

# Xu Yanhong

Email: [yanhong.xu1@ucalgary.ca](mailto:yanhong.xu1@ucalgary.ca)

## EDUCATION

---

### Ph.D. in Mathematics

Aug 2014–Jan 2019

*Nanyang Technological University, Singapore*

CGPA: 4.9/5.0

- *Supervisors:* Professor Wang Huaxiong, Professor Ling San, Dr Khoa Nguyen

### B.S. in Mathematics

Sep 2010–Jun 2014

*Xiamen University, China*

CGPA: 3.71/4.0

- *Thesis Advisor:* Professor Ni Du

## PROFESSIONAL EXPERIENCE

---

### Postdoc Associate in Computer Science

Feb 2019–Feb 2021

*University of Calgary, Canada*

- *Supervisor:* Professor Rei Safavi-Naini

## CONFERENCE PUBLICATIONS

---

- Forward-Secure Group Signatures from Lattices. San Ling, Khoa Nguyen, Huaxiong Wang, and **Yanhong Xu**. In PQCrypto 2019. LNCS, vol. 11505, pp. 44-64. Springer, 2019.
- Accountable Tracing Signatures from Lattices. San Ling, Khoa Nguyen, Huaxiong Wang, and **Yanhong Xu**. In CT-RSA 2019. LNCS, vol. 11405, pp. 556-576. Springer, 2019.
- Constant-size group signatures from lattices. San Ling, Khoa Nguyen, Huaxiong Wang, and **Yanhong Xu**. In PKC 2018, volume 10770 of LNCS, pages 58–88. Springer, 2018.
- Lattice-Based Group Signatures: Achieving Full Dynamicity with Ease. San Ling, Khoa Nguyen, Huaxiong Wang, and **Yanhong Xu**. In ACNS 2017, volume 10355 of LNCS, pages 293–312. Springer, 2017.

## JOURNAL PUBLICATIONS

---

- Lattice-Based Group Signatures: Achieving Full Dynamicity (and Deniability) with Ease. San Ling, Khoa Nguyen, Huaxiong Wang, and **Yanhong Xu**. In Theoretical Computer Science, vol. 783 (2019), pp. 71-94.

## MANUSCRIPTS

---

- Traceable Policy-Based Signatures and Instantiation from Lattices. **Yanhong Xu**, Rei Safavi-Naini, Khoa Nguyen, and Huaxiong Wang. In arXiv preprint arXiv:2007.00033.
- Compressing the Transaction Data of Blockchain. Ivan Lau, Shang Li, Evan MacNeil, Alexandra McSween, Abhishek Kumar Shukla, and **Yanhong Xu**. The final report of the Math to Power Industry Workshop Aug 2020.

## TALKS

---

7. “Accountable Tracing Signatures From Lattices”. At CT-RSA 2019, San Francisco, US, 8 Mar 2019.
6. “Group Signatures with Advanced Features From Lattices”. Thesis defense at NTU, Singapore, 11 Dec 2018.
5. “Stern-Like Zero-Knowledge Protocol”. At Shaanxi Normal University, Xi’an, China, 29 Sep, 2018.
4. “Introduction of Group Signatures”. At IFHS, XiDian University, Xi’an, China, 28 Sep 2018.
3. “Stern-Like Zero-Knowledge Protocol”. At IFHS, XiDian University, Xi’an, China, 26 Sep, 2018.
2. “Constant-size group signatures from lattices”. At PKC 2018, Rio de Janeiro, Brazil, 28 Mar 2018.
1. “Lattice-Based Group Signatures: Achieving Full Dynamicity with Ease”. At ACNS 2017, Kanazawa, Japan, 11 July 2017.

## PROFESSIONAL ACTIVITIES

---

- **Program Committees:** ProvSec 2020
- **External Conference reviews:** Asiacrypt, PKC, ESORICS, ACNS, CT-RSA, FC, AsiaCCS, ACISP, ISC, ACM-CCSW
- **Journal reviews:** Theoretic Computer Science, Finite Fields and Their Applications, Advances in Mathematics of Communication, IJACT, IET Information Security

## HONORS & AWARDS

---

- Nanyang Research Scholarship by Nanyang Technological University, Aug 2014–Aug 2018.
- First Grade National Scholarship by Ministry of Education, China, in AY 2011–2012.
- First Grade National Scholarship of Encouragement by Ministry of Education, China, in AY 2010–2011 and AY 2012–2013.
- Travel grants sponsored by Division of Mathematical Sciences, SPMS, Nanyang Technological University, July 2017, Mar 2018.

## PROFESSIONAL LEARNING AND DEVELOPMENT

---

### Postdoctoral Certificate in University Teaching and Learning

*University of Calgary, Canada*

- *SoTL Foundations:* badge awarded on 17 Jun 2020
- *Emerging Teachers Development:* badge awarded on 30 Jan 2020
- *Developing Your Teaching Dossier:* badge awarded on 30 Jan 2020
- *Theories and Practices:* badge awarded on 30 Jan 2020

### Quality Graduate Supervision MOOC

*University of Calgary, Canada*

- Badge awarded on 07 Apr 2020

## TEACHING EXPERIENCE

---

### Teaching Assistant

*Nanyang Technological University*

- Discrete Mathematics – MH1812 (2016 Spring, 2016 Fall, 2017 Spring, 2017 Fall, 2018 Spring).
- Mathematics II – MH1811 (2016 Spring)

### Part-Time Teacher

Dec 2013–Jun 2014

*Pashu Gaoshou Tuition Center, Xiamen, China*

- Grade 6 and Grade 8 Mathematics