Vahid Jahandideh

Kroonpark 446, 6831 GV Arnhem, The Netherlands +31 6 43 69 88 27
v.jahandideh@cs.ru.nl | v.jahandideh@gmail.com | vahid-jahandideh.github.io

Professional Summary

Ph.D. candidate in Digital Security (Radboud University) specialising in side-channel cryptography, deterministic masking, and random-probing security. Hands-on with masked implementations (Ascon, AES), ChipWhisperer measurements, and algebraic/empirical leakage evaluation. Strong background in RF/DSP and software-defined radio (GNU Radio), with extensive Python/C/C++ tooling and teaching experience.

Skills

Side-channel	Leakage modelling, TVLA/t-tests, SNR; masked Ascon/AES; ChipWhisperer
Cryptography	Probing model, deterministic masking, algebraic security analysis
Programming	Python (NumPy, SciPy, PyTorch), C/C++, MATLAB, GNU Radio, Git, ARM/STM32
RF/DSP	SDR pipelines, signal classification, blind demodulation/decoding

Education

Ph.D. Candidate in Digital Security 2022 – Present
Radboud University, Nijmegen, The Netherlands

- Expected completion: February 2026. Supervisors: Prof. Lejla Batina, Prof. Bart Mennink.
- Focus: probing security, deterministic masking, composability; masked Ascon/AES implementations.

Ph.D. Candidate in Communication Theory (programme not completed) 2012 – 2015
Sharif University of Technology, Tehran, Iran

- Coursework GPA: 18.2/20. Supervisor: Dr. Mahmoud Salmasizadeh.

M.Sc. in Electrical Engineering 2008 – 2010
Sharif University of Technology, Tehran, Iran

- Specialisation: Coding and Secure Communication. GPA: 17.7/20. Supervisor: Dr. Mahmoud Salmasizadeh.

B.Sc. in Electrical Engineering 2004 – 2008
University of Tabriz, Tabriz, Iran

- Specialisation: Communication Theory.

Experience

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

- Led an SDR-based RF signal analysis platform (GNU Radio), supporting identification of public RF standards and flexible DSP pipelines.
- Performed GSM security analyses with live demonstrations for 2G/3G/4G, highlighting vulnerabilities and risks.
- Reverse-engineered proprietary RF protocols for a lawful regulator; designed and delivered "Blind Signal Identification Techniques" (algebraic and estimation-theoretic methods for blind demodulation/decoding).
- Contributed to base-station development (LTE eNodeB / 5G gNodeB).
- Built audio processing pipelines, including vocoder analysis and a low-rate vocoder design.

Researcher 2011 – 2019
Electronics Research Center, Sharif University of Technology

- Studied and implemented leakage-resilient cryptographic primitives; member of the Side-Channel Laboratory.
- Contributed to the national secure-communications roadmap.
- Lecturer for "Advanced Topics in Cryptography" (five years).

Teaching

Teaching Assistant 2022 – 2025
Radboud University, Digital Security Group

- Computer Security.

Lecturer 2014 – 2018
Sharif University of Technology, Dept. of Electrical Engineering

- Advanced Topics in Cryptography.

Teaching Assistant 2012 – 2014
Sharif University of Technology, Dept. of Electrical Engineering

- Mathematics of Cryptography.

Selected Publications

- Probing Secure Composability Without Fresh Randomness: Theory and Application to Ascon, V. Jahandideh, B. Mennink, L. Batina, *IACR Transactions on Cryptographic Hardware and Embedded Systems* (TCHES), 2025.
- An Algebraic Approach for Evaluating Random Probing Security with Application to AES, V. Jahandideh, B. Mennink, L. Batina, *IACR TCHES*, 2024.
- A New Leakage Exploitation Framework and Its Application to Authenticated Encryption, V. Jahandideh, L. Weissbart, B. Mennink, L. Batina, *NIST Lightweight Cryptography Workshop*, 2023.
- Verification of the Security in Boolean Masked Circuits, V. Jahandideh, *IACR ePrint* 2021/860, 2021.
- Concrete Evaluation of the Random Probing Security, V. Jahandideh, *IACR ePrint* 2021/859, 2021.
- Deterministic Multiple-Access Wiretap Channel, V. Jahandideh, S. Salimi, M. Salmasizadeh, *IEEE ICITIS*, 2010.
- Secrecy Capacity of Wiretap Channel for a New Scenario and Designing Code for Wiretap Channel, V. Jahandideh, S. Salimi, M. Salmasizadeh, *18th ICEE*, 2010.
- Cryptanalysis and Security Enhancement on the Generation of Mu-Varadharajan Electronic Voting Protocol, V. Jahandideh, A.S. Mortazavi, Y. Baseri, J. Mohajeri, *IACR ePrint* 2009/425, 2009.

Referees

- Prof. Lejla Batina lejla@cs.ru.nl— Ph.D. supervisor.
- Prof. Bart Mennink bart.mennink@maastrichtuniversity.nl— Ph.D. supervisor.
- Prof. Joan Daemen joan@cs.ru.nl— Head of Digital Security Group, Radboud University (Ph.D. host group).