Pui Yung Anna WOO

+852 52138716 | pywoo@link.cuhk.edu.hk

RESEARCH INTERESTS

Applied Cryptography, Computer Security, Distributed Systems, Theoretical Computer Science

EDUCATION

The Chinese University of Hong Kong (CUHK), Hong Kong *Sep. 2017 – Present*
B.S. in Mathematics and Information Engineering (ELITE Stream Student)
∘ A demanding and boutique double-major program that admits ∼15 students each year
∘ Graduate school destinations of our alumni: `https://www.ie.cuhk.edu.hk/mie/mieg_further_study.shtml`
∘ ELITE Stream: Offer to students with top ∼10% academic performance in the Faculty of Engineering
Minor: Computer Science
Major GPA 3.917/4.000 | Cumulative GPA 3.828/4.000

PUBLICATIONS

Goten: GPU-Outsourcing Trusted Execution of Neural Network Training.
Lucien K. L. Ng, Sherman S. M. Chow, **Anna P. Y. Woo**, Donald P. H. Wong, Yongjun Zhao.
In AAAI Conference on Artificial Intelligence (**AAAI**), 2021. (Acceptance rate: 21.3%)

LDSP: Shopping with Cryptocurrency Privately and Quickly under Consortium Leadership.
Lucien K. L. Ng, Sherman S. M. Chow, Donald P. H. Wong, **Anna P. Y. Woo**.
In IEEE International Conference on Distributed Computing Systems (**ICDCS**), 2021. (Acceptance rate: 19.8%)

RESEARCH EXPERIENCES

Note: All of the following projects are supervised by Prof. Sherman S. M. Chow

Goten: GPU-Outsourcing Trusted Execution of Neural Network Training *Jun. 2019 – Dec. 2020*

- A privacy-preserving training framework leveraging GPU and a trusted processor – Intel SGX
- Proposed efficient SIMD input-oblivious primitives to defend against side channel attacks targeted at Intel SGX
- Demonstrated my implementations to be data-oblivious using Intel PinTools, instrumentation tools for program analysis
- Implemented training and inference on datasets CIFAR-10 and a public medical dataset

GForce: GPU-Friendly Oblivious and Rapid Neural Network Inference *Dec. 2019 – Sep. 2020*

- An oblivious inference protocol that works over a low-precision integer domain while maintaining high accuracy
- Solved some issues in integrating SWALP, a low-precision training scheme, with oblivious neural network inference
- Improved the accuracy, e.g. from a recall of 78% to 93% in the CIFAR-10 dataset over VGG-16 architecture
- Implemented training and inference over A-MT and VGG neural network architectures on CIFAR-10/100 datasets
- To be acknowledged in a paper in USENIX Security: `https://github.com/Lucieno/gforce-public#acknowledgement`

LDSP: Shopping with Cryptocurrency under Consortium Leadership *Jul. 2020 – May. 2021*

- A layer-2 cryptocurrency payment system supporting a dynamic and distributed setup with scalability and payer privacy
- Implemented a withdrawal protocol that allows customers to invest an on-chain coin for an off-chain coin
- Built an off-chain payment system between customers, merchants and leaders and designed methods to optimize it
- Reduced the payment latency by >50% via proposing a trick that pre-computes the elliptic curve pairing

Ongoing Personal Research Projects *Feb. 2021 – Present*

- Password-Controlled Outsourced Two-Party Computation
  ∘ A system that securely stores the user data and allows the server to compute over the encrypted user data
  ∘ With privacy guarantees for user data and passwords and features, e.g. minimal user involvement, key rotation, etc.
- Secure Storage System with Biometric Password Authentication
  ∘ A secure storage system that only allows the server to retrieve the user data after biometric password authentication
  ∘ Adopt additive homomorphic encryption scheme for efficiency and upgrade the scheme to support one multiplication

SELECTED AWARDS AND HONORS

Best Project Award, UG Summer Research Internship, Faculty of Engineering of CUHK *2018–19*

- The internship programme accepted outstanding engineering students to do research with a professor in summer
- My project is to realize privacy-preserving deep neural network training using Intel SGX
- Awards were given to the top 10% projects assessed by a committee

Professor Charles K. Kao Research Exchange Scholarship, Faculty of Engineering of CUHK *2019–20*

- Selection was conducted by the Faculty based on the candidates' academic performance and research potentials
- Maximum 7 awards in the Faculty of Engineering of CUHK in 2019–20
- Award up to HK$50,000 to cover the travel expenses and living allowance for joining the research exchange programmes

OTHER AWARDS AND HONORS

Faculty of Engineering Admission Scholarships	*2017–18*
ELITE Stream Student Scholarship	*2017–18, 2018–19*
GOAL Programme Non-local Service Learning Scholarship	*2018–19*
Shum Choi Sang Scholarship	*2018–19*
Swire Scholarship (1 award in the Faculty of Engineering of CUHK each year; Covered the tuition for 1 year)	*2018–19*
Ko Ho Ning Scholarship	*2019–20*
Cheung Chuk Shan Scholarship (Covered the tuition for 1 year)	*2020–21*
UNIQLO Hong Kong Scholarship	*2020–21*
College Head's List	*2020–21, 2021–22*

CANCELLED PROGRAMMES DUE TO COVID-19

Exchange Programme at Nanyang Technological University, Singapore

- Selected to attend the exchange programme in Fall 2020–2021

Overseas Research Exchange Program

- Selected to do research with a designated professor overseas in Summer 2020
- Supported by Professor Charles K. Kao Research Exchange Scholarship

PROGRAMMING SKILLS

Programming languages:

- Python, C, C++, C#, Java, Solidity, MATLAB, Bash

Tools/Frameworks/Libraries:

- Git, gRPC, Intel SGX, CUDA, Androguard, ApkTool, PinTools, Docker, Hadoop, PyTorch, NumPy, Eigen