

ZHOU, JUNDA

The Chinese University of Hong Kong, Hong Kong, China
(+852) 6760 2495 ♦ davidjdzhou@link.cuhk.edu.hk

EDUCATION

The Chinese University of Hong Kong (CUHK)

August 2023 – July 2027 (Expected)

PhD Information Engineering
Hong Kong PhD Fellowship Scheme awardee
Supervisor: Prof. Pascal O. VONTOBEL

ETH Zurich

February 2022 – August 2022

Exchange student

GPA: 5.320/6.0

Department of Computer Science

Courses: Formal Methods and Functional Programming, Information Security, Signals and Systems II, Communication and Detection Theory

The Chinese University of Hong Kong

September 2019 – July 2023

B.Sc. in Mathematics and Information Engineering, First Class Honours Cumulative GPA: 3.804/4.0
Stream: Engineering Leadership, Innovation, Technology and Entrepreneurship (ELITE)
Chung Chi College

AREAS OF INTEREST

Information and coding theory, Quantum information science

RESEARCH EXPERIENCE

Undergraduate Graduation Thesis

September 2022 – May 2023

- Topic: Research on information-theoretic security
- Supervised by Prof. LI Cheuk Ting, Department of Information Engineering
- Studied security and secret-key rates of information-theoretically secure key agreement schemes
- Investigated a one-shot key agreement scheme where the variable-length secret key depends on a random stopping time
- Formulated the definition of the randomly-stopped key agreement scheme and its security, and proposed an approach to bound the optimal secret-key length

Prof. CHAU Sze Yiu's research group

September 2021 – December 2021

- Participated in weekly group meetings and learnt about recent progress on implementations of cryptographic protocols
- Tested PKCS#1 v1.5 RSA signature verification implementations (continuation of summer research internship)

Undergraduate Summer Research Internship

June 2021 – August 2021

Faculty of Engineering, CUHK

- Topic: Research on implementations and deployments of cryptographic protocols
- Supervised by Prof. CHAU Sze Yiu, Department of Information Engineering
- Studied the foundations of Elliptic Curve Cryptography, theoretical attacks and reported vulnerabilities in implementations
- Studied PKCS#1 v1.5 RSA signature protocol, focusing on the construction and verification of the encoded messages

- Tested PKCS#1 v1.5 RSA signature verification implementations with project Wycheproof and identified the vulnerabilities and the corresponding root causes

AWARDS AND SCHOLARSHIPS

Hong Kong PhD Fellowship Scheme 2023–2024	<i>August 2023</i>
CUHK Vice-Chancellor HKPFS Scholarship	<i>August 2023</i>
The Charles Kao Top Performance Award 2022–23	<i>July 2023</i>
Dean’s List 2022–2023	<i>July 2023</i>
Chung Chi College Departmental Prize 2022–2023	<i>April 2023</i>
Chung Chi EYE Award 2021–2022	<i>September 2022</i>
Academic Excellence Scholarship for Non-local Fee-paying Students 2021–2022	<i>May 2022</i>
Class of 1977 Fortieth Graduation Anniversary Scholarship	<i>March 2022</i>
Information Engineering Award for Academic Exchange	<i>December 2021</i>
Chung Chi College Class Scholarship 2021–2022	<i>November 2021</i>
ELITE Stream Scholarship 2020–2021	<i>October 2021</i>
Yasumoto International Exchange Scholarship	<i>August 2021</i>
Dean’s List 2020–2021	<i>July 2021</i>
Dean’s List 2019–2020	<i>July 2020</i>
Mathematics Scholarship	<i>January 2020</i>

TECHNICAL STRENGTHS

Programming Languages	C, C#, Python, Haskell
Software & Tools	Git, MATLAB

TEACHING

Teaching Assistant

- Discrete Mathematics for Engineers (2023 Fall), Discrete Structures and Probability (2024 Spring)

LANGUAGES

Mandarin	Native
English	Fluent (IELTS: 8.0)

EXTRACURRICULAR ACTIVITIES

Volunteer for organizing Ultimate Frisbee activities at CUHK and with other teams	<i>2022</i>
Trained for Chinese Physics Olympiad	<i>2016 – 2017</i>