Arsalan Malik

Security Researcher and Design Engineer

aamalik3@ncsu.edu Raleigh,US in/aamalik3 https://rb.gy/lgwtsj https://rb.gy/kzm2k3

Profile

Pursuing a Ph.D. at North Carolina State University. I specialize in uncovering and mitigating security vulnerabilities in hardware systems. My research emphasizes thorough security evaluations across various implementations, particularly focusing on conducting physical attacks like fault and side-channel assaults. This work aims to heighten security awareness and bolster the defenses of complex systems, thereby fortifying them against potential vulnerabilities. With a deep understanding of hardware design, I have adeptly enhanced the speed and security of multiple applications on ASIC/FPGA platforms. Motivated & experienced individual in applied cryptography area with 7+ years experience.

Education

Ph.D. Computer Engineering *(North Carolina State University)* **Raleigh, USA** *2022-2026 (Expected)*

Relevant Courses: Cryptographic engineering & hardware security, Microprocessor architecture, Architecture of parallel computers, Operation systems, Compiler optimization & scheduling, ASIC & FPGA design with Verilog, ASIC verification.

M.Sc. Computer Engineering *(Sir Syed CASE Institute of Technology)* **Islamabad, Pakistan** *2017-2020*

Thesis: Evaluation of isolation design flow for single chip cryptographic applications

Relevant Courses: Cryptography & network security, Reconfigurable computing, Advanced computer networks.

B.Sc. Electrical Engineering *(Sir Syed CASE Institute of Technology)* **Islamabad, Pakistan** *2011-2015*

Relevant Courses: OOP and data structures using C++, Microprocessor & computer architecture, Digital signal processing, Microprocessor based embedded system design, Digital system design, Industrial Automation, Network programming, Engineering project management, Network Security, Professional ethics, Parallel processing, Entrepreneurship

Work Experience

Research Assitant, *(North Carolina State University)* **Raleigh, US** *08/2022 - Present*

- Fault injections and side-channel attacks on AI/ML implementations (Supported by US Navy – Office Of Naval Research)
- Secure preemption and context switching in cloud FPGAs (Supported by US Navy – Office Of Naval Research)
- Reconfigurable designs for multi-tenant FPGAs
- Secure & efficient FPGA virtualization support in the cloud (Supported by US Navy – Office Of Naval Research)

Senior FPGA Engineer, *(RAPIDEV)* **Islamabad, PK** *09/2021 - 07/2022*

- Key management system for HCLOS radios
- Developed hardware security module for secure communication
- Active/passive intrusion detection & prevention
- Cryptographic primitives RTL-implementation
- Smart Card & Bio-Metric integration for $2 - FA$

Research Officer, *(Crypto Research & Development Center)* **Islamabad, PK** *03/2016 - 08/2021*

- FPGA & embedded processors based system designing
- Secure system designing as per FIPS 140-2, MIL-STD-810 F & MIL-STD-461 G STD's
- Reverse Engineering
- MIL-STD Complaint system development for aerial and ground platforms
- FPGA design security & side-channel secure implementations
- Recruitment and training of human resource

Publications

1. **Malik, Arsalan Ali**, Karabulut, Emre, Amro Awad, and Aydin Aysu. "Enabling Secure and Efficient Sharing of Accelerators in Expeditionary Systems." **Accepted in Journal of Hardware and Systems Security (2024).**
2. **Malik, Arsalan Ali**, Karabulut, Emre, Amro Awad, and Aydin Aysu. "DEFENSER: Defense Framework for Secure Accelerator Sharing in Expeditionary Systems." **Accepted in GOMACTech (2024).**
3. Nasir, Neelam, **Malik, Arsalan Ali**, Ifra Tahir, Ammar Masood, and Naveed Riaz. "Ephemeral Key-based Hybrid Hardware Obfuscation." in 19th International Bhurban Conference on Applied Sciences and Technology (IBCAST), pp. 646-652. IEEE, (2022).
4. Sultana, Bushra, Anees Ullah, **Malik, Arsalan Ali**, Ali Zahir, Pedro Reviriego, Fahad Bin Muslim, Nasim Ullah, and Waleed Ahmad. "VR-ZYCAP: A versatile resourse-level ICAP controller for ZYNQ SOC." in Electronics 10, no. 8 (2021): 899.
5. **Malik, Arsalan Ali**, Anees Ullah, Ali Zahir, Affaq Qamar, Shadan Khan Khattak, and Pedro Reviriego. "Isolation Design Flow Effectiveness Evaluation Methodology for Zynq SoCs." in Electronics 9, no. 5 (2020): 814.

Certificates & Trainings

- CITI Conflicts of Interest (NC State University)
- CITI Responsible Conduct of Research (NC State University)
- CITI Human Subject Research (NC State University)
- CCNA Training of Routing & Switching (CORVIT)
- Linux System Administration (CORVIT)
- Certified Training in FIPS 140-2, NIST-SP {800-21, 800-38A, 800-56 & 800-57} and IPC-A-600 Standards (CRDC)

Skills

- **ASIC/FPGA Design:** Power & Performance Optimization, Scripting (MATLAB, Tcl), SystemVerilog, C and C++, Code and Functional Coverage Analysis
- **Hardware Security:** Cryptography, Fault-Injection Attack, Secure Architecture Design, Side-Channel Countermeasures
- **Tools:** Dev C++, Xilinx {ISE, Plan-ahead, Vivado, SDK, Vitis}, Microsoft {Project, Visio & Office}, LaTeX, Packet Tracer, Proteus, ORCAD Capture, MATLAB, ModelSim, QuestaSim, Synopsys Clion.
- **Soft Skills:** Presentation, Planning, Organized, Creative Problem-Solving, Teamwork, Analytical Thinking

Languages

- **English** [Advanced] - C1
- **Urdu** [Native]