Vahid Jahandideh

Post-quantum cryptography | Side-channel security

Arnhem, The Netherlands | +31 6 43 69 88 27 | vahid-jahandideh.github.io
v.jahandideh@cs.ru.nl | v.jahandideh@gmail.com

Research profile

Postdoctoral researcher at Radboud University specialising in post-quantum implementation security, side-channel analysis and masking. Research spans Kyber/ML-KEM and HQC, combining power-trace experiments with algebraic and probabilistic methods. Experienced in embedded implementations, Python/C/C++, and RF/DSP.

Research and professional experience

Postdoctoral Researcher Mar 2026 - Present
Digital Security Group / CESCALAB, Radboud University, Nijmegen

- Study attacks and countermeasures for Kyber/ML-KEM and HQC with Prof. Lejla Batina.
- Co-developed a belief-propagation attack recovering the long-term key of first-order masked Kyber768 on Cortex-M4 from about 2,200 decapsulation power traces, without lattice reduction.
- Analysed single-trace leakage in ML-KEM key generation and designed a sampler countermeasure based on random representatives modulo q; work published at ACTIVE 2026.

Doctoral Researcher Mar 2022 - Mar 2026
Digital Security Group, Radboud University, Nijmegen

- Developed algebraic and probabilistic methods for random probing security, noisy leakage and composition, including exact and importance-sampling evaluation in the LAPSE tool.
- Designed and analysed deterministic masking constructions and masked Ascon/AES implementations; combined security analysis with ChipWhisperer measurements and leakage evaluation.

Researcher & Software Developer 2012 - 2021
Saba Ertebat Company, Tehran, Iran

- Led a GNU Radio-based RF signal analysis platform for public-standard identification and flexible DSP pipelines; reverse-engineered proprietary RF protocols for a lawful regulator.
- Performed cellular-security analyses and demonstrations across 2G/3G/4G; designed and delivered training in blind signal identification, demodulation and decoding.
- Contributed to LTE eNodeB / 5G gNodeB development and audio-processing pipelines, including vocoder analysis and low-rate vocoder design.

Researcher 2011 - 2019
Electronics Research Center, Sharif University of Technology, Tehran

- Studied and implemented leakage-resilient cryptographic primitives in the Side-Channel Laboratory; contributed to the national secure-communications roadmap.

Technical expertise

Implementation security: Power analysis, profiled neural-network leakage models, belief propagation, TVLA/t-tests, SNR, ChipWhisperer; Kyber/ML-KEM, HQC, masked Ascon/AES.
Security analysis: Random probing, noisy leakage, deterministic and higher-order masking, composition, algebraic methods, Monte Carlo and importance sampling.
Software and platforms: Python (NumPy, SciPy, PyTorch), C/C++, MATLAB, Git, ARM Cortex-M4/STM32.
RF/DSP: GNU Radio, software-defined radio, signal classification, blind demodulation and decoding.

Education

PhD in Digital Security, Radboud University 2022 - 2026
Successfully defended 4 November 2026. Supervisors: Prof. Lejla Batina and Prof. Bart Mennink.
Thesis: *Evaluating and Engineering Masking Security: Random Probing Tools and Deterministic Gadgets*.

Doctoral studies in Communication Theory, Sharif University of Technology 2012 - 2015
Programme not completed; coursework GPA: 18.2/20. Supervisor: Dr. Mahmoud Salmasizadeh.

MSc in Electrical Engineering, Sharif University of Technology 2008 - 2010
Coding and Secure Communication; GPA: 17.7/20. Supervisor: Dr. Mahmoud Salmasizadeh.

BSc in Electrical Engineering, University of Tabriz 2004 - 2008

Publications and preprints

Post-quantum implementation security

[1] **Breaking First-Order Masked Kyber with Belief Propagation Alone**
V. Jahandideh, L. Batina. ePrint 2026/2448. *Under review for CHES 2027; major revision addressed.*

[2] **Too Small to Hide: Single-Trace Key Recovery from ML-KEM Key Generation**
V. Jahandideh. *ACTIVE 2026*. doi:10.1145/3847162.3849237; ePrint 2026/2137.

Masking, probing security and leakage analysis

[3] **Leakage-Diagrams, Importance Sampling, and Composition in the Random Probing Model**
V. Jahandideh, B. Mennink, L. Batina. ePrint 2026/444. *Accepted for CHES 2027.*

[4] **A Decomposition Approach for Evaluating Security of Masking**
V. Jahandideh, B. Mennink, L. Batina. *ASIACRYPT 2025*, pp. 580–612.

[5] **Probing Secure Composability Without Fresh Randomness: Theory and Application to Ascon**
V. Jahandideh, B. Mennink, L. Batina. *IACR TCHES*, 2025.

[6] **Clustering Approach for Higher-Order Deterministic Masking**
V. Jahandideh, J. Schoone, L. Batina. Cryptology ePrint 2025/273, 2025. *Preprint.*

[7] **An Algebraic Approach for Evaluating Random Probing Security With Application to AES**
V. Jahandideh, B. Mennink, L. Batina. *IACR TCHES*, 2024.

[8] **A New Leakage Exploitation Framework and Its Application to Authenticated Encryption**
V. Jahandideh, L. Weissbart, B. Mennink, L. Batina. *NIST Lightweight Cryptography Workshop*, 2023.

[9] **Verification of the Security in Boolean Masked Circuits**
V. Jahandideh. Cryptology ePrint 2021/860, 2021. *Preprint.*

[10] **Concrete Evaluation of the Random Probing Security**
V. Jahandideh. Cryptology ePrint 2021/859, 2021. *Preprint.*

Earlier work in secure communications and cryptanalysis

[11] **Deterministic Multiple-Access Wiretap Channel**
V. Jahandideh, S. Salimi, M. Salmasizadeh. *IEEE ICITIS*, 2010.

[12] **Secrecy Capacity of Wiretap Channel for a New Scenario and Designing Code for Wiretap Channel**
V. Jahandideh, S. Salimi, M. Salmasizadeh. *18th ICEE*, 2010.

[13] **Cryptanalysis and Security Enhancement on the Generation of Mu-Varadharajan Electronic Voting Protocol**
V. Jahandideh, A. S. Mortazavi, Y. Baseri, J. Mohajeri. Cryptology ePrint 2009/425, 2009. *Preprint.*

Teaching

Teaching Assistant, Computer Security, Radboud University 2022 - 2025
Lecturer, Advanced Topics in Cryptography, Sharif University of Technology 2014 - 2018
Teaching Assistant, Mathematics of Cryptography, Sharif University of Technology 2012 - 2014

Referees

Prof. Lejla Batina, PhD supervisor lejla@cs.ru.nl
Prof. Bart Mennink, PhD supervisor bart.mennink@maastrichtuniversity.nl
Prof. Joan Daemen, Radboud University joan@cs.ru.nl