

Bardia Taghavi

PhD Candidate & Cryptographic Hardware Engineer

Boca Raton, FL | bardia.taghavi@pqsecurity.com | staghavi2024@fau.edu | bardiataghavi.com |
linkedin.com/in/bardia-taghavi | github.com/bardiat94

PROFESSIONAL SUMMARY

PhD Candidate and Cryptographic Hardware Engineer at PQSecure Technologies, specializing in hardware for post-quantum cryptography. Bringing deep expertise in Post-Quantum Cryptography (PQC), VHDL/SystemVerilog RTL development, and FPGA validation to design quantum-resistant, ultra-lightweight, and high-performance secure systems. Possess a strong mathematical foundation with actively developing knowledge in side-channel analysis and countermeasures.

CORE PROFICIENCIES & SKILLS

- Cryptography:** Post-Quantum Cryptography, Module-Lattice-Based Cryptography (ML-KEM/ML-DSA), Number Theoretic Transform, Modular Arithmetic, Traditional Cryptography Schemes (AES, RSA, ECC, etc.). *Developing:* Side-Channel Resistance (Masking/Shuffling).
- Hardware & Architecture:** RTL Design (VHDL/SystemVerilog/Verilog), Synthesis & Simulation (Vivado), FPGA Validation (Xilinx Artix-7, Zynq UltraScale+), Microarchitecture, Datapath Design, Pipelining, Resource Constrained Hardware Design, Software/Hardware Co-design.
- Software & Environments:** Python, C/C++, Machine Learning, Deep Learning, Image Processing, Signal Processing, ARM Microcontrollers, Embedded Systems, Assembly, Linux, LaTeX, Git.

EDUCATION

Florida Atlantic University

Doctor of Philosophy – PhD, Computer Engineering

Research Focus: Hardware Architectures for Post-Quantum Cryptography

GPA: 4.0 / 4.0

Boca Raton, FL

Expected May 2028

University of Tehran

Master of Science – MS, Mechatronics & Electronics

Research Focus: Machine Learning for Biosignal Processing on Embedded Systems

GPA: 3.54 / 4.0

Tehran, Iran

Sep 2017 – Feb 2021

K. N. Toosi University of Technology

Bachelor of Science – BS, Electrical and Electronics Engineering

Tehran, Iran

Sep 2012 – Sep 2016

RESEARCH & PROFESSIONAL EXPERIENCE

PQSecure Technologies

Cryptographic Hardware Engineer

- Developing post-quantum cryptography IP cores, including several arithmetic cores for ML-KEM and ML-DSA spanning compact to high-throughput architectures.

Boca Raton, FL

May 2026 – Present

Florida Atlantic University

Graduate Research Assistant, Cryptography & Hardware Design

- Unified Full-Spectrum Polynomial Core:** Developed a highly optimized, unified polynomial multiplier architecture "HyperPoly" for maximum performance in lattice-based cryptography, capable of handling all polynomial multiplication operations required in ML-KEM/ML-DSA in a single unified core, currently under review at IEEE TCAD.
- Architecting High-Performance PQC Hardware:** Designed "ParallelNTT", an innovative, completely parallel architecture for forward and inverse NTT for ML-DSA and ML-KEM. Extensively parallelized datapath to bypass RAM bottlenecks and achieve a $24\times$ latency reduction over state-of-the-art designs using Virtex UltraScale+ FPGAs.

Boca Raton, FL

May 2024 – Present

- **Resource-Constrained Security Modules:** Developed “KNightCore,” an ultra-lightweight Hardware IP for ML-KEM polynomial multiplication geared towards Internet of Things (IoT) devices, utilizing zero DSP blocks and optimal SystemVerilog logic implementation.
- **Efficient Algorithm Implementation:** Initiated and deployed “LightNTT”, a highly-efficient hardware unit featuring constant-geometry dataflow and optimized pipelined Barrett multipliers for Module-Lattice-Based Cryptography.
- **Hardware Validation:** Mapped cryptographic modules onto Xilinx FPGAs, focusing on secure synthesis and researching integration of side-channel countermeasures to protect against timing and fault injection attacks.
- **Teaching Experience:** Served as a Teaching Assistant and Lab Instructor for several graduate and undergraduate courses, including Advanced FPGA Design, Cryptographic Engineering, Structured VLSI Design, and Design of Digital Systems.

University of Tehran

Tehran, Iran

Mechatronics Engineer, Advanced Service Robots (ASR) Lab

Sep 2017 – Feb 2021

- Designed and implemented a deep learning model for gait analysis for amputee subjects utilizing Python on a RaspberryPi board, with data collected and categorized in an STM32-based system.

PUBLICATIONS & ACADEMIC CONTRIBUTIONS

1. **B. Taghavi et al.**, “*High-Performance Post-Quantum Cryptographic Engineering in Hardware*”. Book Chapter, Springer, 2026. DOI: 10.1007/978-3-032-09303-5_14.
2. **B. Taghavi**, R. Azarderakhsh, M. Mozaffari Kermani, “*HyperPoly: A Unified, Max-Performance Polynomial Core*”. Under review, IEEE TCAD.
3. **B. Taghavi**, R. Azarderakhsh, M. Mozaffari Kermani, “*ParallelNTT: Maximizing Performance of Forward and Inverse NTT on FPGA for ML-DSA and ML-KEM*”. DOI: 10.1145/3716368.3735214.
4. **B. Taghavi**, R. Azarderakhsh, M. Mozaffari Kermani, “*KNightCore: An Ultra-Lightweight NTT-Based Polynomial Multiplier for ML-KEM on Resource-Constrained Platforms*”. DOI: 10.1145/3733820.3764684.
5. **B. Taghavi**, R. Azarderakhsh, M. Mozaffari Kermani, “*LightNTT: A Tiny NTT/iNTT Core for ML-DSA Featuring a Constant-Geometry Pipelined Design*”. DOI: 10.1007/978-3-032-15541-2_4.

PROFESSIONAL SERVICE

Reviewer for IEEE HOST 2025 and 2026, ARITH 2026, IEEE TCAD, and IACR TCHES.