Moshe Avital

1 BIOS

Name: Moshe Avital
Married +3
Address: Moshav Manot, Western Galilee, Israel
Email: mosheavi@gmail.com
Phone: +972-50-6943242

2 BACKGROUND

I earned my B.Sc. degrees in Mathematics and Electrical Engineering from Ben-Gurion University in 2006, as part of the joint program for outstanding students, and the M.Sc. degree in Electrical Engineering from Ben-Gurion University in 2012. I was a System Engineer with Texas Instruments from 2007 to 2011, and specialized in digital hardware implementations. I completed my Ph.D. in 2017 at Bar-Ilan University. My Ph.D. thesis deals with hardware security, and specifically countermeasures against side-channel attacks with the overarching goal of improving the security of cryptographic systems, hardware protections against power attack algorithms, better theoretic security evaluations of cryptographic devices and further development of Random Number Generator (RNG) circuits. My skills include the design, examination and optimization of security of hardware\embedded designs, and the development of countermeasures to mitigate physical attack algorithms. My expertise also includes digital design optimization and simulation, front-end designs, device level analysis, cryptographic architectures and low power design techniques.

3 EDUCATION

2012-2017 **Bar-Ilan University , Ramat Gan, Israel**
Ph.D. in Electrical and Computer Engineering

- Advisors: Prof. Alexander Fish and Dr. Osnat Keren
- Thesis: **Hardware Design Methodologies against Side-Channel Analysis Attacks on Secure Systems.**
    - The thesis analyzes and develops gate/circuit level countermeasures against Side-Channel Analysis, and in particular against Power Analysis attacks. The countermeasures incorporate custom and standard library cell designs. The underlying concepts involve the efficient utilization of random signals and power profile flattening. In addition, a highly area and integration-efficient solution for random bit stream generation has been implemented.

2010-2012 **Ben-Gurion University of the Negev, Be'er Sheva, Israel**
M.Sc. in Electrical and Computer Engineering

- Advisor: Prof. Raul Rabinovici
- Thesis: **Power Rectifiers and Input Filters.**
    - The thesis characterized general power rectifiers with either passive or active loads using 3-D manifolds of total harmonic distortion (THD) and output ripple. In addition, *input* current THD manifolds for an active load rectifier model were examined relative to the major harmonic induced by the active load inter-modulation.

2002-2006 **Ben-Gurion University of the Negev, Be'er Sheva, Israel**
B.Sc. in Electrical and Computer Engineering

2002-2006 **Ben-Gurion University of the Negev, Be'er Sheva, Israel**
B.Sc. in Mathematics

4 EMPLOYMENT HISTORY

2017-present **Rafael Advanced Defense Systems Ltd. , Haifa, Israel**

- Researcher in Failure Analysis and Reliability lab, performing mathematical analyses on physical parameters of electronic chips and circuits.

2012-2017 **EnICS Labs, Bar-Ilan University, Ramat Gan, Israel**
Research

- Lead researcher on VLSI secure cryptographic circuits against Power Analysis in the EnICS Labs of Bar Ilan University, and advisor on one M.Sc. thesis and two Senior projects.

2010-2016 **Bar-Ilan/ Ben-Gurion University, Israel**
Teaching Assistant

- Teaching assistant for *Digital Electronic Circuits*, and Lab assistant for *Introductory Electricity*, *Analog Circuits*, *Digital Electronic Circuits*, and *Advanced Semiconductor Devices*.

2007-2010 **Texas Instruments, Ra'anana, Israel**
System Engineer

- System engineer in chips containing Bluetooth, WLAN, GPS and NFS systems.
- Block level architecture, system integration, post silicon performance analysis, and design of system level test suites.
- SLIMbus standard integration in the new generation chips.

2005-2006 **Ben-Gurion University of the Negev, Be'er Sheva, Israel**
Research Assistant

- Research assistant in the acoustic lab of Prof. Boaz Rafaely as part of the "Spherical Microphone Arrays" project.

1997-2002 **Technological Unit of the Intelligence Corps, military post 2470, Israel**

- R&D team.