JIA-CHNG (JASON) LOH

PhD Candidate @ University of Wollongong, Australia

@ jasonlohjc@gmail.com   Australia   in linkedin.com/in/j7sz

WORKING EXPERIENCES

Casual Teaching Staff

University of Wollongong

Feb 2023 – Current   Australia

- Tutorial/Lab Demostration:
  - Ethical Hacking
  - Security Essentials

Research Assistant

National University of Singapore

July 2019 – 2021   Singapore

- Research Works & Implementations:
  - Secure Multiparty Computation
  - Privacy-preserving Biometric Authentication/Identification

Researcher (Internship)

National University of Singapore

January 2019 – June 2019   Singapore

- Research Works & Implementations:
  - Searchable Encryption
  - Deep Packet Inspection over Encrypted Traffic with Middleware

Graduate Research Assistant

Multimedia University

August 2016 – April 2018   Malaysia

- Teaching assistant in Cybersecurity
- Research Works in Cryptography

REFEREES

Distinguished Prof. Dr. Willy SUSILO

@ Director of Institute of Cybersecurity and Cryptology (iC2), SCIT, University of Wollongong

✉ wsusilo@uow.edu.au

Dr. Geong Sen POH

@ Assistant Director at Cyber Security AI R & D, S-Lab for Advanced Intelligence

✉ geongsen@gmail.com

Prof. Dr. Swee Huay HENG

@ Professor at Faculty of Information Science & Technology, Multimedia University

✉ shheng@mmu.edu.my

EDUCATIONS

Doctor of Philosophy

University of Wollongong

2021 – Current

- Provably, Tightly Secure Signatures
- Algebraic Group Model

M.Sc. (by Research) in Information Technology

Multimedia University

2016 – 2019

- Generic Framework for Accountable Optimistic Fair Exchange
- Cryptanalysis on Undeniable Signature Schemes

B.IT. (Hons.) in Security Technology

Multimedia University

2013 – 2016

CGPA: 3.52

Certified Ethical Hacker v9

EC-Council

2017

ID: ECC68868351978

ACHIEVEMENTS

🏆 **Best Paper Award**
ESORICS 2020.

🏆 **1st Prize at HackWEEKDAY 2014**
Hackathon competition to brainstorm for new ideas with prototypes.

🏆 **Champion at F-Secure IT Security Competition Malaysia 2015**
Capture the flag (CTF) competition. Identifying and solving secrets that are hidden in purposefully-vulnerable programs or websites.

🏆 **2nd Runner-up at KPMG Cyber Security Challenge 2016**
CTF competition.

PUBLICATIONS

Conference Proceedings

- **Loh, Jia-Chng**, Fuchun Guo, Willy Susilo, and Guomin Yang (2023). "A Tightly Secure ID-Based Signature Scheme Under DL Assumption in AGM". in: *ACISP 2023*. Springer, pp. 199–219.
- **Loh, Jia-Ch'ng**, Swee-Huay Heng, Syh-Yuan Tan, and Kaoru Kurosawa (2020a). "A Note on the Invisibility and Anonymity of Undeniable Signature Schemes". In: *WISA 2019*. Springer-Verlag, pp. 112–125.
- Ning, Jianting, Xinyi Huang, Geong Sen Poh, Shengmin Xu, **Loh, Jia-Chng**, Jian Weng, and Robert H Deng (2020). "Pine: Enabling Privacy-Preserving Deep Packet Inspection on TLS with Rule-Hiding and Fast Connection Establishment". In: *ESORICS 2020*. Springer, pp. 3–22.
- Ning, Jianting, Geong Sen Poh, **Loh, Jia-Ch'ng**, Jason Chia, and Ee-Chien Chang (2019). "PrivDPI: Privacy-Preserving Encrypted Traffic Inspection with Reusable Obfuscated Rules". In: *ACM CCS 2019*, pp. 1657–1670.
- **Loh, Jia-Ch'ng**, Swee-Huay Heng, and Syh-Yuan Tan (2018a). "A Generic Framework for Accountable Optimistic Fair Exchange Protocol". In: *ISPEC 2018*, pp. 299–309.
- – (2018b). "Revisiting the Invisibility of Yuen et al.'s Undeniable Signature Scheme". In: *Cryptology2018*, pp. 76–84.
- – (2017). "A Survey on Optimistic Fair Exchange Protocol and Its Variants". In: *ICOICT 2017*, pp. 1–6.

Journal Articles

- **Loh, Jia-Ch'ng**, Swee-Huay Heng, Syh-Yuan Tan, and Kaoru Kurosawa (2020b). "On the Invisibility and Anonymity of Undeniable Signature Schemes". In: *JoWUA* 11.1, pp. 18–34.
- **Loh, Jia-Ch'ng**, Swee-Huay Heng, and Syh-Yuan Tan (2019). "A Generic Framework for Accountable Optimistic Fair Exchange Protocol". In: *Symmetry* 11.2. 285.

PROJECTS

Morse Code Signature (MorSign)

Final Year Project with Extension Results

MorSign consists of three bundled applications: (i) Morse Pass, the phone login authentication (lock screen); (ii) Morse Rescue, a SOS function which can be triggered with "one touch", and also embedded with location monitoring and tracking function, and; (iii) Morse Vault, the highly protected and encrypted password management tool.

Project Awards:

- **Gold Award @ MMU Invention Showcase 2016 (Category in Security Authentication)**
- **Gold Medal @ ITEX 2016**
- **Gold Medal @ PECIPTA 2017**
- **Silver Award @ PERINTIS 2018**
- **Bronze Medal @ Malaysia Technology Expo 2018**

(CONT.)

A Generic Framework for Accountable Optimistic Fair Exchange (OFE) Protocol

Fundamental Research Grant Scheme (FRGS)

A fair exchange protocol that allows two parties to exchange in a fair manner; and trusted third party (TTP) is asked to resolve if there is dispute happens. A provably secure generic framework in the standard model is proposed.

Project Award:

- **Silver Award @ RICES 2018**