

## XIAOLU HOU

*Postal Address:*  
CSL, SCSE, NTU  
Singapore – 639798.

*Email:* houxiaolu.email@gmail.com  
*Nationality:* China  
*Residency Status:* Singapore PR

### EDUCATION

---

**Ph. D. in Mathematical Sciences** Jan 2013 – May 2017  
Nanyang Technological University(NTU), Singapore CGPA: 5.00/5.00  
*Thesis title:* Algebraic Constructions of Modular Lattices  
*Advisor:* Assoc Prof. Frédérique Oggier

**B. S. in Mathematical Sciences, Specialization in Pure mathematics** August 2009 – Jan 2012  
NTU, Singapore First-Class Honor with CGPA 4.96/5.00

### EXPERIENCE IN RESEARCH

---

**Research Fellow at NTU** Aug 2017 – present  
*Supervisor:* Assoc. Prof. Liu Yang  
*Research Topics:*

- Hardware security.
- Cryptography.
- Fault injection attacks.

**Researcher at Singapore University of Technology and Design (SUTD)** Feb 2017 – Aug 2017  
Research Fellow (May 2017 – Aug 2017)  
Research Assistant (Feb 2017 – May 2017)  
*Supervisor:* Assist. Prof. Martín Ochoa  
*Research Topics:*

- Location privacy

**Graduate Student at NTU** Jan 2013 – May 2017  
*Supervisor:* Assoc. Prof. Frédérique Oggier  
*Research Topics:*

- Construction of modular lattices from number fields.
- Construction of modular lattices from quaternion algebras.
- Construction of modular lattices from linear codes by construction A.

*Collaborations:*

- Software countermeasures in crypto-system against fault injection.
- Publication in CT-RSA 2017 (C1).

**Project Officer at NTU** Feb 2012 – Jan 2013  
*Supervisor:* Assoc. Prof. Frédérique Oggier  
*Research Topics:*

- Construction of modular lattices from number fields and application.

### PUBLICATIONS

---

#### In Review Process:

1. “Automated Fault Analysis of Assembly Code With a Case Study on PRESENT Implementation,” Jakub Breier and Xiaolu Hou, Cryptology ePrint Archive Report 2017/829.
2. “Quantifying Attacker Effort in Location Proximity Attacks against Moving Targets”, Xiaolu Hou, Ruben Rios, Per Hallgren and Martín Ochoa.
3. “Construction of Arakelov-modular Lattices from Number Fields,” Xiaolu Hou, arXiv:1609.03134.

#### Journal:

- J1. “Modular Lattices from a Variation of Construction A over Number Fields,” Xiaolu Hou and Frédérique Oggier, to appear in Advances in Mathematics of Communications, arXiv:1604.01583.
- J2. “Construction of Arakelov-modular Lattices over Totally Definite Quaternion Algebras,” Xiaolu Hou, to appear in International Journal of Number Theory, arXiv:1604.02875.
- J3. “Hilbert spaces of entire Dirichlet series and composition operators,” Xiaolu Hou, Le Hai Khoi and Bingyang Hu, J. Mathematical Analysis Applications, vol. 401, no. 1, pp. 416–429, 2013.
- J4. “Composition operators on Hilbert spaces of entire Dirichlet series,” Xiaolu Hou, Le Hai Khoi and Bingyang Hu, C. R. Acad. Sci. Paris, Ser. I 350, no. 19–20, pp. 875–878, 2012.
- J5. “Some properties of composition operators on entire Dirichlet series with real frequencies,” Xiaolu Hou and Le Hai Khoi, C. R. Acad. Sci. Paris, Ser. I 350, no. 3–4, pp. 149–152, 2012.

### Conference Proceedings:

- C1. “Feeding two cats with one bowl: On designing a fault and side-channel resistant software encoding scheme,” Jakub Breier, and Xiaolu Hou, RSA Conference Cryptographers’ Track (CT-RSA) 2017, San Francisco, US, Cryptology ePrint Archive Report 2016/931.
- C2. “On LCD Codes and Lattices,” Xiaolu Hou, and Frédérique Oggier, IEEE International Symposium on Information Theory (ISIT) 2016, Barcelona, Spain.
- C3. “Construction and Secrecy Gain of a Family of 5-modular Lattices,” Xiaolu Hou, Fuchun Lin and Frédérique Oggier, IEEE Information Theory Workshop 2014, Hobart, Tasmania, Australia.

### HONORS

- Awarded Nanyang President’s Graduate Scholarship, a competitive and prestigious scholarship scheme for outstanding graduates – Jan 2013 to Jan 2017.
- Awarded Lee Kuan Yew Gold Medal, the most prestigious award in NTU, which is given to the top student in each degree programme of the graduating cohort who has excelled in general proficiency and has obtained a First Class Honors – Jun 2012.
- Awarded Dean’s list, which is for the top 5% of the cohort every academic year – 2009-2010, 2010-2011, 2011-2012.
- NTU President Research Scholar and participated in URECA, which is by invitation only to the most academically able second and third year undergraduate – 2010-2011.
- Awarded SM2 Scholarship for undergraduate studies at NTU through a selection with exams and interview – 2009-2012.

### SKILLS

<u>Language</u>	<u>Programming Languages</u>	<u>Tools</u>
• English ( <i>Fluent</i> )	• Python ( <i>Basic</i> )	• Magma ( <i>Intermediate</i> )
• Mandarin ( <i>Native</i> )	• C ( <i>Basic</i> )	• Sage ( <i>Intermediate</i> )
	• Java ( <i>Basic</i> )	• L <sup>A</sup> T <sub>E</sub> X ( <i>Intermediate</i> )
	• AVR Assembly ( <i>Basic</i> )	

### OTHER SCIENTIFIC AND SOCIETAL IMPACT

- Lecturer for training camp for undergraduate students joining International Mathematics Competition – Jun 2016
- Lecturer for seeNTU, a premium enrichment programme designed for pre-tertiary students to attend lectures, seminars and laboratory sessions under the tutelage of NTU staff – June 2015
- Participated SPCoding School, a summer school held by Unicamp – Jan 2015
- Lecturer for seeNTU – June 2014
- Judge for Singapore International Mathematics Challenge 2014 – May 2014
- Co-organizer for reading group in algebraic number theory – Aug 2013 to June 2014
- Lecturer for seeNTU – June 2013
- Lecturer for Malaysian Chinese Independent Secondary School Teachers Mathematics Workshop – Aug 2012
- Lecturer for training camp for undergraduate students joining International Mathematics Competition – May 2012
- Judge for Singapore International Mathematics Challenge 2012– May 2012
- Lecturer for Math Magic Hour, an undergraduate mathematics seminar for students – March 2012

---

**TEACHING EXPERIENCE**


---

**Nanyang Technological University, Singapore:**

- Teaching Assistant for Discrete Mathematics, an introductory course of discrete mathematics for first year mathematics students, two tutorials per week, involved in grading quizzes and assignments – Jan 2016 - May 2016 and Jan 2015 - May 2015
- Teaching Assistant for Group and Symmetries, an introductory course of abstract algebra for second year mathematics students, two tutorials per week, involved in grading quizzes and assignments – Aug 2015 - Dec 2015
- Teaching Assistant for Discrete Mathematics for Engineering School, an introductory course of discrete mathematics for first year computer science and computer engineering students, two tutorials and one mini lecture per week, involved in grading quizzes – Aug 2014 - Dec 2014
- Teaching Assistant for Engineering Math, an introductory course of linear algebra and calculus for first year engineering students, three tutorials per week, involved in grading assignments and quizzes – Aug 2012 - Dec 2012

---

**POSTER PRESENTATION**


---

- “Automated Analysis of Assembly Code,” Cryptographic Hardware and Embedded Systems (CHES), Taipei, Sep 2017.
- “Algebraic Constructions of Modular Lattices,” Noncommutative rings and their applications, IV, Lens, France, June 2015.
- “Algebraic Constructions of Modular Lattices,” SPCoding School, Unicamp, Brazil, Jan 2015.
- “Algebraic Constructions of Modular Lattices,” The Fifth Singapore Mathematics Symposium, Singapore, Sep 2014.

---

**TALKS**


---

- “Construction of Modular Lattices from Linear Codes and Number Fields”, invited talk, Computational & Statistical Sciences (MCSS) Seminar, Yale-NUS, Singapore, 26th Sep, 2016.
- “On LCD Codes and Lattices,” IEEE International Symposium on Information Theory (ISIT) 2016, Barcelona, Spain, July 2016.
- “Construction and Secrecy Gain of a Family of 5-modular Lattices,” IEEE Information Theory Workshop 2014, Hobart, Tasmania, Australia, Nov 2014.

---

**UNDERGRADUATE PROJECTS**


---

**Supervised Independent Study at NTU**

Aug 2011 – Nov 2011

*Supervisor:* Assoc Prof. Frédérique Oggier*Research Topics:*

- Algebraic Number Theory
  - Studied “Algebraic Theory and Fermat’s Last Theorem by Ian Stewart and David Tall.

**Final Year Project and its Continuation at NTU**

Oct 2011 – Jan 2013

*Supervisor:* Dr. Le Hai Khoi*Research Topics:*

- Composition operators on entire Dirichlet series with real frequencies.
- Composition operators on Hilbert spaces of entire Dirichlet series.
  - Publications J3, J4, J5.

**Undergraduate Research Experience in Mathematical Sciences at NTU**

May 2011 – Aug 2011

*Supervisor:* Prof. Peng Gao*Research Topics:*

- L-functions and their properties.

- Studied "Multiplicative Number Theory I. Classical Theory" by Hugh L. Montgomery, R. Vaughan.

**Undergraduate Research Experience on Campus(URECA) at NTU**

Oct 2010 – Jun 2011

*Supervisor:* Dr. Le Hai Khoi*Research Topics:*

- Bohr's Theorem for Classical Dirichlet Series and its generalizations.
  - Studied the abscissas of Classical Dirichlet Series and investigated the proof for Bohr's Theorem.