Xiaolu Hou

FIIT, STU, Room 403,
Ilkovičova 2,
842 16 Bratislava, Slovakia

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 Aug 2009 – Jan 2012
NTU, Singapore First-Class Honor with CGPA 4.96/5.00

EXPERIENCE

Assistant Professor at Faculty of Informatics and Information Technologies (FIIT), Slovak University of Technology (STU) Mar 2021 – Present

- Research in hardware security and cryptography
- Research in AI security

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

- 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.

PUBLICATIONS

Book:

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

Book Chapter:

1. *On Implementation-Level Security of Edge-Based Machine Learning Models*, Lejla Batina, Shivam Bhasin, Jakub Breier, Xiaolu Hou, Dirmanto Jap, Security and Artificial Intelligence: A Crossdisciplinary Approach, Springer Nature, 2022.

Journal:

J1. *FooBaR: Fault Fooling Backdoor Attack on Neural Network Training*, Jakub Breier, Xiaolu Hou, Martín Ochoa, Jesus Solano, IEEE Transactions on Dependable and Secure Computing (TDSC), to appear.

J2. *SNIFF: reverse engineering of neural networks with fault attacks*, Jakub Breier, Dirmanto Jap, Xiaolu Hou, Shivam Bhasin, Yang Liu, IEEE Transactions on Reliability, to appear.

J3. *Constrained Proximity Attacks on Mobile Targets*, Xueou Wang, Xiaolu Hou, Ruben Rios, Nils Ole Tippenhauer, Martín Ochoa, ACM Transactions on Privacy and Security, no. 2, 2022.

J4. *A Finer-Grain Analysis of the Leakage (Non) Resilience of OCB*, Francesco Berti, Shivam Bhasin, Jakub Breier, Xiaolu Hou, Romain Poussier, François-Xavier Standaert, Balazs Udvarhelyi, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), no. 1, 2022.

J5. *Back To The Basics: Seamless Integration of Side-Channel Pre-processing in Deep Neural Networks*, Yoo-Seung Won, Xiaolu Hou, Dirmanto Jap, Jakub Breier, Shivam Bhasin, IEEE Transactions on Information Forensics and Security (TIFS), 2021.

J6. *Physical Security of Deep Learning on Edge Devices: Comprehensive Evaluation of Fault Injection Attack Vectors*, Xiaolu Hou, Jakub Breier, Dirmanto Jap, Lei Ma, Shivam Bhasin, Yang Liu, Microelectronics Reliability, Elsevier, 2021.

J7. *On Evaluating Fault Resilient Encoding Schemes in Software*, Jakub Breier, Xiaolu Hou and Yang Liu, IEEE Transactions on Dependable and Secure Computing (TDSC), no. 3, 2021.

J8. *A Countermeasure Against Statistical Ineffective Fault Analysis*, Jakub Breier, Mustafa Khairallah, Xiaolu Hou, Yang Liu, IEEE Transactions on Circuits and Systems–II, no. 12, 2020.

J9. *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, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), no. 1, 2020.

J10. *On Side Channel Vulnerabilities of Bit Permutations in Cryptographic Algorithms*, Jakub Breier, Dirmanto Jap, Xiaolu Hou and Shivam Bhasin, IEEE Transactions on Information Forensics and Security (TIFS), 2020.

J11. *Fully Automated Differential Fault Analysis on Software Implementations of Block Ciphers*, Xiaolu Hou, Jakub Breier, Fuyuan Zhang and Yang Liu, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), no. 3, 2019.

J12. *Fault Attacks Made Easy: Differential Fault Analysis Automation on Assembly Code*, Jakub Breier, Xiaolu Hou and Yang Liu, IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES), no. 2, 2018.

J13. *Modular Lattices from a Variation of Construction A over Number Fields*, Xiaolu Hou and Frédérique Oggier, Advances in Mathematics of Communications, no. 4, 2017.

J14. *Construction of Arakelov-modular Lattices over Totally Definite Quaternion Algebras*, Xiaolu Hou, International Journal of Number Theory, no. 7, 2017.

J15. *Hilbert spaces of entire Dirichlet series and composition operators*, Xiaolu Hou, Le Hai Khoi and Bingyang Hu, Journal of Mathematical Analysis and Applications, no. 1, 2013.

J16. *Composition operators on Hilbert spaces of entire Dirichlet series*, Xiaolu Hou, Le Hai Khoi and Bingyang Hu, Comptes Rendus Mathematique, no. 19–20, 2012.

J17. *Some properties of composition operators on entire Dirichlet series with real frequencies*, Xiaolu Hou and Le Hai Khoi, Comptes Rendus Mathematique, no. 3–4, 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 SIGSAC Conference on Computer and Communications Security (CCS) 2018, Toronto, Canada.

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, Cryptographers' Track at the RSA Conference (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.

GRANTS

• *Implementation Security of Neural Networks*, project of the Slovak Research and Development Agency, SK-SRB-21-0059, 2022 - 2023, principal investigator.
• *Hardware Security of Neural Networks*, SASPRO-2 Grant, European Union's Horizon 2020 research and innovation programme, Marie Skłodowska-Curie funding scheme No. 945478, 2021 - 2024, main recipient.

PROGRAM COMMITTEE MEMBER

- IACR Cryptographic Hardware and Embedded Systems Conference (CHES) 2021, 2022.
- 30th IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC) 2022
- 27th Australasian Conference on Information Security and Privacy (ACISP) 2022.
- 3rd workshop on Artificial Intelligence in Hardware Security (AIHWS) 2022.
- Informatics and Information Technologies Student Research Conference (IIT.SRC) 2021, 2022.
- 29th IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC) 2021.
- IEEE International Conference on High Performance Computing and Communications (HPCC) 2020, 2021.

OTHER SCIENTIFIC AND SOCIETAL IMPACT

- Guest editor for special issue on Fault Analysis in Cryptography in Cryptography journal, MDPI, 2022.
- Session chair for IACR Cryptographic Hardware and Embedded Systems Conference (CHES) 2020, 2021.
- Member of organization team for International Workshop on Constructive Side-Channel Analysis and Secure Design (Cosade) 2018.
- Judge for Singapore International Mathematics Challenge 2014.
- Reviewer for international scientific journals.

HONORS

- *Nanyang President's Graduate Scholarship*, a competitive and prestigious scholarship scheme for outstanding graduate. 2013 - 2017.
- *Lee Kuan Yew Gold Medal*, the most prestigious award in NTU, 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. 2012.
- *Dean's list*, 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.
- *SM2 Scholarship* for undergraduate studies at NTU through a selection with exams and interview. 2009 - 2012.

TEACHING EXPERIENCE

Teaching Assistant at NTU, Singapore:

- *Discrete Mathematics*, an introductory course of discrete mathematics for first year mathematics students, Jan - May 2016 and Jan - May 2015
- *Group and Symmetries*, an introductory course of abstract algebra for second year mathematics students, Aug - Dec 2015
- *Discrete Mathematics for Engineering School*, an introductory course of discrete mathematics for first year computer science and computer engineering students, Aug - Dec 2014
- *Engineering Math*, an introductory course of linear algebra and calculus for first year engineering students, Aug - Dec 2012

INVITED TALKS

- *Reverse Engineering of Neural Networks with Fault Attacks*, AICrypt workshop, collocated with Eurocrypt 2021, Zagreb, Croatia, 16th Oct 2021.
- *AI for Physical Attacks and Physical Attacks on AI*, Advances in Applied Mathematical Sciences Webinar, Department of Mathematics and Statistics, Newman College, Thodupuzha (affiliated to M G University, Kottayam), Kerala, India, 23rd Sep 2021.
- *Side-Channel Attacks*, Information security seminar at FIIT STU, Bratislava, Slovakia, 11th Jun 2021.
- *On Side Channel and Fault Attacks against Machine Learning*, Virtual Workshop on Machine Learning & Hardware Security, 26th August 2020.
- *Side-Channel Analysis for Reverse Engineering of Secret Cipher*, 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*, Computational & Statistical Sciences (MCSS) Seminar, Yale-NUS, Singapore, 26th Sep 2016.

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*)