JAKUB BREIER

jakub.breier@gmail.com | +421 948 752 069 | jbreier.com | LinkedIn | Google Scholar | dblp

STRATEGIC PROFILE

Hardware security researcher and Principal Security Architect with over a decade of experience in fault injection, side-channel analysis, cryptography, and AI model security. PhD in Applied Informatics, with a focus on information security, and co-author of two Springer books. Research contributions span physical attacks on cryptographic implementations and neural networks, with over 2,600 citations and an h-index of 29 (November 2026). Current industry work focuses on security architecture and assurance for quantum key distribution (QKD) systems.

CORE COMPETENCIES & TECHNICAL EXPERTISE

Hardware Security Research: Fault Injection (laser, electromagnetic), Side-Channel Analysis, Physical Security of Deep Learning Models, Hardware Security Modules
Cryptography: Symmetric Ciphers, Post-Quantum Cryptography (Ascon-Sign – NIST PQC Round 1 candidate), Implementation Security, Co-designer of DEFAULT and BAKSHEESH cipher primitives, Quantum Key Distribution
AI & Machine Learning Security: Physical Attacks on Neural Networks, Fault Backdoor Attacks, Side-Channel Leakage Detection, Adversarial ML Security
Embedded Systems: Automotive ECUs, HMIs, Edge AI Devices, Microcontrollers, FPGAs
Programming & Tools: Python, C/C++, Java, MATLAB, Atmel Assembly; Oscilloscopes, Lasers, Pulse Generators, High-Power Amplifiers

EXPERIENCE

Principal Security Architect November 2026 – Present
qtlabs – Quantum Technology Laboratories GmbH *Vienna, Austria*

- Designing and assessing security architectures for satellite-based quantum key distribution (QKD) systems, including interfaces between space and ground segments
- Developing system-level security requirements and threat models, with attention to protocol, implementation, and physical attack surfaces
- Supporting security assurance and Common Criteria (ISO/IEC 15408) certification activities, including evaluation planning and requirements traceability
- Contributing security expertise to EU-funded quantum communication projects

Senior Cybersecurity Manager July 2023 – October 2026
TTControl GmbH *Vienna, Austria*

- Conducted hardware security research on automotive ECUs and HMIs, investigating physical attack surfaces including fault injection and side-channel vulnerabilities on embedded AI and cryptographic implementations
- Contributed as a researcher to Horizon Europe project aerOS[1], focusing on security of IoT edge-cloud systems
- Contributed as a researcher to Chips Joint Undertaking project Mosaic[2], focusing on next-generation, energy-efficient, and robust cognitive electronic components and systems.
- Established the company's cybersecurity function as the sole security professional, covering 40+ products across automotive ECU and HMI product lines, including hardware security architecture and threat modeling for embedded systems
- Delivered end-to-end ISO/SAE 21434 CSMS and managed compliance across EU Cyber Resilience Act, IEC 62443, and RED Cyber

Senior Scientist, Embedded Security September 2020 – June 2023
Silicon Austria Labs *Graz, Austria*

- Conducted research on physical security of edge AI models, including side-channel vulnerabilities of embedded neural network inference

[1] https://aeros-project.eu
[2] https://chips-mosaic.eu/

- Conceived and executed the SECAI project (Security of Edge AI) as sole researcher, from proposal authorship through research delivery
- Published research in IEEE TIFS, TCHES, and other top venues on cryptographic implementation security

Cybersecurity Research Lead / **Principal Research Fellow** May 2019 – September 2020

HP-NTU Digital Manufacturing Corporate Lab *Singapore*

- Directed a multidisciplinary team of 12 researchers across four industrial projects, managing the full research budget and reporting directly to C-level executives
- Investigated the following topics: Secure machine learning; Evaluation of malware detection techniques; 3D object identification; Visual inspection of printed circuit assembly components
- Supported cooperation between the university and HP

Senior Cryptography Security Analyst September 2018 – April 2019

Underwriters Laboratories *Singapore*

- Evaluated security of smart cards against physical attacks and certified them in accordance with certification criteria (EMVco, VISA, MasterCard, American Express)
- Evaluated the resistance of cryptographic implementations used in payment schemes – both public key and symmetric key encryption
- Developed novel attacks and protection methods for side-channel analysis and fault analysis
- Contributed to ISO 17025 certification of the laboratory equipment

Research Scientist (Senior from July 2017) November 2013 – September 2018

Nanyang Technological University *Singapore*

- Unit: Physical Analysis and Cryptographic Engineering Laboratory
- Improved state-of-the-art of secure cryptographic implementations with respect to resistance against physical attacks
- Developed software and hardware countermeasures against side-channel and fault attacks

Visiting Researcher April 2014 – July 2014

Fraunhofer AISEC *Munich, Germany*

- Worked in the field of laser fault injection attacks

EDUCATION

Slovak University of Technology Bratislava, Slovakia

PhD in Applied Informatics *25 October 2013*

- Faculty: Faculty of Informatics and Information Technologies
- Thesis title: Security Evaluation Supported by Information Security Risk Mechanisms
- The thesis developed a novel security evaluation with respect to the ISO/IEC 27002 standard and explored new ways of improving the objectivity and the repeatability of such evaluation.

Masaryk University Brno, Czech Republic

Master in Information Technology Security *29 June 2010*

- Faculty: Faculty of Informatics
- Thesis title: Differential Power Analysis of Rijndael Operations on a Selected Microcontroller
- The main goal of the thesis was to perform the differential power analysis attack in different conditions and on multiple implementations of AES.

Slovak University of Technology Bratislava, Slovakia

Bachelor of Informatics *4 July 2008*

- Faculty: Faculty of Informatics and Information Technologies
- Thesis title: Catalogue of Changes Realized by Aspect-oriented Programming
- This thesis aimed to investigate the possibilities of compilation-level changes that could be done by aspect-oriented programming.

Editorial Board and Program Committee Memberships (selected venues)

- Editorial board member of the IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) 2027
- Editorial board member of the IACR Communications in Cryptology (CiC) 2024, 2025, 2026, 2027
- Co-chair of the SEC3: Hardware Security Attack and Defense track at The Chips to Systems Conference (DAC) 2027
- Co-chair of the Hardware and System Security Track at The International Symposium on Low Power Electronics and Design (ISLPED) 2025, 2026
- Program committee member of the Hardware Security: Attack and Defense track at The Chips To Systems Conference (DAC) 2026
- Program committee member of DT6 Track: Design and Test of Secure Systems at The Design, Automation and Test in Europe Conference (DATE) 2027
- Program committee member of the International Symposium on Hardware Oriented Security and Trust (HOST) 2026, 2027
- Program committee member of the International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC) 2022, 2023, 2024, 2025
- Program committee member of the International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE) 2021, 2022, 2023, 2024

Selected Key Achievements

- Co-designer of *Ascon-Sign*[3], a NIST Post-Quantum Cryptography Competition candidate for Digital Signature Schemes (Round 1 Additional Signatures)
- Co-author of a technical disclosure “Managing Risk when Deploying a Solution Using Machine Learning” in collaboration with Adrian Baldwin and Helen Balinsky from HP Inc.[4]
- Delivered talks at RSA Conference USA in 2017 and 2019

Project Participation

- Senior project member for the “Autonomous, Scalable, Trustworthy, Intelligent European Meta Operating System for the IoT Edge-Cloud Continuum” (aerOS) project, funded by the European Commission via Horizon Europe funding programme.
- Project manager and proposal author for the “Security of Edge Artificial Intelligence” (SECAI) project, funded by Silicon Austria Labs, Graz.
- Principal scientist (lead) for four industrial projects in collaboration with HP Inc.: “Secure Machine Learning”, “Evaluation of Malware Detection Techniques”, “3D Object Identification”, and “Visual Inspection of Printed Circuit Assembly Components”, co-funded by HP Inc. and National Research Foundation, Singapore.
- Senior project member and proposal co-author for the “Hyper Side-Channel Analysis” (Hyper-SCA) project, funded by DSO National Laboratories, Singapore.
- Senior project member for the “Physical Analysis and Cryptographic Engineering” (PACE) project, funded by DSO National Laboratories, Singapore.

[3] https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/Ascon-sign-spec-web.pdf
[4] https://www.tdcommons.org/cgi/viewcontent.cgi?article=5267&context=dpubs_series

Most Important Scientific Talks

AI-accelerated Implementation Testing: Research vs. Practice
Online; Worcester Polytechnic Institute, MA, USA 10 April 2025
- An Open Source Ecosystem for Implementation Security Testing (OPTIMIST)[5]

Security Evaluation of Vehicular Electronic Control Units
Online; Štrbské Pleso, Slovakia 19 September 2024
- Road Transport Safety Conference BECEP 2024

Hardware Security of Cryptography and Deep Learning
Online; Palo Alto, CA, USA 30 August 2022
- Dealer Seminar, Palo Alto Research Center (PARC), Xerox

Machine Learning Assisted Differential Distinguishers For Lightweight Ciphers
Online 2 February 2021
- Design, Automation and Test in Europe Conference

Cryptography in Payment Systems
Yogyakarta, Indonesia 26 July 2019
- SEAMS-UGM-ITB Summer Course on Coding Theory and Cryptography

Fully Automated Differential Fault Analysis on Software Implementations of Block Ciphers
Atlanta, USA 28 August 2019
- Conference on Cryptographic Hardware and Embedded Systems

Automated Fault Analysis of Block Cipher Implementations
San Francisco, USA 6 March 2019
- RSA Conference 2019

Fault Analysis Automation on Software Targets
Kharagpur, India 3 July 2018
- Targeted Training on Advanced Side Channel Evaluation of Hardware Security

Fault Injection Attacks and Countermeasures
Brno, Czech Republic 28 March 2018
- Brno Security Meetings, FEKT VUT

Fault Attacks on Cryptographic Devices
Vienna, Austria 18 May 2016
- IEEE CS/SMCS Austria Chapter, SBA Research

Security Evaluation Supported by Information Security Mechanisms
Munich, Germany 25 June 2014
- Technical University Munich, EI SEC PhD Seminar

[5] https://optimist-ose.org/docs/ai/intro

Teaching Experience

Cryptography and Embedded Systems Security (graduate)
Slovak University of Technology 2022 – Present
- Side-channel attacks, fault injection attacks, secure cryptographic implementations, countermeasures
- Course textbook:
  Xiaolu Hou and Jakub Breier. *Cryptography and Embedded Systems Security,* Springer, 2024.

Cryptography and Embedded Systems Security (online on-demand)
EC-Council 2025 – Present
- A 5-hour online course covering a subset of topics of the university course
- Accessible at https://codered.eccouncil.org/course/cryptography-and-embedded-systems-security

Team Project (graduate)
Slovak University of Technology 2024 – Present
- Leading two-semester 6-person team projects focused on various security topics
- 2025/2026: Developing an intelligent automated TARA framework for automotive security
- 2024/2025: Building a laser fault injection station for hardware attacks

SEAMS-UGM-ITB Summer Course on Coding Theory and Cryptography
Universitas Gadjah Mada, Yogyakarta, Indonesia July 15-26, 2019
- Side-channel attacks, real-world security evaluation and certification

Targeted Training on Advanced Side Channel Evaluation of Hardware Security
Indian Institute of Technology, Kharagpur, India July 2-6, 2018
- Hardware attacks, fault injection attacks, attack automation

Security of Computer Systems (graduate)
Slovak University of Technology 2010 - 2013
- Communication security, security of operating systems, software security, cryptography, security evaluation

Security on Internet (graduate)
Slovak University of Technology 2010 - 2013
- Security of Internet protocols, web security, authentication protocols, penetration testing, PKI

Linear Algebra I (undergraduate)
Slovak University of Technology 2012 - 2013
- Linear systems, vector spaces, matrix operations

Supervised Theses

Hardware Security of Neural Networks | *Doctoral Thesis (co-supervision with Dr. Xiaolu Hou)* ongoing
- Student: Ján Mikulec

Laser Fault Attacks on Embedded Neural Network Implementations | *Master Thesis* ongoing
- Student: Marko Šebest

Remote Attacks by Using the DVFS Technique | *Master Thesis* ongoing
- Student: Jaroslav Samuel Griščík

Deep Learning-Based Side-Channel Analysis | *Master Thesis* 2025
- Student: Samuel Filo

Data Mining for Security Purposes | *Master Thesis* 2014
- Student: Martin Uhrin

Anomaly Detection From Log Files Using Data Mining and Visualization | *Master Thesis* 2014
- Student: Jana Branišová
- Resulted in two international peer-reviewed publications (conference+journal)

Qualified Electronic Signature via Mobile Phone | *Master Thesis* 2013
- Student: Adam Pomothy
- Resulted in one international peer-reviewed conference publication

E-learning System for Teaching Network Security | *Bachelor Thesis* 2012
- Student: Michal Petráš

ACADEMIC SERVICE

- External examiner for Patrik Dobiáš's PhD thesis, Brno University of Technology, Czech Republic, 2026
- External examiner for Petr Socha's PhD thesis, Czech Technical University in Prague, Czech Republic, 2023
- External examiner for Josef Kokeš's PhD thesis, Czech Technical University in Prague, Czech Republic, 2022
- Reviewer of a grant proposal submitted to the Deutsche Forschungsgemeinschaft (DFG), 2022
- Reviewer of a Vici grant proposal submitted to The Netherlands Organisation for Scientific Research, NWO, 2019

List of Publications

ORCID: https://orcid.org/0000-0002-7844-5267
Google Scholar: https://scholar.google.com/citations?user=LOENK6IAAAAJ&hl=en
citations: 2721; h-index: 29; i10-index: 63 (as of 27 Nov 2026)

Best paper award:ACM CompSysTech 2012 (conference publication [43])

Preprints & manuscripts under review

[1] Jakub Breier and Xiaolu Hou. *Automotive Hardware Attacks: An Architect's Guide to TARA*. Under Review. 2026. URL: https://arxiv.org/abs/2610.09697.

[2] Jakub Breier, Štefan Kučerák, and Xiaolu Hou. *The Weight of a Bit: EMFI Sensitivity Analysis of Embedded Deep Learning Models*. Under Review. 2026. URL: https://arxiv.org/abs/2602.16309.

[3] Štefan Kučerák, Jakub Breier, and Xiaolu Hou. *Characterizing the Fault Response of the Intel Neural Compute Stick 2 Under Single-Pulse Electromagnetic Fault Injection*. Under Review. 2026. URL: https://arxiv.org/abs/2605.22437.

[4] Camilo A Martínez-Mejía, Jesus Solano, Jakub Breier, Dominik Bucko, and Xiaolu Hou. *DeepBaR: Fault backdoor attack on deep neural network layers*. Under Review. 2026. URL: https://arxiv.org/abs/2407.21220.

[5] Ján Mikulec, Jakub Breier, and Xiaolu Hou. *Beyond TVLA: Anderson-Darling Leakage Assessment for Neural Network Side-Channel Leakage Detection*. Under Review. 2026. URL: https://arxiv.org/abs/2603.18647.

[6] Andrii Tyvodar, Andreas Rechberger, Dirmanto Jap, Shivam Bhasin, Bernhard Jungk, Jakub Breier, and Xiaolu Hou. *A Constant-Time Implementation Methodology for Activation Functions on Microcontrollers*. Under Review. 2026. URL: https://arxiv.org/abs/2605.22441.

Books

[1] Xiaolu Hou and Jakub Breier. *Cryptography and Embedded Systems Security*. Springer, 2024. ISBN: 978-3-031-62204-5. URL: https://link.springer.com/book/9783031622045.

[2] Jakub Breier, Xiaolu Hou, and Shivam Bhasin. *Automated Methods in Cryptographic Fault Analysis*. Springer, 2019. ISBN: 978-3-030-11333-9. DOI: 10.1007/978-3-030-11333-9.

Book chapters

[1] Jakub Breier. "Foreword". In: *Implementation and Analysis of Ciphers in Quantum Computing*. Ed. by Anubhab Baksi and Kyungbae Jang. Springer, 2023. ISBN: 978-981-97-0024-0. DOI: 10.1007/978-981-97-0025-7.

[2] Lejla Batina, Shivam Bhasin, Jakub Breier, Xiaolu Hou, and Dirmanto Jap. "On Implementation-Level Security of Edge-Based Machine Learning Models". In: *Security and Artificial Intelligence: A Crossdisciplinary Approach*. Ed. by Lejla Batina, Thomas Bäck, Ileana Buhan, and Stjepan Picek. Springer, 2022, pp. 335–359. ISBN: 978-3-030-98795-4. DOI: 10.1007/978-3-030-98795-4_14.

[3] Jakub Breier, Wei He, and Shivam Bhasin. "Reactive Design Strategies Against Fault Injection Attacks". In: *Fault Tolerant Architectures for Cryptography and Hardware Security*. Ed. by Sikhar Patranabis and Debdeep Mukhopadhyay. Singapore: Springer Singapore, 2018, pp. 213–229. ISBN: 978-981-10-1387-4. DOI: 10.1007/978-981-10-1387-4_11.

[4] Jakub Breier, Dirmanto Jap, and Chien-Ning Chen. “Laser-Based Fault Injection on Microcontrollers”. In: *Fault Tolerant Architectures for Cryptography and Hardware Security*. Ed. by Sikhar Patranabis and Debdeep Mukhopadhyay. Singapore: Springer Singapore, 2018, pp. 81–110. ISBN: 978-981-10-1387-4. DOI: 10.1007/978-981-10-1387-4_5.

[5] Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, and Shivam Bhasin. “Side-Channel Assisted Fault Analysis”. In: *Fault Tolerant Architectures for Cryptography and Hardware Security*. Ed. by Sikhar Patranabis and Debdeep Mukhopadhyay. Singapore: Springer Singapore, 2018, pp. 59–77. DOI: 10.1007/978-981-10-1387-4_4.

Articles in peer-reviewed journals

[1] Anubhab Baksi, Jakub Breier, Anupam Chattopadhyay, Tomáš Gerlich, Sylvain Guilley, Naina Gupta, Takanori Isobe, Arpan Jati, Petr Jedlicka, Hyunjun Kim, Fukang Liu, Zdeněk Martinásek, Kosei Sakamoto, Hwajeong Seo, and Rentaro Shiba. “BAKSHEESH: Similar Yet Different From GIFT (and ZORRO)”. In: *IACR Communications in Cryptology* 2.4 (Jan. 8, 2026). ISSN: 3006-5496. DOI: 10.62056/ae890lmol.

[2] Patrik Velčický, Jakub Breier, Mladen Kovačević, and Xiaolu Hou. “DeepNcode: Encoding-Based Protection against Bit-Flip Attacks on Neural Networks”. In: *IEEE Transactions on Emerging Topics in Computing* (2026).

[3] Kyungbae Jang, Anubhab Baksi, Jakub Breier, Hwajeong Seo, and Anupam Chattopadhyay. “Quantum Implementation and Analysis of DEFAULT”. In: *Cryptography and Communications* (2025), pp. 359–375. DOI: 10.1007/s12095-023-00666-y.

[4] Leonard Puškáč, Marek Benovič, Jakub Breier, and Xiaolu Hou. “Make Shuffling Great Again: A Side-Channel Resistant Fisher-Yates Algorithm for Protecting Neural Networks”. In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2025). DOI: 10.1109/TVLSI.2025.3564357.

[5] Xiaolu Hou, Jakub Breier, and Mladen Kovačević. “Another Look at Side-Channel-Resistant Encoding Schemes”. In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2024).

[6] Anubhab Baksi, Shivam Bhasin, Jakub Breier, Dirmanto Jap, and Dhiman Saha. “A Survey on Fault Attacks on Symmetric Key Cryptosystems”. In: *ACM Comput. Surv.* 55.4 (2023). ISSN: 0360-0300. DOI: 10.1145/3530054.

[7] Jakub Breier, Xiaolu Hou, Martín Ochoa, and Jesus Solano. “FooBaR: Fault Fooling Backdoor Attack on Neural Network Training”. In: *IEEE Transactions on Dependable and Secure Computing* 20.3 (2023), pp. 1895–1908. DOI: 10.1109/TDSC.2022.3166671.

[8] Francesco Berti, Shivam Bhasin, Jakub Breier, Xiaolu Hou, Romain Poussier, François-Xavier Standaert, and Balasz Udvarhelyi. “A Finer-Grain Analysis of the Leakage (Non) Resilience of OCB”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022), pp. 461–481.

[9] Jakub Breier and Xiaolu Hou. “How Practical Are Fault Injection Attacks, Really?” In: *IEEE Access* 10 (2022), pp. 113122–113130. DOI: 10.1109/ACCESS.2022.3217212.

[10] Jakub Breier, Dirmanto Jap, Xiaolu Hou, Shivam Bhasin, and Yang Liu. “SNIFF: Reverse Engineering of Neural Networks With Fault Attacks”. In: *IEEE Transactions on Reliability* 71.4 (2022), pp. 1527–1539. DOI: 10.1109/TR.2021.3105697.

[11] Xiaolu Hou, Jakub Breier, and Shivam Bhasin. “SBCMA: Semi-Blind Combined Middle-Round Attack on Bit-Permutation Ciphers With Application to AEAD Schemes”. In: *IEEE Transactions on Information Forensics and Security* 17 (2022), pp. 3677–3690. DOI: 10.1109/TIFS.2022.3213424.

[12] Satyam Kumar, Vishnu Asutosh Dasu, Anubhab Baksi, Santanu Sarkar, Dirmanto Jap, Jakub Breier, and Shivam Bhasin. “Side Channel Attack On Stream Ciphers: A Three-Step Approach To State/Key Recovery”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2022), pp. 166–191.

[13] Xiaolu Hou, Jakub Breier, Dirmanto Jap, Lei Ma, Shivam Bhasin, and Yang Liu. “Physical security of deep learning on edge devices: Comprehensive evaluation of fault injection attack vectors”. In: *Microelectronics Reliability* 120 (2021), p. 114116.

[14] Yoo-Seung Won, Xiaolu Hou, Dirmanto Jap, Jakub Breier, and Shivam Bhasin. “Back to the Basics: Seamless Integration of Side-Channel Pre-Processing in Deep Neural Networks”. In: *IEEE Transactions on Information Forensics and Security* 16 (2021), pp. 3215–3227.

[15] Manaar Alam, Arnab Bag, Debapriya Basu Roy, Dirmanto Jap, Jakub Breier, Shivam Bhasin, and Debdeep Mukhopadhyay. “Neural Network-based Inherently Fault-tolerant Hardware Cryptographic Primitives without Explicit Redundancy Checks”. In: *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 17.1 (2020), pp. 1–30.

[16] Shivam Bhasin, Jakub Breier, Xiaolu Hou, Dirmanto Jap, Romain Poussier, and Siang Meng Sim. “SITM: See-In-The-Middle — Side-Channel Assisted Middle Round Differential Cryptanalysis on SPN Block Ciphers”. In: *Transactions on Cryptographic Hardware and Embedded Systems (TCHES)* 3.1 (Nov. 2020), pp. 95–122.

[17] Jakub Breier, Dirmanto Jap, Xiaolu Hou, and Shivam Bhasin. “On Side Channel Vulnerabilities of Bit Permutations in Cryptographic Algorithms”. In: *Transactions on Information Forensics and Security (TIFS)* 15 (2020), pp. 1072–1085.

[18] Jakub Breier, Mustafa Khairallah, Xiaolu Hou, and Yang Liu. “A countermeasure against statistical ineffective fault analysis”. In: *IEEE Transactions on Circuits and Systems II: Express Briefs* 67.12 (2020), pp. 3322–3326.

[19] Jakub Breier, Xiaolu Hou, and Yang Liu. “On evaluating fault resilient encoding schemes in software”. In: *IEEE Transactions on Dependable and Secure Computing* (2019).

[20] Xiaolu Hou, Jakub Breier, Fuyuan Zhang, and Liu Yang. “Fully Automated Differential Fault Analysis on Software Implementations of Block Ciphers”. In: *Transactions on Cryptographic Hardware and Embedded Systems (TCHES)* 2.3 (May 2019), pp. 1–29.

[21] Sikhar Patranabis, Nilanjan Datta, Dirmanto Jap, Jakub Breier, Shivam Bhasin, and Debdeep Mukhopadhyay. “SCADFA: Combined SCA+DFA Attacks on Block Ciphers with Practical Validations”. In: *Transactions on Computers* 68.10 (Oct. 2019), pp. 1498–1510.

[22] Jakub Breier, Xiaolu Hou, and Liu Yang. “Fault Attacks Made Easy: Differential Fault Analysis Automation on Assembly Code”. In: *Transactions on Cryptographic Hardware and Embedded Systems (TCHES)* 1.2 (Apr. 2018), pp. 96–122.

[23] Jakub Breier and Jana Branišová. “A Dynamic Rule Creation Based Anomaly Detection Method for Identifying Security Breaches in Log Records”. In: *Wireless Personal Communications* 94.3 (2017), pp. 497–511. ISSN: 1572-834X. DOI: 10.1007/s11277-015-3128-1.

[24] Jakub Breier, Wei He, Shivam Bhasin, Dirmanto Jap, Samuel Chef, Hock Guan Ong, and Chee Lip Gan. “Extensive Laser Fault Injection Profiling of 65 nm FPGA”. In: *Journal of Hardware and Systems Security* 1.3 (Sept. 2017), pp. 237–251.

[25] Jakub Breier, Wei He, Dirmanto Jap, Shivam Bhasin, and Anupam Chattopadhyay. “Attacks in Reality: The Limits of Concurrent Error Detection Codes against Laser Fault Injection”. In: *Journal of Hardware and Systems Security* 1.4 (Dec. 2017), pp. 298–310.

[26] Jakub Breier, Dirmanto Jap, and Shivam Bhasin. “A Study on Analyzing Side-Channel Resistant Encoding Schemes With Respect to Fault Attacks”. In: *Journal of Cryptographic Engineering* 7.4 (Nov. 2017), pp. 311–320. ISSN: 2190-8516. DOI: 10.1007/s13389-017-0166-5.

[27] Jakub Breier. “Asset Valuation Method for Dependent Entities”. In: *Journal of Internet Services and Information Security* 4.3 (2014), pp. 72–81. ISSN: 2182-2077.

[28] Jakub Breier and Ladislav Hudec. “Security Mechanisms Role in Information Security Evaluation”. In: *Information Technology Applications* 1.2 (2012), pp. 5–15. ISSN: 1338-6468.

[29] Jakub Breier and Marcel Kleja. “On Practical Results of the Differential Power Analysis”. In: *Journal of Electrical Engineering* 63.2 (2012), pp. 125–129. ISSN: 1335-3632.

International peer-reviewed conferences/proceedings

[1] Timon Lumír Fillo, Ján Mikulec, Anubhab Baksi, Jakub Breier, and Xiaolu Hou. “Guess My Weight: Profiled Side-Channel Recovery of Floating-Point Neural-Network Weights”. In: *Security, Privacy and Applied Cryptographic Engineering (SPACE)*. Accepted; preprint available at arXiv:2610.04436. 2026.

[2] Zdenko Lehocký, Jakub Breier, Dirmanto Jap, Shivam Bhasin, and Xiaolu Hou. “Side-Channel Analysis of OpenVINO-based Neural Network Models”. In: *International Conference on Availability, Reliability and Security (ARES)*. IEEE. 2025.

[3] Aneesh Kandi, Anubhab Baksi, Peizhou Gan, Sylvain Guilley, Tomáš Gerlich, Jakub Breier, Anupam Chattopadhyay, Ritu Ranjan Shrivastwa, Zdeněk Martinásek, and Shivam Bhasin. “Side-Channel and Fault Resistant ASCON Implementation: A Detailed Hardware Evaluation”. In: *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. IEEE. 2024.

[4] Jan Schröder and Jakub Breier. “RMF: A Risk Measurement Framework for Machine Learning Models”. In: *International Conference on Availability, Reliability and Security (ARES)*. IEEE. 2024.

[5] Jakub Breier, Dirmanto Jap, Xiaolu Hou, and Shivam Bhasin. “A Desynchronization-Based Countermeasure Against Side-Channel Analysis of Neural Networks”. In: *International Symposium on Cyber Security, Cryptology, and Machine Learning*. Springer. 2023, pp. 296–306.

[6] Anubhab Baksi, Arghya Bhattacharjee, Jakub Breier, Takanori Isobe, and Mridul Nandi. “Big Brother is Watching You: A Closer Look at Backdoor Construction”. In: *Security, Privacy, and Applied Cryptography Engineering: 12th International Conference (SPACE’22)*. Jaipur, India: Springer, Dec. 2022, pp. 1–32.

[7] Anubhab Baksi, Shivam Bhasin, Jakub Breier, Anupam Chattopadhyay, and Vinay BY Kumar. “Feeding Three Birds With One Scone: A Generic Duplication Based Countermeasure To Fault Attacks”. In: *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE. 2021, pp. 561–564.

[8] Anubhab Baksi, Shivam Bhasin, Jakub Breier, Mustafa Khairallah, Thomas Peyrin, Sumanta Sarkar, and Siang Meng Sim. “DEFAULT: Cipher level resistance against differential fault attack”. In: *27th Annual International Conference on the Theory and Application of Cryptology and Information Security (Asiacrypt)*. Springer. 2021.

[9] Anubhab Baksi, Jakub Breier, Yi Chen, and Xiaoyang Dong. “Machine learning assisted differential distinguishers for lightweight ciphers”. In: *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE. 2021, pp. 176–181.

[10] Xiaolu Hou, Jakub Breier, and Shivam Bhasin. “DNFA: Differential no-fault analysis of bit permutation based ciphers assisted by side-channel”. In: *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE. 2021, pp. 182–187.

[11] Mustafa Khairallah, Xiaolu Hou, Zakaria Najm, Jakub Breier, Shivam Bhasin, and Thomas Peyrin. “SoK : On DFA Vulnerabilities of Substitution-Permutation Networks”. In: *2019 ACM SIGSAC Asia Conference on Computer & Communications Security (AsiaCCS)*. Auckland, New Zealand: ACM, 2019, pp. 403–414.

[12] Anubhab Baksi, Shivam Bhasin, Jakub Breier, Mustafa Khairallah, and Thomas Peyrin. “Protecting Block Ciphers against Differential Fault Attacks without Re-keying”. In: *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. Washington DC, USA, Apr. 2018, pp. 191–194.

[13] Jakub Breier, Xiaolu Hou, Dirmanto Jap, Lei Ma, Shivam Bhasin, and Yang Liu. “Practical Fault Attack on Deep Neural Networks”. In: *2018 ACM SIGSAC Conference on Computer & Communications Security (CCS)*. Toronto, Canada: ACM, Oct. 2018, pp. 2204–2206.

[14] Jakub Breier, Dirmanto Jap, and Shivam Bhasin. “SCADPA: Side-Channel Assisted Differential-Plaintext Attack on Bit Permutation Based Ciphers”. In: *2018 Design, Automation and Test in Europe (DATE)*. Dresden, Germany: IEEE, Mar. 2018, pp. 1129–1134.

[15] Samuel Chef, Chung Tah Chua, Jing Yun Tay, Yu Wen Siah, Shivam Bhasin, Jakub Breier, and Chee Lip Gan. “Descrambling of Embedded SRAM Using a Laser Probe”. In: *2018 IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*. Singapore: IEEE, June 2018, pp. 1–6.

[16] Mustafa Khairallah, Rajat Sadhukhan, Radhamanjari Samanta, Jakub Breier, Shivam Bhasin, Rajat Subhra Chakraborty, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. “DFARPA: Differential Fault Attack Resistant Physical Design Automation”. In: *2018 Design, Automation and Test in Europe (DATE)*. Dresden, Germany: IEEE, Mar. 2018, pp. 1171–1174.

[17] Prasanna Ravi, Shivam Bhasin, Jakub Breier, and Anupam Chattopadhyay. “PPAP and iPPAP: PLL-based Protection Against Physical Attacks”. In: *2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. Hong Kong SAR, China: IEEE, June 2018, pp. 620–625.

[18] Sayandeep Saha, Dirmanto Jap, Jakub Breier, Shivam Bhasin, Debdeep Mukhopadhyay, and Pallab Dasgupta. “Breaking Redundancy-Based Countermeasures with Random Faults and Power Side Channel”. In: *2018 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. Amsterdam, Netherlands: IEEE, Sept. 2018, pp. 1–8.

[19] Jakub Breier, Wei He, and Shivam Bhasin. “An Electromagnetic Fault Injection Sensor using Hogge Phase-Detector”. In: *Proceedings of the 18th International Symposium on Quality Electronic Design (ISQED 2017)*. Santa Clara, CA, USA: IEEE, Mar. 2017, pp. 307–312.

[20] Jakub Breier and Xiaolu Hou. “Feeding Two Cats with One Bowl: On Designing a Fault and Side-Channel Resistant Software Encoding Scheme”. In: *Topics in Cryptology – CT-RSA 2017: The Cryptographers’ Track at the RSA Conference 2017, San Francisco, CA, USA, February 14–17, 2017, Proceedings*. Ed. by Helena Handschuh. Cham: Springer International Publishing, Feb. 2017, pp. 77–94. ISBN: 978-3-319-52153-4. DOI: 10.1007/978-3-319-52153-4_5.

[21] Wei He, Jakub Breier, and Shivam Bhasin. “An FPGA-Compatible PLL-Based Sensor Against Fault Injection Attack”. In: *Proceedings of the 22nd Asia and South Pacific Design Automation Conference (ASP-DAC 2017)*. Tokyo, Japan, Jan. 2017, pp. 1–2.

[22] S V Dilip Kumar, Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, Shivam Bhasin, Anupam Chattopadhyay, and Anubhab Baksi. “A Practical Fault Attack on ARX-like Ciphers with a Case Study on ChaCha20”. In: *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. Taipei, Taiwan: IEEE, Dec. 2017, pp. 1–8.

[23] Sikhar Patranabis, Debdeep Mukhopadhyay, Jakub Breier, and Shivam Bhasin. “One Plus One is More than Two: A Practical Combination of Power and Fault Analysis Attacks on PRESENT and PRESENT-like Block Ciphers”. In: *2017 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. Taipei, Taiwan: IEEE, Dec. 2017, pp. 1–8.

[24] Jakub Breier. “On Analyzing Program Behavior under Fault Injection Attacks”. In: *2016 11th International Conference on Availability, Reliability and Security (ARES)*. Aug. 2016, pp. 474–479. DOI: 10.1109/ARES.2016.4.

[25] Jakub Breier and Chien-Ning Chen. “On Determining Optimal Parameters for Testing Devices Against Laser Fault Attacks”. In: *Proceedings of The 15th International Symposium on Integrated Circuits (ISIC)*. Singapore: IEEE, Dec. 2016, pp. 1–4.

[26] Jakub Breier, Dirmanto Jap, and Shivam Bhasin. “The Other Side of The Coin: Analyzing Software Encoding Schemes Against Fault Injection Attacks”. In: *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. McLean, VA, USA, May 2016, pp. 209–216. DOI: 10.1109/HST.2016.7495584.

[27] Wei He, Jakub Breier, and Shivam Bhasin. “Cheap and Cheerful: A Low-Cost Digital Sensor for Detecting Laser Fault Injection Attacks”. In: *Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings*. Ed. by Claude Carlet, M. Anwar Hasan, and Vishal Saraswat. Cham: Springer International Publishing, Dec. 2016, pp. 27–46. ISBN: 978-3-319-49445-6. DOI: 10.1007/978-3-319-49445-6_2.

[28] Wei He, Jakub Breier, Shivam Bhasin, and Anupam Chattopadhyay. “Bypassing Parity Protected Cryptography Using Laser Fault Injection in Cyber-Physical System”. In: *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security*. CPSS ’16. Xi’an, China: ACM, May 2016, pp. 15–21. ISBN: 978-1-4503-4288-9. DOI: 10.1145/2899015.2899019.

[29] Wei He, Jakub Breier, Shivam Bhasin, Dirmanto Jap, Hock Guan Ong, and Chee Lip Gan. “Comprehensive Laser Sensitivity Profiling and Data Register Bit-Flips for Cryptographic Fault Attacks in 65 Nm FPGA”. In: *Security, Privacy, and Applied Cryptography Engineering: 6th International Conference, SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings*. Ed. by Claude Carlet, M. Anwar Hasan, and Vishal Saraswat. Cham: Springer International Publishing, Dec. 2016, pp. 47–65. ISBN: 978-3-319-49445-6. DOI: 10.1007/978-3-319-49445-6_3.

[30] Wei He, Jakub Breier, Shivam Bhasin, Noriyuki Miura, and Makoto Nagata. “Ring Oscillator under Laser: Potential of PLL-based Countermeasure against Laser Fault Injection”. In: *2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*. Aug. 2016, pp. 102–113. DOI: 10.1109/FDTC.2016.13.

[31] Jakub Breier and Jana Branišová. “Anomaly Detection from Log Files Using Data Mining Techniques”. In: *Information Science and Applications (ICISA), 2015 Sixth International Conference on*. Pattaya, Thailand: Springer, Feb. 2015, pp. 449–457.

[32] Jakub Breier and Wei He. “Multiple Fault Attack on PRESENT with a Hardware Trojan Implementation in FPGA”. In: *Proceedings of the 2015 Workshop on Secure Internet of Things (SIoT)*. Ed. by Linawati, MadeSudiana Mahendra, ErichJ. Neuhold, AMin Tjoa, and Ilsun You. Conference Publishing Services. Vienna, Austria: IEEE, Sept. 2015, pp. 58–64.

[33] Jakub Breier and Dirmanto Jap. “Testing Feasibility of Back-Side Laser Fault Injection on a Microcontroller”. In: *Proceedings of the WESS’15: Workshop on Embedded Systems Security*. WESS’15. Amsterdam, Netherlands: ACM, Sept. 2015, 5:1–5:6. ISBN: 978-1-4503-3667-3. DOI: 10.1145/2818362.2818367.

[34] Jakub Breier, Dirmanto Jap, and Chien-Ning Chen. “Laser Profiling for the Back-Side Fault Attacks (With a Practical Laser Clock Glitch Attack on AES)”. In: *First Cyber-Physical System Security Workshop (CPSS 2015)*. Singapore: ACM, Apr. 2015, pp. 99–103.

[35] Dirmanto Jap and Jakub Breier. “Differential Fault Attack on LEA”. In: *Information and Communication Technology: Third IFIP TC 5/8 International Conference, ICT-EurAsia 2015, and 9th IFIP WG 8.9 Working Conference, CONFENIS 2015, Held as Part of WCC 2015*. Ed. by Linawati, Made Sudiana Mahendra, Erich J. Neuhold, A Min Tjoa, and Ilsun You. Lecture Notes in Computer Science. Daejeon, Korea: Springer Berlin Heidelberg, Oct. 2015, pp. 265–274.

[36] Jakub Breier and Dirmanto Jap. “A Survey of the State-of-the-Art Fault Attacks”. In: *Proceedings of The 14th International Symposium on Integrated Circuits (ISIC)*. Singapore: IEEE, Dec. 2014, pp. 152–155.

[37] Jakub Breier and Adam Pomothy. “Qualified Electronic Signature via SIM Card Using JavaCard 3 Connected Edition Platform”. In: *Availability, Reliability and Security (ARES), 2014 Ninth International Conference on*. Fribourg, Switzerland: IEEE, Sept. 2014, pp. 349–355. DOI: 10.1109/ARES.2014.53.

[38] Jakub Breier and Frank Schindler. “Assets Dependencies Model in Information Security Risk Management”. In: *Proceedings of the 2014 International Conference on Information and Communication Technology*. Ed. by Linawati, MadeSudiana Mahendra, ErichJ. Neuhold, AMin Tjoa, and Ilsun You. Vol. 8407. Lecture Notes in Computer Science. Bali, Indonesia: Springer Berlin Heidelberg, 2014, pp. 405–412. ISBN: 978-3-642-55031-7. DOI: 10.1007/978-3-642-55032-4_40.

[39] Dirmanto Jap and Jakub Breier. “Comparison of Machine-Learning Based Side-Channel Analysis Methods”. In: *Proceedings of The 14th International Symposium on Integrated Circuits (ISIC)*. Singapore: IEEE, Dec. 2014, pp. 38–41.

[40] Jakub Breier and Ladislav Hudec. “On Identifying Proper Security Mechanisms”. In: *Proceedings of the 2013 International Conference on Information and Communication Technology*. ICT-EurAsia’13. Yogyakarta, Indonesia: Springer-Verlag, 2013, pp. 285–294. ISBN: 978-3-642-36817-2. DOI: 10.1007/978-3-642-36818-9_29.

[41] Jakub Breier and Ladislav Hudec. “On Selecting Critical Security Controls”. In: *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*. Regensburg, Germany: IEEE, Sept. 2013, pp. 582–588. DOI: 10.1109/ARES.2013.77.

[42] Jakub Breier and Ladislav Hudec. “New Approach in Information System Security Evaluation”. In: *Satellite Telecommunications (ESTEL), 2012 IEEE First AESS European Conference on*. Rome, Italy: IEEE, Oct. 2012, pp. 1–6. DOI: 10.1109/ESTEL.2012.6400145.

[43] Jakub Breier and Ladislav Hudec. “Towards a Security Evaluation Model Based on Security Metrics”. In: *Proceedings of the 13th International Conference on Computer Systems and Technologies*. CompSysTech ’12. Ruse, Bulgaria: ACM, 2012, pp. 87–94. ISBN: 978-1-4503-1193-9. DOI: 10.1145/2383276.2383291.

[44] Jakub Breier and Ladislav Hudec. “Risk Analysis Supported by Information Security Metrics”. In: *Proceedings of the 12th International Conference on Computer Systems and Technologies*. CompSysTech ’11. Vienna, Austria: ACM, 2011, pp. 393–398. ISBN: 978-1-4503-0917-2. DOI: 10.1145/2023607.2023673.