Yunhao Wang

Department of Computer Science, Columbia University | 11004 100th Ave NE, Kirkland, WA, 98033
yw3736@columbia.edu | Phone: (206)-419 4394

EDUCATION

Columbia University, New York *Sep 2021 – Present*
Master of Computer Science, Thesis Track, Advanced Research Program
GPA: 4.12/4.0 Advisor: Tal Malkin

University of California, Los Angeles *Sep 2014 – Jun 2018*
Bachelor of Science in Computer Science *Latin honor of Cum Laude*
Bachelor of Science in Applied Mathematics

PUBLICATIONS

1. Zeyu Liu, Eran Tromer, **Yunhao Wang**, "Group Oblivious Message Retrieval." (2022). (eprint version will be available in Dec; in preparation for submission to CRYPTO 2023, GitHub link)
2. **Yunhao Wang**, Tianyuan Zheng, and Lior Horesh. "From String Detection to Orthogonal Vector Problem." *QIP* (2023).
3. Shuo Liu*, **Yunhao Wang***, Xu Chen, Yongjie Fu, Sharon Di. "An Integrated SUMO-Gym Framework for Multi-Agent-Reinforcement Learning in Electric Fleet Management Problem." *IEEE ITSC.* (2022).

RESEARCH EXPERIENCE

Research Assistant, Advisor: Tal Malkin *Oct 2022 - Present*
The Cryptography Lab, Columbia University

- Working on the secure model of Lenzen's routing algorithm which might serve as a building block to the unbalanced communication of MPC; investigating a novel non-trivial routing algorithm that hide the source and destination information of each message, such that each server only knows the information of its own messages as well as the assumption that eventually each server should receive the same amount of messages.
- Investigating on the secure schemes to solve graph problems such as perfect matching based on topography-hiding computation under incomplete communication network

Research Assistant, Advisor: Eran Tromer *Jun 2022 - Present*
The Cryptography Lab, Columbia University

- Contributed to the generalization of the definition of Oblivious Message Retrieval (OMR) into Group OMR (GOMR), which captures two scenarios, one with group formed by sender on-flight (Ad-hoc GOMR), and one with group pre-formed by recipients offline (Fixed GOMR), both aims to allow recipients to retrieve messages securely against Denial-of-Service attacks and key-likability attacks.
- Designed a homomorphic-encryption-friendly approach to transform a linear dependent matrix to a linear independent matrix which facilitate the completeness and privacy requirement against attacks from malicious sender/recipients of the GOMR scheme.
- Constructed and implemented both the Ad-hoc GOMR and Fixed GOMR algorithms based on different lattice-based schemes, including PVW and BFV leveled-homomorphic encryption, and optimized the performance by reducing the multiplicative depth. Implementation is public on GitHub.
- Contributed to the formalization of a conjecture (Snake-Eye Conjecture) related to Regev05, and investigating its relation to Knowledge of Knapsack of Noisy Inner Product Assumption.

Research Assistant, Advisor: Lior Horesh *Feb 2022 - Sep 2022*

Columbia University, IBM Research

- Revisited the Grover's Search Algorithm (GSA) under the setting of unstructured search problems with non-uniform initial distributions and formally defined the orthogonal vector problem under quantum settings (QOVP). Paper accepted for poster presentation in Quantum Information Processing 2023.
- Implemented the circuits with the standard as well as state-of-the-art variations of GSA for QOVP and performed a case analysis on the performance via Qiskit.
- Proposed a theorem that generalizes the condition under which GSA (and its variations) cannot be applied (i.e., no stable measurement can be achieved), and formally derived the final distribution of marked state under certain initial condition.
- Implemented a constant-depth quantum circuit for QOVP redefined based on one's complement.

Research Assistant, Advisor: Sharon Di *Sep 2021 - Apr 2022*

Data Science Institute, Columbia University

- Designed and implemented a Hierarchical Reinforcement Learning scheme with two layers of decision making to solve the Electric Fleet Management Problem, paper accepted by IEEE ITSC.
- Integrated with SUMO simulator to embed noise vehicles in model training and to visualize the asynchronous action made by the model.

Research Assistant *Mar 2018 - Jun 2018*

Automated Reasoning Group, University of California, Los Angeles

- Analyzed algorithms that calculated the treewidth of graphs and integrated the algorithms from 1st Parameterized Algorithms and Computational Experiments Challenge in the system that converts CNF into d-DNNF for benchmark.

TEACHING EXPERIENCE

Department of Computer science, Columbia University *Sep 2022 - Dec 2022*

Teaching Assistant *Course: Advanced Software Engineering*

Department of Computer science, Columbia University *Sep 2021 - Dec 2021*

Teaching Assistant *Course: Clean object-oriented design*

WORKING EXPERIENCE

Amazon/AWS, Seattle, WA *Aug 2018 - Aug 2021*

Software Development Engineer II

- Designed and implemented a workflow to perform feasibility check based on product demand and inventory configurations inside of a supply chain optimization solver
- Designed a post-processing system to take an optimization output of a linear programming problem and convert it into financial matrices that are understandable to general users and can be easily integrated to other systems
- Designed and implemented a data lake based on Athena and S3 to store customer data and data center configurations and provided API to re-drive, query and backfill authorized data sources
- Designed and implemented a routing system based on AWS IAM Roles, Kinesis Firehose and Simple Notification Services to perform authentication check on users, parse valid data strings into uniform structures, and route data to interested downstream systems.