

Alireza Rohani

RESEARCH SCIENTIST · SECURITY EXPERT

☎ (+65) 84-2364-18 | ✉ alireza.rohani1@gmail.com | 🇳🇱 Nationality: Dutch

Summary

Current security researcher in Physical Analysis and Cryptographic Engineering Lab. in Singapore. Experience in different aspects of security and fault-tolerance including side-channel attack, security assessment, hardware secure design and digital design. I enjoy understanding and working with cryptographic algorithms, as well as deploying them on real world devices.

Education

University of Twente

PHD. IN COMPUTER SCIENCE

- Computer Architecture for Embedded Systems Group (CAES)
- Thesis: Error-Mitigation Techniques in Modern CMOS Processors
- supervisor: Dr. Hans G. Kerkhoff, Prof. Gerard J. M. Smit

Enschede, The Netherlands

Jun. 2010 - Dec. 2014

Amirkabir University of Technology

M.SC. IN COMPUTER ARCHITECTURE

- Thesis: Fault Tolerance FPGA Design
- GPA: 3.6/4

Tehran, Iran

Sep. 2007 - Jan. 2010

Amirkabir University of Technology

B.SC. IN COMPUTER SCIENCE

- GPA: 3.2/4

Tehran, Iran

Sep. 2001 - Jan. 2006

Work Experience

Physical Analysis and Cryptographic Engineering Lab.

RESEARCH SCIENTIST

- Deployed modern cryptographic algorithms on hardware (FPGAs)
- Evaluated the security of cryptographic algorithms against side-channel attack
- Developed advanced side-channel attacks based on machine-learning
- Developed secure designs to resist side-channel attacks in hardware and software

Singapore

Oct. 2016 - PRESENT

University of Twente

POSTDOC.

- Developed a mathematical model to correlate fault-tolerance and heat-generation in 45nm processors
- Delivered lectures for graduate and undergraduate courses in computer science in CAES group
- Supervised one PhD student towards finishing his doctorate thesis
- Leader of a team of four graduate students to finish their final project of SoC design

Enschede, The Netherlands

Jan. 2015 - Oct. 2016

University of Twente

PHD CANDIDATE

- Developed a software tool to automate reliability assessment of digital circuits
- Developed a design to increase resilience of DSP processors against radiation-induced faults
- Published more than 10 technical articles in international journals and conferences, to see the complete list, see the appendices

Enschede, The Netherlands

Jun. 2010 - Dec. 2014

IroC Technologies

INTERN

- Conducted evaluation test to evaluate the sensitivity of network card against single-bit faults
- Developed a reliability evaluation platform to automate fault injection & evaluation on hardware

Grenoble, France

Feb. 2012, May. 2012

Recore Systems

INTERN

- Worked on the design file of a modern DSP processor used in space applications.
- Developed a reliable design for the DSP processor which was used by European Space Agency

Enschede, The Netherlands

Jan. 2011, May. 2011

Skills

Programming	Python, Matlab, Assembly, VHDL, Verilog, LaTeX
Hardware Design	ModelSim, ISE Xilinx, Synopsis
Web	HTML5, CSS, Wordpress.org
Languages	English (fluent), Dutch (intermediate), Persian (native), Spanish (basics)

Presentation (selective)

VLSI Test Symposium

SPEAKER

- Technical Presentation about new issues in testing of digital systems

Las Vegas, United States

April. 2016

TEDxUTwente, Breaking Barriers

SPEAKER

- Non-technical presentation about how to manage PhD life

Enschede, The Netherlands

April. 2016

European Test Symposium

PRESENTER

- Technical presentation about the design of our secure processor

Paderborn, Germany

Jul. 2014

Recore Systems

PRESENTER

- Technical presentation to convince the managerial team to invest on security mechanisms

Enschede, The Netherlands

Jan. 2013

Toastmaster Club

SPEAKER

- Non-technical presentation (twice a month) mostly to practice impromptu speaking and storytelling

Singapore - The Netherlands

Dec. 2015 - Present

Program Committees (selective)

2015-PRESENT **Reviewer**, Transaction on Reconfigurable Technology and Systems

Journal Paper

2014-PRESENT **Reviewer**, Elsevier Journal of Microelectronics reliability

Journal Paper

2014-PRESENT **Reviewer**, IEEE transaction on Circuits and Systems

Journal Paper

2014-PRESENT **Reviewer**, Elsevier Journal of Microelectronics reliability

Journal Paper

2012 **Session Chair**, 2012 IEEE Design for Test Symposium

Austin, United States

Extracurricular Activity

Toastmaster Club

PUBLIC SPEAKER

- Speaking two times per month to practice impromptu speaking and storytelling

Singapore - Netherlands

Dec. 2015 - PRESENT

TEDxUtwente & TEDxSaxion

MEMBER

- Spoke in TEDxUtwente about "The hidden danger of achieving your one big goal"
- Member of the curating team to find speakers for our TEDx salon (5000+ participants)

Enschede, The Netherlands

Dec. 2015 - Oct. 2016

Blogger

WRITER

- Writing mostly about life hacks that knowledge workers need to know in order to thrive in their professional life

www.alirezarohani.net

Jan. 2016 - PRESENT

D.R.V. Hippocampus & Vleugellam

SPORTS

- Member of the horse riding club and gliding association in Enschede

Enschede, The Netherlands

Dec. 2014 - Oct. 2016

APPENDICES

- [1] Hassan Ebrahimi, **Alireza Rohani**, and Hans G. Kerkhoff. Detecting intermittent resistive faults in digital CMOS circuits. In *2016 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, DFT 2016, Storrs, CT, USA, September 19-20, 2016*, pages 87–90, 2016.
- [2] **Alireza Rohani**, Hassan Ebrahimi, and Hans G. Kerkhoff. A software framework to calculate local temperatures in CMOS processors. In *26th International Workshop on Power and Timing Modeling, Optimization and Simulation, PATMOS 2016, Bremen, Germany, September 21-23, 2016*, pages 183–188, 2016.
- [3] J. Alt, Paolo Bernardi, Alberto Bosio, Riccardo Cantoro, Hans G. Kerkhoff, Andreas Leininger, Wolfgang Molzer, A. Motta, Christian Pacha, A. Pagani, **Alireza Rohani**, and R. Strasser. Thermal issues in test: An overview of the significant aspects and industrial practice. In *34th IEEE VLSI Test Symposium, VTS 2016, Las Vegas, NV, USA, April 25-27, 2016*, pages 1–4, 2016.
- [4] Riccardo Cantoro, Matteo Sonza Reorda, **Alireza Rohani**, and Hans G. Kerkhoff. On the maximization of the sustained switching activity in a processor. In *21st IEEE International On-Line Testing Symposium, IOLTS 2015, Halkidiki, Greece, July 6-8, 2015*, pages 34–35, 2015.
- [5] **Alireza Rohani** and Hans G. Kerkhoff. Two soft-error mitigation techniques for functional units of DSP processors. In *19th IEEE European Test Symposium, ETS 2014, Paderborn, Germany, May 26-30, 2014*, pages 1–6, 2014.
- [6] **Alireza Rohani** and Hans G. Kerkhoff. Rapid transient fault insertion in large digital systems. *Microprocessors and Microsystems - Embedded Hardware Design*, 37(2):147–154, 2013.
- [7] **Alireza Rohani**, Hans G. Kerkhoff, Enrico Costenaro, and Dan Alexandrescu. Pulse-length determination techniques in the rectangular single event transient fault model. In *2013 International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation, SAMOS 2013, Agios Konstantinos, Samos Island, Greece, July 15-18, 2013*, pages 213–218, 2013.
- [8] **Alireza Rohani** and Hans G. Kerkhoff. An on-line soft error mitigation technique for control logic of VLIW processors. In *2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems, DFT 2012, Austin, TX, USA, October 3-5, 2012*, pages 85–91, 2012.
- [9] **Alireza Rohani** and Hans G. Kerkhoff. A technique for accelerating injection of transient faults in complex socs. In *14th Euromicro Conference on Digital System Design, Architectures, Methods and Tools, DSD 2011, August 31 - September 2, 2011, Oulu, Finland*, pages 213–220, 2011.
- [10] **Alireza Rohani** and Hans G. Kerkhoff. Study of the effects of SET induced faults on submicron technologies. In *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W 2011), Hong Kong, China, June 27-30, 2011*, pages 41–46, 2011.
- [11] **Alireza Rohani** and Hamid R. Zarandi. Two effective methods to mitigate soft error effects in sram-based fpgas. *Microelectronics Reliability*, 50(8):1171–1180, 2010.
- [12] **Alireza Rohani** and Hamid R. Zarandi. An analysis of fault effects and propagations in AVR microcontroller atmega103(l). In *Proceedings of the The Forth International Conference on Availability, Reliability and Security, ARES 2009, March 16-19, 2009, Fukuoka, Japan*, pages 166–172, 2009.
- [13] **Alireza Rohani** and Hamid R. Zarandi. A new CLB architecture for tolerating SEU in sram-based fpgas. In *ReConFig'09: 2009 International Conference on Reconfigurable Computing and FPGAs, Cancun, Quintana Roo, Mexico, 9-11 December 2009, Proceedings*, pages 83–88, 2009.