8223 Paint Branch Dr
College Park
MD 20740

Aria Shahverdi

(508)250-7476
ariash@umd.edu
www.ashahverdi.com

Education

Ph.D. in Electrical and Computer Engineering **Expected May 2019**
University of Maryland, College Park, MD GPA: 3.88/4.0

M.S. in Electrical and Computer Engineering **May 2015**
Worcester Polytechnic Institute, Worcester, MA GPA: 3.91/4.0

B.S. in Electrical Engineering **May 2013**
Sharif University of Technology, Tehran, Iran GPA: 3.6/4.0

Technical Skills

Software: Cadence Virtuoso, Xilinx ISE, Vivado Design Suite, Modelsim, MATLAB, intel VTune

Languages: C, Python, Verilog, Haskell, C++, C#, OpenGL, 8085/x86 Assembly

Platforms: Unix/Linux based OS's, Windows

Experience

Research and Teaching Assistant **Aug. 2015 - Present**
University of Maryland, College Park, MD
- Teaching Assistant of the course "Introduction to Cryptology".

Design for Security Intern **May - Jun. 2015**
Mentor Graphics Corporation, Wilsonville, OR
- Measured performance of PUF on FPGA and designed scalable implementation of SIMON.

Research and Teaching Assistant **Aug. 2013 - May 2015**
Worcester Polytechnic Institute, Worcester, MA
- Teaching Assistant of the course "Introduction to Cryptography and Information Security" and "Computer Organization and Design".

Intern at Access Section **Jun. - Sep. 2011**
Telecommunication Company of Tehran (TCT), Tehran, Iran
- Analyzed TCP/IP for LAN and Wireless LAN networks. Evaluated the behavior of IEEE 802.3 protocol and how different access methods such as Aloha and CSMA will affect the network.

Research Projects

Leakage Resilient Lattice Cryptography **Sep. 2017**
Consider the leakage resilience of the Ring-LWE analogue of the Dual-Regev encryption scheme. Put forth a high-level approach for proving the leakage resilience of the R-Dual-Regev scheme, by generalizing the original proof and we proved security for three instances of leakage function.

Side-Channel (Cache) Attacks on Databases **Aug. 2017**
Examined the BTree as an example of a data structure which is being used in databases. Identified the instruction cache behavior during the range queries. Based on the activities, detected how large the response to the query was and constructed the database from this information.

Locally Decodable and Updateable Non-Malleable Codes **Oct. 2016**
Constructed local non-malleable codes in the split-state model, that are secure against bounded retrieval adversaries. Computed a tight upper and lower bound for leakage resilient local non-malleable codes.

Threshold Implementation of SIMON **May 2015**

Analyzed a bit-serialized version of SIMON cipher against power side-channel attacks. Showed that the implementation is vulnerable on a FPGA and implemented a threshold version of SIMON which is proved to be secure against first and second order side-channel attacks.

Implementation of PRINCE – A Low-latency Block Cipher **Feb. 2014**

Implemented PRINCE cipher for microprocessor using parallel processing of states. Proposed a way to secure the implementation against side-channel attacks. Thanks to simple structure of non-linear level of this cipher, implemented homomorphic evaluation of this cipher. Published series of papers in peer-reviewed conference.

Design and Simulation of an ARM7500 Processor **May 2013**

Designed a 5-stage pipeline processor with dedicated L1 D-cache and a dynamic branch prediction.

Publications

On the Leakage Resilience of Ideal-Lattice Based Public Key Encryption, Under Review.

D. Dachman-Soled, M. Kulkarni, **A. Shahverdi**, "Local Non-Malleable Codes in the Bounded Retrieval Model", To Appear in PKC 2018.

D. Dachman-Soled, M. Kulkarni, **A. Shahverdi**, "Tight Upper and Lower Bounds for Leakage-Resilient, Locally Decodable and Updatable Non-Malleable Codes", PKC 2017.

A. Shahverdi, M. Taha, T. Eisenbarth, "Lightweight Side Channel Resistance: Threshold Implementations of SIMON", IEEE Transactions on Computers.

A. Shahverdi, M. Taha, T. Eisenbarth, "Silent SIMON: A Threshold Implementation under 100 Slices", 2015 IEEE Int. Symp. on Hardware-Oriented Security and Trust (HOST).

C. Chen, T. Eisenbarth, **A. Shahverdi**, X. Ye, "Balanced Encoding to Mitigate Power Analysis: A Case Study", Smart Card Research and Advanced Application Conference – CARDIS 2014.

Y. Doröz, **A. Shahverdi**, T. Eisenbarth, B. Sunar, "Toward practical homomorphic evaluation of block ciphers using prince", Workshop on Applied Homomorphic Cryptography and Encrypted Computing – WHAC14, 2014.

A. Shahverdi, C. Chen, T. Eisenbarth, "AVRprince - An Efficient Implementation of PRINCE for 8-bit Microprocessors", Technical Report, Worcester Polytechnic Institute, 2014.

Related Graduate Courses

Intro. to Modern Cryptography	Intro. to Quantum Info. Processing
Parallel Algorithm	Algorithm
Computer Security	Software Security
Advanced Cryptography	Information Theory & Coding
Cryptography & Data Security	Advanced Microprocessor

Leadership and Extracurricular Activities

President of Iranian Graduate Student Foundation at University of Maryland **Since 2017**

Treasurer of Iranian Student Association at Worcester Polytechnic Institute **2015**