Xiaolu Hou

Postal Address:
#30-01/02 Suntec Tower 3,
8 Temasek Boulevard,
Singapore – 038988.

Email: houxiaolu.email@gmail.com
Phone: +6598376372
Nationality: China
Residency Status: Singapore PR
Web: http://xiaoluhou.github.io/

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

Secure Computing Researcher at Acronis Nov 2018 – present

Job Responsibilities:

- Research and development focusing on secure multiparty computation.
- Developing new methods and implementing software frameworks in security domains.
- Converting theoretical concepts from cryptography into practical solutions for industry.

Research Fellow at NTU Aug 2017 – Nov 2018

Supervisor: Assoc. Prof. Yang Liu
Research Topics:

- Security of deep neural networks – analyzing vulnerabilities of activation functions in neural networks w.r.t. fault attacks.
- Fault injection and side-channel attacks on cryptographic implementations and countermeasures.
- Evaluation of security controls – quantifying the robustness and implementation quality of information security controls in an organization w.r.t. ISO 27002 standard.

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 – estimating the effort of an attacker for locating a victim utilizing applications on a mobile device.

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.

Project Officer at NTU Feb 2012 – Jan 2013

Supervisor: Assoc. Prof. Frédérique Oggier
Research Topics:

- Construction of modular lattices from number fields and application.

SKILLS

Language

- English (*Fluent*)
- Mandarin (*Native*)

Programming Languages

- Python (*Advanced*)
- C++ (*Intermediate*)
- Java (*Advanced*)
- AVR Assembly (*Intermediate*)

Tools

- LaTeX(*Expert*)
- Sage (*Advanced*)
- Magma (*Advanced*)

PUBLICATIONS

Book:

1. "Automated Methods in Cryptographic Fault Analysis", Jakub Breier, Xiaolu Hou and Shivam Bhasin (Eds.), ISBN: 978-3-030-11332-2, 334 pages, Springer, 2019.

Manuscripts under review:

1. "On Side-Channel Vulnerabilities of Bit Permutations: Key Recovery and Reverse Engineering," Jakub Breier, Dirmanto Jap, Xiaolu Hou and Shivam Bhasin, IACR Cryptology ePrint Archive 2018: 219 (2018).
2. "SITM: See-in-the-Middle Attack on SPN-based Ciphers", Shivam Bhasin, Jakub Breier, Xiaolu Hou, Dirmanto Jap, Siang Meng Sim.

Journal:

J1. "Fully Automated Differential Fault Analysis on Software Implementations of Block Ciphers," Xiaolu Hou, Jakub Breier, Fuyuan Zhang and Yang Liu, Transactions on Cryptographic Hardware and Embedded Systems (TCHES), 2019, to appear.

J2. "On Evaluating Fault Resilient Encoding Schemes in Software," Jakub Breier, Xiaolu Hou and Yang Liu, Transactions on Dependable and Secure Computing (TDSC), IEEE, 2019, to appear.

J3. "Fault Attacks Made Easy: Differential Fault Analysis Automation on Assembly Code," Jakub Breier, Xiaolu Hou and Yang Liu, Transactions on Cryptographic Hardware and Embedded Systems (TCHES), vol. 1, issue 2, 2018.

J4. "Modular Lattices from a Variation of Construction A over Number Fields," Xiaolu Hou and Frédérique Oggier, Advances in Mathematics of Communications, vol. 11, issue 4, pp. 719-745, 2017.

J5. "Construction of Arakelov-modular Lattices over Totally Definite Quaternion Algebras," Xiaolu Hou, International Journal of Number Theory, vol. 13, issue 7, 2017.

J6. "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.

J7. "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.

J8. "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. "SoK: On DFA Vulnerabilities of Substitution-Permutation Networks", Mustafa Khairallah, Xiaolu Hou, Zakaria Najm, Jakub Breier, Shivam Bhasin, Thomas Peyrin, ACM SIGSAC Asia Conference on Computer & Communications Security (AsiaCCS) 2019, Auckland, New Zealand, to appear.

C2. "Poster: Practical Fault Attack on Deep Neural Networks," Jakub Breier, Xiaolu Hou, Dirmanto Jap, Lei Ma, Shivam Bhasin and Yang Liu, ACM Conference on Computer and Communications Security (CCS) 2018, Toronto, Canada. (Extended version CoRR abs/1806.05859).

C3. "Location Proximity Attacks against Mobile Targets: Analytical Bounds and Attacker Strategies," Xueou Wang, Xiaolu Hou, Ruben Rios, Per Hallgren, Nils Tippenhauer and Martin Ochoa, European Symposium on Research in Computer Security (ESORICS) 2018, Barcelona, Spain.

C4. "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.

C5. "On LCD Codes and Lattices," Xiaolu Hou, and Frédérique Oggier, IEEE International Symposium on Information Theory (ISIT) 2016, Barcelona, Spain.

C6. "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.

OTHER SCIENTIFIC AND SOCIETAL IMPACT

- External reviewer for conferences (SPACE 2018, CCS 2018, ICICS 2018).
- Member of organization team for International Workshop on Constructive Side-Channel Analysis and Secure Design (Cosade) – April 2018
- 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

TALKS

- "Side-Channel Analysis for Reverse Engineering of Secret Cipher", invited talk, Targetted Training on Advanced Side Channel Evaluation of Hardware Security (ASCEHS), IIT Kharagpur, India, 4th July, 2018.
- "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.

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.

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 J6, J7, J8.

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.