8125 Paint Branch Dr
College Park
MD 20740

Aria Shahverdi

(Permanent Resident)

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

Summary/Objective

- Experience in Post-Quantum Cryptography (Lattice-Based Cryptography and Cryptanalysis of Assumptions such as LWE), Side-Channel Attacks (Cache Attacks, Power Analysis Attack)
- Looking for Research Scientist Position and SWE roles

Education

Ph.D. in Electrical and Computer Engineering — **Expected Early 2022**
University of Maryland, College Park, MD — GPA: 3.88/4.0

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

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

Experience

Research and Teaching Assistant — **Aug. 2013 - Present**
University of Maryland and Worcester Polytechnic Institute

- TA for Computer Systems Security, Intro to Cryptology, Computer Organization and Design.
- Developed tutorials and assignments for the Network Security part of the course.

Research Intern — **May - Aug. 2018**
Intellispar LLC (for Envieta), Columbia, MD

- Implemented Picnic post-quantum signature scheme in VHDL.

Design for Security Intern — **May - Aug. 2015**
Superior Talent Resource Inc. (for Mentor Graphics Corporation), Wilsonville, OR

- Measured performance of PUF on FPGA and designed scalable implementation of SIMON.

Research Projects

⋆ *The numbers in the parenthesis are referring to the paper listed in the Publications section.*

Studying Sparse Learning Parity with Noise (LPN) Problem (1)

- Studied a novel attack idea based on analyzing Fourier coefficients of the secret value.
- Proved the efficiency of the attack for certain parameters.

Side-Channel (Cache) Attacks on SQLite Databases (2)

- Identified the instruction cache behavior during the range queries.
- Demonstrated that the cache reveals the volume of the queries.
- Full reconstruction of the database based on the leaked information.

Leakage Resilient of Lattice-based Cryptography (3,4)

- Showed an attack on Ring LWE even if the secret key retains 3/4 of its entropy.

Fairness of a Machine Learning Models (5)

- Defined new fairness called *controlled fairness* with respect to protected features and filters.
- Proposed algorithms for retraining a given classifier to achieve controlled fairness.

Threshold Implementation of SIMON (9, 10)

- Analyzed a bit-serialized version of SIMON cipher against power side-channel attacks.
- Developed a version that is provably secure against first and second order side-channel attacks.

Publications

⋆ *The order of authors in publications marked with † is alphabetical.*

1. † D. Dachman-Soled, H. Gong, H. Kippen, **A. Shahverdi**, *BKW Meets Fourier: New Algorithms for LPN with Sparse Parities*, TCC 2021.
2. **A. Shahverdi**, M. Shirinov, D. Dachman-Soled, *Database Reconstruction from Noisy Volumes: A Cache Side-Channel Attack on SQLite*, 30th USENIX Security Symposium (USENIX Security 21).
3. † D. Dachman-Soled, H. Gong, M. Kulkarni, **A. Shahverdi**, *In Security of Ring LWE Under Partial Key Exposure*, Journal of Mathematical Cryptology 2020.
4. † D. Dachman-Soled, H. Gong, M. Kulkarni, **A. Shahverdi**, *Towards a Ring Analogue of the Leftover Hash Lemma*, Journal of Mathematical Cryptology 2020.
5. M. Chen, **A. Shahverdi**, S. Anderson, S. Y. Park, J. Zhang, D. Dachman-Soled, K. Lauter, M. Wu, *Transparency Tools for Fairness in AI (Luskin)*, Research in Mathematics and Public Policy 2020.
6. † D. Dachman-Soled, M. Kulkarni, **A. Shahverdi**, *Tight upper and lower bounds for leakage-resilient, locally decodable and updatable non-malleable codes*, Information and Computation 2019.
7. † D. Dachman-Soled, M. Kulkarni, **A. Shahverdi**, *Local Non-Malleable Codes in the Bounded Retrieval Model*, PKC 2018.
8. † D. Dachman-Soled, M. Kulkarni, **A. Shahverdi**, *Tight Upper and Lower Bounds for Leakage-Resilient, Locally Decodable and Updatable Non-Malleable Codes*, PKC 2017.
9. **A. Shahverdi**, M. Taha, T. Eisenbarth, *Lightweight Side Channel Resistance: Threshold Implementations of SIMON*, IEEE Transactions on Computers 2016.
10. **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).
11. 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.

Technical Skills

Languages: Python (including ML Packages), C/C++, Verilog/VHDL

Software: Xilinx ISE, Vivado Design Suite, Intel Quartus Prime, Modelsim, MATLAB, intel VTune

Platforms: Unix/Linux based OS's, Windows

Related Graduate Courses

Intro. to Modern Cryptography	Blockchain & Cryptocurrency Technologies
Statistical Pattern Recognition (Machine Learning)	Intro. to Quantum Info. Processing
Computer Security	Software Security
Cryptography & Data Security	Machine Learning (Coursera)
Parallel Algorithm	Deep Learning (Coursera)

Leadership and Extracurricular Activities

ECE Program's Representatives at Graduate Student Government	**2018- 2020**
Ex-Officio (GSG Representative) on the Student Affairs Committee at University Senate	**2018**
President of Iranian Graduate Student Foundation at University of Maryland	**2017-2018**