Hossein Hadipour

Curriculum Vitae

Education

2025–Present **Postdoc in Computer Science**, *Ruhr Univeristy Bochum*, Bochum, Germany.

2021–2024 **Ph.D. in Computer Science**, *Graz Univeristy of Technology*, Graz, Austria.

- Thesis: Automated Methods in Design and Analysis of Symmetric-Key Primitives
- Supervisors: Dr. Maria Eichlseder

2014–2016 **Master of Pure Mathematics**, *University of Tehran*, Tehran, Iran.

- Thesis: Topics in Algebraic Attacks on Cryptosystems
- Supervisors: Dr. Hosein Sabzrou

2012–2016 **Bachelor of Electrical Engineering**, *K. N. Toosi University of Technology*, Tehran, Iran.

- Project 1: Evaluation of Algebraic Attacks on Cryptosystems
- Project 2: Implementation of RFID Access Control System via AVR Microcontrollers
- Supervisors: Dr. Bahareh Akhbari

2010–2014 **Bachelor of Applied Mathematics**, *K. N. Toosi University of Technology*, Tehran, Iran.

- Supervisor: Professor. A. Reza Moghaddamfar

Research and Publications

- **Hosein Hadipour**, Patrick Derbez, and Maria Eichlseder. "Revisiting Differential-Linear Attacks via a Boomerang Perspective with Application to AES, Ascon, CLEFIA, SKINNY, PRESENT, KNOT, TWINE, WARP, LBlock, Simeck, and SERPENT". in: *Advances in Cryptology - CRYPTO 2024*. LNCS (2024). URL: https://ia.cr/2024/255
- Debasmita Chakraborty, **Hosein Hadipour**, Phuong Hoa Nguyen, and Maria Eichlseder. "Finding Complete Impossible Differential Attacks on AndRX Ciphers and Efficient Distinguishers for ARX Designs". In: *IACR Trans. Symmetric Cryptol.* 2024.3 (2024), pp. 84–176. DOI: 10.46586/TOSC.V2024.I3.84-176
- **Hosein Hadipour**, Sadegh Sadeghi, and Maria Eichlseder. "Finding the Impossible: Automated Search for Full Impossible-Differential, Zero-Correlation, and Integral Attacks". In: *Advances in Cryptology - EUROCRYPT 2023*. Ed. by Carmit Hazay and Martijn Stam. Vol. 14007. LNCS. Springer, 2023, pp. 128–157. DOI: 10.1007/978-3-031-30634-1_5

- **Hosein Hadipour** and Yosuke Todo. "Cryptanalysis of QARMAv2". In: *IACR Trans. Symmetric Cryptol.* 2024.1 (2024), pp. 188–213. DOI: 10.46586/TOSC.V2024.I1.188-213
- **Hosein Hadipour**, Simon Gerhalter, Sadegh Sadeghi, and Maria Eichlseder. "Improved Search for Integral, Impossible Differential and Zero-Correlation Attacks Application to Ascon, ForkSKINNY, SKINNY, MANTIS, PRESENT and QARMAv2". In: *IACR Trans. Symmetric Cryptol.* 2024.1 (2024), pp. 234–325. DOI: 10.46586/TOSC.V2024.I1.234-325
- Hosein Hadipour, Marcel Nageler, and Maria Eichlseder. "Throwing Boomerangs into Feistel Structures: Application to CLEFIA, WARP, LBlock, LBlock-s and TWINE". in: *IACR Trans. Symmetric Cryptol.* 2022.3 (2022), pp. 271–302. DOI: 10.46586/tosc.v2022.i3.271-302
- **Hosein Hadipour** and Maria Eichlseder. "Integral Cryptanalysis of WARP based on Monomial Prediction". In: *IACR Trans. Symmetric Cryptol.* 2022.2 (2022), pp. 92–112. DOI: 10.46586/tosc.v2022.i2.92-112
- **Hosein Hadipour** and Maria Eichlseder. "Autoguess: A Tool for Finding Guess-and-Determine Attacks and Key Bridges". In: *ACNS*. vol. 13269. LNCS. Springer, 2022, pp. 230–250. DOI: 10.1007/978-3-031-09234-3_12
- Hadi Soleimany, Nasour Bagheri, **Hosein Hadipour**, Prasanna Ravi, Shivam Bhasin, and Sara Mansouri. "Practical Multiple Persistent Faults Analysis". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.1 (2022), pp. 367–390. DOI: 10.46586/tches.v2022.i1.367-390
- **Hosein Hadipour** and Nasour Bagheri. "Improved Rectangle Attacks on SKINNY and CRAFT". in: *IACR Trans. Symmetric Cryptol.* 2021.2 (2021), pp. 140–198. DOI: 10.46586/tosc.v2021.i2.140-198
- **Hosein Hadipour**, Sadegh Sadeghi, Majid M. Niknam, and Nasour Bagheri. "Comprehensive security analysis of CRAFT". in: *IACR Trans. Symmetric Cryptol.* 2019.4 (2019), pp. 290–317. DOI: 10.13154/tosc.v2019.i4.290-317

Presentations and Visits

- **Inria - Paris, France, May 2024**: Visiting Professor Maria Naya-Plasencia's Lab
- **IRISA - Rennes, France, May 2024**: Visiting IRISA Lab
- **LORIA - Nancy, France, May 2024**: Visiting LORIA Lab
- **Lorentz Center - Leiden, Netherlands, April 2024**: Invited attendee
- **FSE 2024 - Leuven, Belgium**: Paper presentation
- **FSE 2024 - Leuven, Belgium**: Paper presentation
- **University of Hyogo, Kobe, Japan**: Visiting Professor Takanori Isobe's Lab
- **EUROCRYPT 2023 - Lyon, France**: Paper presentation
- **FSE 2023 - Kobe, Japan**: Paper presentation
- **FSE 2023 - Kobe, Japan**: Paper presentation
- **ACNS 2022 - Rome, Italy**: Paper presentation
- **FRISIACRYPT 2022 - Netherlands**: Invited attendee
- **CHES 2022 - Louven, Belgium**: Paper presnetation
- **FSE 2022 - Atehns, Greece**: Paper presentation

Reviews

- Subreviewer for CRYPTO 2025
- Subreviewer for Selected Area in Cryptography (SAC) 2025
- Subreviewer for ASIACRYPT 2024

- Subreviewer for EUROCRYPT 2024
- Subreviewer for EUROCRYPT 2023
- Subreviewer for ASIACRYPT 2023
- Subreviewer for EUROCRYPT 2023
- Subreviewer for CRYPTO 2022
- Subreviewer for ASICRYPT 2022
- Reviewer for IET Information Security 2022
- Reviewer for Designs, Codes and Cryptography (DCC) 2022

Honors

- **Bronze medal**, 38th National Mathematical Competition for University Students, Kerman, May 2014. http://www.ims.ir
- **Bronze medal**, 37th National Mathematical Competition for University Students, Semnan, May 2013. http://www.ims.ir
- **Among the winners of NSUCRYPTO-2019** (October 13-21, 2019). https://nsucrypto.nsu.ru/archive/2019/total_results/round/1/section/2/#data

Computer Skills

Programming Language

Advanced	Python, C, C++, VHDL
Intermediate	Java, Assembly(AVR)

Software, Tools & Packages

Math	SageMath, Matlab, Maple, CoCoA
SAT	PySAT, Cadical, Minisat, CryptoMinisat
SMT	PySMT, Z3, STP
MILP	Pulp, Gurobi
CP	Minizinc
Office	LaTeX, Microsoft Office Tools, Texstudio
OS	Linux, Windows
IDE	Visual Studio Code, Microsoft Visual Studio, Eclipse
Electrical Engineering Softwares	Xilinx ISE, Altium Designer, PSpice, CodeVision, Atmelstudio, Arduino, Proteus

Experience

2024–Present **Postdoctoral Researcher**, Ruhr University Bochum.
Working on symmetric-key cryptanalysis under the supervision of Dr. Maria Eichlseder https://informatik.rub.de/symcrypt/

2022–2024 **Ph.D. Candidate**, Graz Univeristy of Technology.
Working on symmetric-key cryptanalysis under the supervision of Dr. Maria Eichlseder https://www.isec.tugraz.at/people/?groupby=alumni

2021–2022 **Ph.D. Student**, Graz Univeristy of Technology.
Working on symmetric-key cryptanalysis under the supervision of Dr. Maria Eichlseder
https://www.iaik.tugraz.at/research-area/crypto/

Teaching Experience

Cryptanalysis.
Guest Lecturer, Graz University of Technology, Summer 2023 and 2024

A Course in Cryptography.
Teaching Assistant, University of Tehran, Fall 2016

Introduction to Cryptography.
Teaching Assistant, K. N. Toosi University, Fall 2014

Research Interests

- Design and Cryptanalysis of Symmetric and Asymmetric Primitives
- Tools for Cryptanalysis
- Side Channel and Fault Aanalyses
- Cryptographic Protocols
- Efficient and Secure Implementations of Cryptographic Primitives

Attended Seminars/Conferences/Workshops

FSE 2023 **Fast Software Encryption (FSE) 2025**, Italy, Rome, March 17-21, 2025. (As an attendee)

SKCAM 2025 **SKCAM 2025**, Italy, Rome, March 2025. (As an invited speaker)

Lorentz Center 2024 **Beating Real-Time Crypto: Solutions and Analysis**, Leiden, Netherlands, April 22-26, 2024. (As an invited attendee and speaker)

FSE 2024 **Fast Software Encryption (FSE) 2024**, Leuven, Belgium, March 25-29, 2024. (As a speaker)

EUROCRYPT 2023 **EUROCRYPT 2023**, Lyon, France, April 23-27, 2023. (As a speaker)

FSE 2023 **Fast Software Encryption (FSE) 2023**, Kobe, Japan, March 20-24, 2023. (As a speaker)

ACNS 2022 **Applied Cryptography and Network Security 2022**, Rome, Italy, June 20-23, 2022. (As a speaker)

FRISIACRYPT 2022 **FRISIACRYPT 2022**, Terschelling, Netherlands, September 25-28, 2022. (As an invited attendee)

CHES 2022 **Cryptographic Hardware and Embedded Systems 2022**, Leuven, Belgium, September 18-21, 2022. (As a speaker)

FSE 2022 **Fast Software Encryption (FSE) 2022**, Athens, Greece, March 20-25, 2022. (As a speaker)

Symmetric Cryptography in Theory and Practice	ISC Winter School on Information Security and Cryptology (ISCwsISC 2020), Iran University of Sciences and Technology, International Academy, February 2-3, 2020. (As a speaker)
ISCISC 19	16^{th} International ISC Conference on Information Security and Cryptology (ISCISC'19) , Ferdowsi University of Mashhad, Mashhad, Iran, August 28-29, 2019
Multi-core Systems and Parallel Platforms	9^{th} IPM-HPC Workshop on Multi-core Systems and Graphic Processors,institute for research in fundamental sciences (IPM), Tehran, Iran, June 8-9, 2019.
Multi-core Systems and Parallel Platforms	8^{th} IPM-HPC Workshop on Multi-core System and Parallel Platforms, multi-core and multi-node CPU programming, institute for research in fundamental sciences (IPM), Tehran, Iran, February 20-21, 2019.
Selected Area in Post-quantum Cryptography	Sharif University of Technology, Tehran, Iran, February 13-14, 2019.
Advanced Matlab Workshop	IEEE Student Branch of Faculty of Electrical Engineering of K.N. Toosi University of Technology, Tehran, Iran, fall 2014.

Languages

Persian	**Mother tongue**
English	**Advanced**
German	**Learning**

Other Information

Memberships

2021-Present	International Association for Cryptologic Research
2012-2013	Iranian Mathematical Society

Interests

- Swimming
- Football
- Mountain climbing
- Biking
- Traveling
- Internet Surfing

Personal Details

Permanent Address	Sperchtsweg 20/2, Bochum 44801, Austria
Languages	Persian, English
Mobile No.	+43 67764289931

Email id	hsn.hadipour@gmail.com
GitHub	https://github.com/hadipourh
Google Scholar	https://scholar.google.com/citations?user=3gNyYaAAAAAJ&hl=en
DBLP	https://dblp.org/pid/244/8979.html
IACR Profile	https://www.iacr.org/cryptodb/data/author.php?authorkey=11275

Declaration

I hereby declare that the above mentioned information is correct up to my knowledge and I bear the responsibility for the correctness of the above mentioned particular.

Date: April 15, 2025

Place: Bochum, Germany

Hossein Hadipour