

# Xiaolu Hou

Faculty of Informatics and Information Technologies,  
Slovak University of Technology in Bratislava

Ilkovičova 2, 842 16 Bratislava, Slovakia

Email: houxiaolu.email@gmail.com Web: <https://xiaoluhou.github.io/>

---

## RESEARCH FOCUS

- Hardware security of neural network and cryptographic implementations
- Fault injection and side-channel attacks, and corresponding countermeasures
- Security assessment and evaluation methodologies

---

## ACADEMIC QUALIFICATIONS

**Habilitation (Docent) in Informatics** Aug 2025  
Slovak University of Technology (STU)  
*Habilitation thesis title:* Hardware Security of Neural Networks

---

## EDUCATION

**PhD 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

**BSc in Mathematical Sciences (Pure Mathematics)** Aug 2009 – Jan 2012  
Nanyang Technological University (NTU), Singapore First-Class Honours, CGPA: 4.96/5.00

---

## EXPERIENCE

**Faculty Member at Faculty of Informatics and Information Technologies (FIIT), STU**

Associate Professor Oct 2025 – Present  
Marie Skłodowska-Curie Research Fellow Oct 2021 – Sep 2025  
Assistant Professor Mar 2021 – Sep 2021

- Research in hardware security, cryptography, and AI security
- Supervision of PhD, Master's, and Bachelor's students

**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 the usage of onboard analog-to-digital converters for side-channel leakage.
- Developing countermeasures against physical attacks.
- Evaluating neural network security with respect to fault attacks.

**Research Fellow at School of Computing, 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)**

**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 to locate a victim using applications on a mobile device

---

#### **GRANTS**

- *Implementation Security of Neural Networks*, project of the Slovak Research and Development Agency, SK-SRB-21-0059, March 2022 - Dec 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, Oct 2021 - Sep 2025, main recipient.

---

#### **HONORS AND AWARDS**

- *L'Oréal-UNESCO for women in science, Slovakia*, 2022
- *Rector's award for female scientist*, Slovak University of Technology, 2021.
- *Nanyang president's graduate scholarship*, a competitive and prestigious scholarship scheme for outstanding graduates. 2013 - 2017.
- *Lee Kuan Yew gold medal*, the most prestigious award for undergraduates at NTU, given to the top student in each degree program of the graduating cohort who has excelled in general proficiency and has obtained the 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 program, 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 interviews. 2009 - 2012.

---

#### **PROGRAM COMMITTEE MEMBER**

- Design, Automation and Test in Europe Conference (DATE) 2024, 2025, 2026.
- International Conference on the Theory and Applications of Cryptology and Information Security (Asiacrypt) 2023, 2026.
- Workshop on Attacks and Solutions in Hardware Security (ASHES), collocated with ACM Conference on Computer and Communications Security (CCS) 2025.
- IACR Cryptographic Hardware and Embedded Systems Conference (CHES) 2021, 2022, 2023, 2025.
- Australasian Conference on Information Security and Privacy (ACISP) 2022, 2023, 2025, 2026.
- IEEE/ACM International Symposium on Low Power Electronics and Design (ISLPED) 2025.
- International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I), in conjunction with the International Conference on Availability, Reliability and Security (ARES) 2023, 2024, 2025.
- International Symposium on Cyber Security Cryptography and Machine Learning (CSCML) 2024.
- International Conference on the Theory and Applications of Cryptology and Information Security (Eurocrypt) 2024.
- IEEE International Conference on High Performance Computing and Communications (HPCC) 2020, 2021, 2022, 2024.
- IEEE International Conference on Parallel and Distributed Systems (ICPADS) 2023.
- Workshop on Artificial Intelligence in Hardware Security (AIHWS) 2022.
- IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC) 2021, 2022.

---

#### **OTHER SCIENTIFIC AND SOCIETAL IMPACT**

- Editorial board member, IACR Communications in Cryptology (CiC), 2024 – 2026.
- Panelist, Complex View on Generative AI, AmCham conference, Bratislava, Slovakia, April 2023.
- Panelist, European Researcher's Night Science Festival, Bratislava, Slovakia, Sep, 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.

## **TEACHING EXPERIENCE**

---

### **Faculty of Informatics and Information Technologies (FIIT), STU**

- *Cryptography and Embedded Systems Security* — advanced Master's-level course focused on hardware security, side-channel and fault attacks, and countermeasures, Sep 2022 – Present
- *Algebra and Discrete Mathematics* — foundational Bachelor's-level course in the English programme, covering linear algebra and graph theory, Sep 2025 – Present

### **EC-Council (Online)**

- *Cryptography and Embedded Systems Security* — online professional course introducing side-channel analysis, fault attacks, and practical countermeasures, [course link](#), 2024

### **Nanyang Technological University (NTU), Singapore**

- *Discrete Mathematics* — introductory course for first-year mathematics students, Jan – May 2015 and Jan – May 2016
- *Groups and Symmetries* — introductory abstract algebra course for second-year mathematics students, Aug – Dec 2015
- *Discrete Mathematics (Engineering Programme)* — introductory course for first-year computer science and computer engineering students, Aug – Dec 2014
- *Engineering Mathematics* — introductory course in linear algebra and calculus for first-year engineering students, Aug – Dec 2012

## **SUPERVISED MASTER'S THESES**

---

- *Protecting AI from Side-Channel Attacks through Shuffling*, Leonard Puškáč, 2025.
- *AI-assisted Side-Channel Attacks*, Miroslav Todorović, 2025.
- *Encoding-based Protection for Quantized Neural Networks Against Fault Attacks*, Patrik Velčický, 2024.
- *Bit Flip Attack – Analysis of State of the Art Attacks with Proposed Countermeasures*, Marek Benovič, 2024.
- *Fault Attacks on Training Phase of Deep Neural Networks*, Dominik Bucko, 2023.

## **SUPERVISED BACHELOR THESES**

---

- *Correlation Power Analysis on Public Datasets*, Patrik Baran, 2025.
- *Information Leakage of Neural Network*, Zdenko Lehocký, 2024.
- *Analysis of Quantized Neural Networks*, Martin Čajka, 2024
- *Leakage Assessment for Side-channel Attacks*, Farkas Noémi, 2023.
- *Construction of Data Flow Graph for Cryptographic Implementations*, Yelyzaveta Klysa, 2022.
- *Cryptanalysis Aided by AI*, Patrik Velčický, 2022.
- *Cryptanalysis Aided by AI*, Kristián Escher, 2022.

## **INVITED TALKS**

---

- *Hardware Security of Cryptography*, FIIT Girls Day, Slovakia, April 2025.
- *Attacks and Countermeasures for AI-Assisted Traffic Sign Classification*, Road Transport Safety, BECEP conference, Slovakia, Sep 2024.
- *Adversarial attacks on neural networks*, ITAPA AI & Robotics, Slovakia, Mar 2024.
- *Countermeasures Against Side-Channel Analysis Attacks*, Faculty of Electrical Engineering, Slovak University of Technology, Dec 2023.

- *FooBar: Fault Fooling Backdoor Attack on Neural Network Training*, CNC seminar, Centre for Cognitive Science, Faculty of Mathematics, Physics and Informatics, Comenius University, Bratislava, Slovakia, Feb 2023.
- *Artificial Intelligence-Assisted Side Channel Attacks*, Keynote speaker, The 2nd International Workshop on Security and Privacy in Intelligent Infrastructures, in conjunction with the 17th International Conference on Availability, Reliability and Security, Vienna, Austria, Aug 2022.
- *Reverse Engineering of Neural Networks with Fault Attacks*, AICrypt workshop, collocated with Eurocrypt 2021, Zagreb, Croatia, Oct 2021.
- *AI for Physical Attacks and Physical Attacks on AI*, Advances in Applied Mathematical Sciences Webinar, Department of Mathematics and Statistics, Newman College, India, 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 Aug 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 Jul 2018.
- *Construction of Modular Lattices from Linear Codes and Number Fields*, Computational & Statistical Sciences (MCSS) Seminar, Yale-NUS, Singapore, 26th Sep 2016.

## PATENTS

---

- Systems and Methods for Performing Secure Computing While Maintaining Data Confidentiality, Sivanesan Kailash Prabhu, Mark Will, Sanjeev Solanki, Aarthi Kannan, Xiaolu Hou, Serguei Belousov, and Stanislav Protasov, US20210286883A1, granted 1st March 2023.

## PUBLICATIONS

---

### Book:

1. *Cryptography and Embedded Systems Security*, Xiaolu Hou and Jakub Breier, ISBN: 978-3-031-62205-2, Springer Nature, 2024.
2. *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. *Make Shuffling Great Again: A Side-Channel Resistant Fisher-Yates Algorithm for Protecting Neural Networks*, Leonard Puškáč, Marek Benovič, Jakub Breier, and Xiaolu Hou, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, no. 7, 2025.
- J2. *Another Look at Side-Channel-Resistant Encoding Schemes*, Xiaolu Hou, Jakub Breier, Mladen Kovačević, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, no. 8, 2024.
- J3. *New Results on Machine Learning-Based Distinguishers*, Anubhab Baksi, Jakub Breier, Vishnu Asutosh Dasu, Xiaolu Hou, Hyunji Kim, Hwajeong Seo, IEEE Access, no. 11, 2023.
- J4. *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), no. 3, 2023.
- J5. *SNIFF: reverse engineering of neural networks with fault attacks*, Jakub Breier, Dirmanto Jap, Xiaolu Hou, Shivam Bhasin, Yang Liu, IEEE Transactions on Reliability, no. 4, 2022.
- J6. *How Practical are Fault Injection Attacks, Really?*, Jakub Breier, Xiaolu Hou, IEEE Access, no. 10, 2022.
- J7. *SBCMA: Semi-Blind Combined Middle-Round Attack on Bit-Permutation Ciphers with Application to AEAD Schemes*, Xiaolu Hou, Jakub Breier, Shivam Bhasin, IEEE Transactions on Information Forensics and Security (TIFS), 2022.
- J8. *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.

- J9. *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 (TCCHES), no. 1, 2022.
- J10. *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.
- J11. *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.
- J12. *On Evaluating Fault Resilient Encoding Schemes in Software*, Jakub Breier, Xiaolu Hou, Yang Liu, IEEE Transactions on Dependable and Secure Computing (TDSC), no. 3, 2021.
- J13. *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.
- J14. *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 (TCCHES), no. 1, 2020.
- J15. *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.
- J16. *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 (TCCHES), no. 3, 2019.
- J17. *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 (TCCHES), no. 2, 2018.
- J18. *Modular Lattices from a Variation of Construction A over Number Fields*, Xiaolu Hou and Frédérique Oggier, Advances in Mathematics of Communications, no. 4, 2017.
- J19. *Construction of Arakelov-modular Lattices over Totally Definite Quaternion Algebras*, Xiaolu Hou, International Journal of Number Theory, no. 7, 2017.
- J20. *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.
- J21. *Composition operators on Hilbert spaces of entire Dirichlet series*, Xiaolu Hou, Le Hai Khoi and Bingyang Hu, Comptes Rendus Mathématique, no. 19–20, 2012.
- J22. *Some properties of composition operators on entire Dirichlet series with real frequencies*, Xiaolu Hou and Le Hai Khoi, Comptes Rendus Mathématique, no. 3–4, 2012.

### Conference Proceedings:

- C1. *Side-Channel Analysis of OpenVINO-based Neural Network Models*, Zdenko Lehocký, Jakub Breier, Dirmanto Jap, Shivam Bhasin and Xiaolu Hou, International Workshop on Security and Privacy in Intelligent Infrastructures (SP2I), in conjunction with the International Conference on Availability, Reliability and Security (ARES) 2025.
- C2. *A Desynchronization-Based Countermeasure Against Side-Channel Analysis of Neural Networks*, Jakub Breier, Dirmanto Jap, Xiaolu Hou, and Shivam Bhasin, The International Symposium on Cyber Security, Cryptology and Machine Learning (CSCML) 2023.
- C3. *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.
- C4. *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.
- C5. *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.

- C6. *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.
- C7. *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.
- C8. *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.
- C9. *On LCD Codes and Lattices*, Xiaolu Hou, and Frédérique Oggier, IEEE International Symposium on Information Theory (ISIT) 2016, Barcelona, Spain.
- C10. *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.