WANG, YUJIE (JAYE)

Skype: 2503734534@qq.com ▪ +8615063082657 ▪ ywanggm@ust.hk

EDUCATION

THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY (HKUST) **HONG KONG**
Bachelor of Science in Applied Mathematics, Bachelor of Science in Data Science *2017-2021*
GPA*: 4.097/4.3(top 1%)* | *Dean's List* *(four consecutive semesters)*
Coursework: The Principle of Cybersecurity, Compiler Development, Full Stack Web development, Computer Network, Machine Learning, Regression Analysis, Probability and Statistical, Game Theory

WASHINGTON UNIVERSITY IN ST. LOUIS (WUSTL) **ST. LOUIS, USA**
International Student Research Internship Program *Summer 2020*

THE UNIVERSITY OF SOUTHERN CALIFORNIA(USC) **LOS ANGELES, USA**
International Student Exchange Program *Spring 2020*

RESEARCH EXPERIENCE

"PRIVACY-PRESERVING SOFTWARE SECURITY ANALYSIS"
Final Year Thesis *Aug 2020 – Present*

- Deploy program encoding methods such as Cod2vec and Asm2vec
- Design program embedding encryption scheme with Homomorphic Encryption
- Analyze the semantic properties of the encrypted program with deep learning
- Supervised by Prof. WANG Shuai, Department of Computer Science & Engineering, HKUST

"LARGE-SCALE EVALUATION OF THE SECURITY OF COMPUTER-AIDED DIAGNOSIS ALGORITHMS"
International Student Research Internship Program at Washington University in St. Louis *May 2020 – Present*

- Implement multiple attacks targeting existing CADs with proposed real-world scenarios, where the attackers can cause misdiagnosis} or patient information leakage
- Experiment the efficiency of multiple defenses and give out advise to help secure the CADs
- Supervised by Prof. ZHANG Ning, Department of Computer Science & Engineering, WUSTL

As a core researcher in this summer research project, I am targeting a top tier cybersecurity paper. This project is aimed at demonstrating real-world threats towards existing medical AI systems, and give out advise to help secure the CADs.

"EFFICIENT MPC PROTOCOL FOR PRIVACY-PRESERVING MACHINE LEARNING"
The University of Southern California *Jan 2020 – May 2020*

- Designed a more efficient MPC protocol for neural network training
- Implemented the protocol and compared its efficiency with the standard SGD training and previous MPC protocol
- Supervised by Prof. Muhammad Naveed, Department of Computer Science, USC

"IMPROVEMENT OF AN APPROXIMATED SELF-IMPROVING SORTER AND ERROR ANALYSIS OF ITS ESTIMATED ENTROPY"
Undergraduate Research Opportunity Program, HKUST *Sep 2019 – Dec 2019*

- Designed a generalized algorithm to extend existing self-improving sorters
- Implemented the sorter and compared the experiment result with theoretical values
- Completed a draft as the first author: *https://arxiv.org/abs/2001.05451*
- Supervised by Prof. CHENG Siu-wing, Department of Computer Science & Engineering, HKUST

WORK EXPERIENCE

UNIVERSITY OF BRISTOL **UK**
Summer Research Internship – Biological Statistic *Jun 2019 – Sep 2019*

- Initiated research project: "Identifiability of IBS and PBWT for Demographic Reasoning"
- Proposed a statistical approach to extract informative signals from large genetics data for demographic reasoning
- Conducted research to study the informatics difference between IBS and PBWT
- Reconstructed the population structure from population genetics data using nonparametric regression method
- Supervised by Prof. Feng YU and Prof. Daniel Lawson, Department of Mathematics, University of Bristol

AWARDS & HONORS

▪ *Scholarships*: University’s Scholarship for Continuing UG Students, HKUST Admission Scholarship, Overseas Exchange Scholarship, Hong Kong & Qingdao Association Scholarship

▪ *Awards*: The Epsilon Fund Award in 2019, HKUST Outstanding Academic Performance Award

SKILLS & INTERESTS

▪ *Technical*: Solidity, Javascipt, SQL, Php, CSS, C++, Java, Pytorch, Tensorflow, Python, OpenCV, Matlab, Keras

§ *Languages*: English(Fluent) and Mandarin(Native)

▪ *Interests*: Cybersecurity(especially Multiparty Computation and Adversarial ML), Statistical Machine Learning

▪ *Self-study*: Computer System: A Programmer’s Perspective, Information Security: Principles and Practice, Pattern Recognition and Machine Learning (PRML)