FAU COLLEGE OF ENGINEERING AND COMPUTER SCIENCE
FLORIDA ATLANTIC UNIVERSITY

Announces the Ph.D. Dissertation Defense of

Mila Anastasova

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

“Classical and Post-Quantum Cryptography on Modern ARM-based Processors”

April 1st, 2024, 10 a.m.
Engineering East, Room 303
777 Glades Road
Boca Raton, FL

DEPARTMENT:
Electrical Engineering and Computer Science

ADVISOR:
Reza Azarderakhsh , Ph.D.

PH.D. SUPERVISORY COMMITTEE:
Reza Azarderakhsh, Ph.D., Chair
Mehran Mozaffari Kermani, Ph.D.
Jason Hallstrom, Ph.D.
Mohammad Ilyas, Ph.D.

ABSTRACT OF DISSERTATION

“Classical and Post-Quantum Cryptography on Modern ARM-based Processors”

Cryptographic algorithms are being developed and incorporated into network security protocols to provide secure communication over insecure mediums like the Internet, ensuring data integrity, confidentiality, authentication, and non-repudiation.

The urge to deploy cryptographic protocols on low-end devices, based on the constantly growing Internet of Things (IoT) world, requires optimal design and implementation of the underlying cryptographic algorithms to achieve small communicational and computational cost, while preserving the privacy of the transmitted data. Scenarios of low bandwidth, constrained memory, and limited processing power are common when targeting embedded devices; however, security requirements are still present due to the sensitive information that may be communicated. In our work, we address the need for optimal and secure cryptographic primitive implementation design in terms of computing capabilities, energy and power consumption, and memory usage to accommodate the deployment of classical and post-quantum cryptographical systems on modern ARM-based constrained devices.

BIOGRAPHICAL SKETCH
Sofia, Bulgaria
B.S., Universidad Carlos III de Madrid, Leganes, Madrid, Spain, 2019
M.S., Florida Atlantic University, Boca Raton, Florida, USA, 2022
Ph.D., Florida Atlantic University, Boca Raton, Florida, 2024

CONCERNING PERIOD OF PREPARATION
& QUALIFYING EXAMINATION

Time in Preparation: 2019 – 2024

Qualifying Examination Passed: Spring 2020

Published Papers:

- **Anastasova, M.**, Azarderakhsh, R. and Kermani, M.M., 2021. Fast strategies for the implementation of SIKE round 3 on ARM Cortex-M4. IEEE Transactions on Circuits and Systems I: Regular Papers, 68(10), pp.4129-4141.
- **Anastasova, M.**, Bisheh-Niasar, M., Seo, H., Azarderakhsh, R. and Kermani, M.M., 2022, June. Efficient and side-channel resistant design of high-security Ed448 on ARM Cortex-M4. In 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST) (pp. 93-96). IEEE.
- **Anastasova, M.**, Azarderakhsh, R., Kermani, M.M. and Beshaj, L., 2022, November. Time-Efficient Finite Field Microarchitecture Design for Curve448 and Ed448 on Cortex-M4. In International Conference on Information Security and Cryptology (pp. 292-314). Cham: Springer Nature Switzerland.
- Seo, H., **Anastasova, M.**, Jalali, A. and Azarderakhsh, R., 2020. Supersingular isogeny key encapsulation (SIKE) round 2 on ARM Cortex-M4. IEEE Transactions on Computers, 70(10), pp.1705-1718.
- **Anastasova, M.**, Azarderakhsh, R. and Kermani, M.M., 2022, August. Time-optimal design of finite field arithmetic for sike on cortex-m4. In International Conference on Information Security Applications (pp. 265-276). Cham: Springer Nature Switzerland.
- **Anastasova, M.**, Bisheh-Niasar, M., Azarderakhsh, R. and Kermani, M.M., 2021. Compressed SIKE round 3 on ARM Cortex-M4. In Security and Privacy in Communication Networks: 17th EAI International Conference, SecureComm 2021, Virtual Event, September 6–9, 2021, Proceedings, Part II 17 (pp. 441-457). Springer International Publishing.
- Bisheh-Niasar, M., **Anastasova, M.**, Abdulgadir, A., Seo, H. and Azarderakhsh, R., 2022, October. Side-Channel Analysis and Countermeasure Design for Implementation of Curve448 on Cortex-M4. In Proceedings of the 11th International Workshop on Hardware and Architectural Support for Security and Privacy (pp. 10-17).
- **Anastasova, M.**, El Khatib, R., Laclaustra, A., Azarderakhsh, R. and Kermani, M.M., 2023, November. Highly Optimized Curve448 and Ed448 design in wolfSSL and Side-Channel Evaluation on Cortex-M4. In 2023 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-8). IEEE.
- Aghapour, S., Ahmadi, K., **Anastasova, M.**, Kermani, M.M. and Azarderakhsh, R., 2023. PUF-Kyber: Design of a PUF-Based Kyber Architecture Benchmarked on Diverse ARM Processors. Authorea Preprints.
- Aghapour, S., Ahmadi, K., **Anastasova, M.**, Kermani, M.M. and Azarderakhsh, R., 2023. PUF-Dilithium: Design of a PUF-Based Dilithium Architecture Benchmarked on ARM Processors. Authorea Preprints.
- **Anastasova, M.**, Azarderakhsh, R., Kermani, M. M. (2024). "Fully Hybrid TLSv1.3 in WolfSSL on Cortex-M4." In ACNS Workshop on Secure Crypto- graphic Implementations (SCI), Springer International Publishing.