to estimate the bit security of LPN instances. One can input the scale of LPN instantiations and the noise distribution, and it will give you an estimation of the bit security level based on some known attacks.

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.

HONORS AND AWARDS

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

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).