Xiaolu Hou

Postal Address:
Jurigovo nam. 15,
84104 Bratislava,
Slovakia

Contact:
Email: houxiaolu.email@gmail.com
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

Research Scientist at Physical Analysis & Cryptographic Engineering Lab, NTU Jan 2020 – present

- Analyzing side-channel and fault vulnerabilities of cryptographic implementations in software and hardware.
- Exploring usage of onboard analog-to-digital converters for side-channel leakage.
- Developing countermeasures against physical attacks.
- Evaluating neural network security w.r.t. fault attacks.

Research Fellow at National University of Singapore Jul 2019 – Jan 2020

- Hardware security – countermeasures against fault attacks.
- Differential privacy of deep neural networks.

Secure Computing Researcher at Acronis Nov 2018 – Jul 2019

- Research and development focusing on secure multiparty computation – threat analysis and prototype implementation.
- Development of methods and tools for secure synthetic data generation.

Research Fellow at Cyber Security Lab, NTU Aug 2017 – Nov 2018

- 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.

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)

- Hardware security – developing software based countermeasures against fault attacks.
- Location privacy – estimating the effort of an attacker for locating a victim utilizing applications on a mobile device.

SKILLS

Programming Languages

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

Other Skills

- Fault analysis
- Side-channel Analysis
- Cryptology
- Coding Theory
- Machine Learning and AI

Language

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

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.

Journal:

J1. "A Countermeasure Against Statistical Ineffective Fault Analysis," Jakub Breier, Mustafa Khairallah, Xiaolu Hou, Yang Liu, Transactions on Circuits and Systems–II, IEEE, vol. 67, issue 12, 3322–3326, 2020.

J2. "SITM: See-In-The-Middle–Side-Channel Assisted Middle Round Differential Cryptanalysis on SPN Block Ciphers," Shivam Bhasin, Jakub Breier, Xiaolu Hou, Dirmanto Jap, Romain Poussier, Siang Meng Sim, Transactions on Cryptographic Hardware and Embedded Systems (TCHES), vol. 3, issue 1, 95–122, 2020.

J3. "On Side Channel Vulnerabilities of Bit Permutations in Cryptographic Algorithms," Jakub Breier, Dirmanto Jap, Xiaolu Hou and Shivam Bhasin, Transactions on Information Forensics and Security (TIFS), vol. 15, IEEE, 2020.

J4. "On Evaluating Fault Resilient Encoding Schemes in Software," Jakub Breier, Xiaolu Hou and Yang Liu, Transactions on Dependable and Secure Computing (TDSC), IEEE, 2020, to appear.

J5. "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), vol. 2, issue 3, 1–29, 2019.

J6. "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, 96–122, 2018.

J7. "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, 719–745, 2017.

J8. "Construction of Arakelov-modular Lattices over Totally Definite Quaternion Algebras," Xiaolu Hou, International Journal of Number Theory, vol. 13, issue 7, 2017.

J9. "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, 416–429, 2013.

J10. "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, 875–878, 2012.

J11. "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, 149–152, 2012.

Conference Proceedings:

C1. "DNFA: Differential No-Fault Analysis of Bit Permutation Based Ciphers Assisted by Side-Channel", Xiaolu Hou, Jakub Breier and Shivam Bhasin, IEEE Design, Automation and Test in Europe Conference (DATE 2021), France.

C2. "Security Evaluation of Deep Neural Network Resistance Against Laser Fault Injection", Xiaolu Hou, Jakub Breier, Dirmanto Jap, Lei Ma, Shivam Bhasin and Yang Liu, IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA 2020), Singapore.

C3. "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.

C4. "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).

C5. "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.

C6. "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.

C7. "On LCD Codes and Lattices," Xiaolu Hou, and Frédérique Oggier, IEEE International Symposium on Information Theory (ISIT) 2016, Barcelona, Spain.

C8. "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.

SCIENTIFIC AND SOCIETAL IMPACT

- Reviewer for international conferences and journals.
- Program committee member of IACR Cryptographic Hardware and Embedded Systems Conference (CHES) 2021.
- Session chair for IACR Cryptographic Hardware and Embedded Systems Conference (CHES) 2020.
- Program committee member of IEEE International Conference on High Performance Computing and Communications (HPCC) 2020.
- Member of organization team for International Workshop on Constructive Side-Channel Analysis and Secure Design (Cosade) – April 2018
- Judge for Singapore International Mathematics Challenge 2014 – May 2014

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 program 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.

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

- "On Side Channel and Fault Attacks against Machine Learning", invited talk, Virtual Workshop on Machine Learning & Hardware Security, 26th August, 2020.
- "Side-Channel Analysis for Reverse Engineering of Secret Cipher", invited talk, Targeted 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.