FAU COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Mojtaba Bisheh Niasar

for the degree of Doctor of Philosophy (Ph.D.)

"Efficient and Secure Implementation of Classic and Post-Quantum Public-Key Cryptography"

July 7, 2022, 12:00 p.m.
Virtual Dissertation

Zoom Meeting
Meeting ID: 838 2531 1945
Passcode: Fm5xQ4

DEPARTMENT:
Electrical Engineering and Computer Science

ADVISOR:
Reza Azarderakhsh, Ph.D.

PH.D. SUPERVISORY COMMITTEE:
Reza Azarderakhsh, Ph.D., Chair
Imadeldin Mahgoub, Ph.D.
Mehran Mozaffari Kermani, Ph.D.
Feng-Hao Liu, Ph.D.

ABSTRACT OF DISSERTATION

To address the increased interest in crypto hardware accelerators due to performance and efficiency concerns, implementing hardware architectures of different public-key cryptosystems has drawn growing attention. Pure hardware methodology enhances architecture's performance over a hardware/software co-design scheme at the cost of a more extended design cycle, reducing the flexibility, and demands customized data paths for different protocol-level operations. However, using pure hardware architecture makes the design smaller, faster, and more efficient. This dissertation mainly focuses on designing crypto accelerators that can be used in embedded systems and Internet-of-Things (IoT) devices where performance and efficiency are critical as a hardware accelerator to offload computations from the microcontroller units (MCU). In particular, our objective is to create a system-on-chip (SoC) crypto-accelerator with an MCU that achieves high area-time efficiency. Our implementation can also be integrated as an off-chip solution; however, other criteria, such as performance, are often as important or more important than efficiency in the external crypto-chip design. Not only does our architecture inherently provide protection against timing and simple power analysis (SPA) attacks, but also some advanced security mechanisms to avoid differential power analysis (DPA) attacks are included, which is missing in the literature. Specifically, this dissertation presents (i) several design strategies to port recent standardized elliptic curve cryptography (ECC) based key exchange protocols and digital signature algorithms (DSA) to various platforms considering different design goals (i.e., time-constrained, area-constrained, and area-time trade-off applications) using a precise schedule corresponding to each architecture, (ii) different monolithic hardware implementations to accelerate lattice-based post-quantum cryptography (PQC), and (iii) several effective countermeasures to make our designed cryptosystems (e.g., from both algorithmic and implementation points of view) more secure against side-channel analysis (SCA) information leakage attacks.

BIOGRAPHICAL SKETCH
Born in Kashan, Iran
B.S., Amirkabir University of Technology, Tehran, Iran, 2007-2011
M.S., Iran University of Science and Technology, Tehran, Iran, 2013-2015

Ph.D., Florida Atlantic University, Boca Raton, Florida, 2019-2022

CONCERNING PERIOD OF PREPARATION & QUALIFYING EXAMINATION

Time in Preparation: Fall 2019-Summer 2022

Qualifying Examination Passed: Spring 2020

Published Papers:

Bisheh Niasar, M., Elkhatib, R., Azarderakhsh, R., and Mozaffari Kermani, M., "Fast, Small, and Area-Time Efficient Architectures for Key-Exchange on Curve25519," In: 27th IEEE International Symposium on Computer Arithmetic (ARITH-2020), Portland, Oregon, USA, Jun 2020, pp. 72-79, 2020.

Bisheh Niasar, M., Azarderakhsh, R., and Mozaffari Kermani, M. “Efficient Hardware Implementations for Elliptic Curve Cryptography over Curve448,” In: 21st International Conference on Cryptology in India (IndoCrypt 2020), Kolkata, India, Dec 2020, val 12578, pp. 228-247, Springer, Cham, 2020.

Bisheh Niasar, M., Azarderakhsh, R., and Mozaffari Kermani, M. “Area-Time Efficient Hardware Architecture for Signature Based on Ed448”, IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 68, no. 8, pp. 2942-2946, 2021.

Bisheh Niasar, M., Azarderakhsh, R., and Mozaffari Kermani, M. “Cryptographic Accelerators for Digital Signature Based on Ed25519”, IEEE Transactions on Very Large Scale Integration Systems, vol. 29, no. 7, pp. 1297-1305, 2021.

Bisheh Niasar, M., Azarderakhsh, R., and Mozaffari Kermani, M. “High-Speed NTT-based Polynomial Multiplication Accelerator for Post-Quantum Cryptography,” In: 28th IEEE International Symposium on Computer Arithmetic (ARITH-2021), 2021, pp. 94-101, Turin, Italy, Jun 14-16, 2021.

Bisheh Niasar, M., Azarderakhsh, R., and Mozaffari Kermani, M. “A Monolithic Hardware Implementation of Kyber: Comparing Apples to Apples in PQC Candidates,” In: 7th International Conference on Cryptology and Information Security in Latin America (LatinCrypt 2021), Oct 6-8, 2021, vol 12912, pp. 108-126, Springer, Cham, 2021.

Anastasova M., Bisheh Niasar, M., Azarderakhsh, R., and Mozaffari Kermani, M. “Compressed SIKE Round 3 on ARM Cortex-M4,” In: 17th EAI International Conference on Security and Privacy in Communication Networks (EAI SecureComm 2021), Sep 6-9, 2021, vol 399, pp. 441-457, Springer, Cham, 2021.

Bisheh Niasar, M., Azarderakhsh, R., and Mozaffari Kermani, M. “Instruction-Set Accelerated Implementation of CRYSTALS-Kyber,” IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 68, no. 11, pp. 4648-4659, Nov. 2021.

Anastasova, M., Bisheh Niasar, M., Seo, H. Azarderakhsh, R., and Mozaffari Kermani, M. “Efficient and Side-Channel Resistant Design of High-Security Ed448 on ARM Cortex-M4,” In: 15th IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2022.

Bisheh Niasar, M., Anastasova, M., Abdulgadir, A., Seo, H., Azarderakhsh, R., and Mozaffari Kermani, M. “Accelerated and Protected Microarchitectural Design of Curve448 on Cortex-M4,” IEEE Transactions on Very Large-Scale Integration Systems. (Submitted)

Bisheh Niasar, M., Anastasova, M., Abdulgadir, A., Seo, H., and Azarderakhsh, R. “Security Evaluation Against Side-Channel Analysis for Implementation of Curve448 on ARM Cortex-M4,” IEEE Transactions on Circuits and Systems I: Regular Papers. (Submitted)