# Jubayer Mahmod

**PhD candidate, Bradly Dept. of Electrical & Computer Engineering**
**Graduate research assistant, Forte-Research Group, Computer Science**
**Virginia Tech**

https://computing.ece.vt.edu/∼Jubayer/
jubayer@vt.edu
+1 (334) 524-6872


## RESEARCH INTERESTS

With 6+ years of experience in hardware-oriented system security, my expertise encompasses a wide range of interests, including the security of systems, firmware, and hardware. My current research is centered on leveraging architectural and low-level hardware behaviors to develop system-level attack and defense strategies. This includes work on Trusted Execution Environments (TEE), side-channel attacks, cloud FPGA security, and the creation of innovative frameworks for anti-counterfeit chip detection and avoidance.

## EDUCATION

**PhD, Computer Engineering, Virginia Tech, USA** 08/19–05/24
*Thesis: Designing Attacks and Defenses leveraging SRAM Data Remanence* **Advisor:**Dr. Matthew Hicks

**MS, Electrical & Computer Engineering, Auburn University, AL, USA** 08/17–08/19
*Thesis: Towards Unclonable System Design for Resource-Constrained Applications* **Advisor**: Dr. Ujjwal Guin

**BS, Electrical & Electronic Engineering (EEE)** 03/16
Bangladesh University of Engineering & Technology (BUET), Dhaka
*Thesis: Metal-Insulator-Metal Ring Resonator Design for Sensing Applications* **Advisor:** Dr. Zahurul Islam

## RESEARCH SUMMARY

**First authored publications in top-tier venues (3): Oakland(x1), ASPLOS(x2)**
**Other publications (5)**

## SELECTED PUBLICATIONS

1. **Jubayer Mahmod** & Matthew Hicks. *UnTrustZone: Systematic Accelerated Aging to Expose On-chip Secrets.* IEEE Symposium on Security and Privacy. (To appear Oakland'24[Link])
2. **Jubayer Mahmod** & Matthew Hicks. *Invisible Bits: Hiding Secret Messages in SRAM's Analog Domain.* International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'22)
3. **Jubayer Mahmod** & Matthew Hicks. *SRAM Has No Chill: Exploiting Power Domain Separation to Steal Onchip Secrets.* International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'22)
4. **Jubayer Mahmod** & Ujjwal Guin. *A Robust, Low-Cost and Secure Authentication Scheme for IoT Applications*. Cryptography 4.1 (2020)
5. **Jubayer Mahmod**, Millican Spencer, Ujjawal Guin, and Vishwani Agrawal. *Delay Fault Testing: Present and Future*. IEEE VLSI Test Symposium (VTS'19).
6. Benjamin Cyr, **Jubayer Mahmod**, Ujjwal Guin. *Low-Cost and Secure Firmware Obfuscation Method for Protecting Electronic Systems from Cloning*. IEEE Internet of Things Journal (2019)

## EXPERIENCE & INTERNSHIPS

| | | |
|---|---|---|
| Virginia Tech, VA | Graduate Research Assistant | 01/20– now |
| ForteMedia, Inc, Santa Clara, CA | Graduate Engineering Intern | Summer 2018, 2019 |
| Auburn University, AL | Graduate Research Assistant | 08/17 - 05/19 |

## TEACHING EXPERIENCE

| | | | |
|---|---|---|---|
| Virginia Tech | ECE 4514: Digital Design II | GTA | Fall 2019 |
| Auburn University | ELEC 6970: Hardware Security I | GTA | Fall 2018 |
| Daffodil International University, Dhaka | Undergraduate electronics courses | Lecturer | 09/16-07/17 |

## TECHNICAL SKILLS

• Hardware/software co-design • Applied Cryptography • Cloud FPGA design (aws F1)
• Trusted execution environment: ARM TrustZone, SGX • Linux kernel, Coreboot, OpenOCD/JTAG.
• C, Assembly (x86 & ARM), Verilog, Python • Cadence Design Tools, Hspice.

## SELECTED PROJECTS

- **Exploiting SRAM data remanence to design attacks**: Leveraged SRAM's analog characteristics and power domain separation to design **Volt Boot** and **UntrustZone**. Volt Boot shows

how to create artificial data retention across power cycles in an SoC 100% accuracy. Using a secure boot or a trusted execution environment can be potential mitigation, which inspired a more robust form of attack, UntrustZone, that still exfiltrates data/code ($> 98\%$ accuracy) from on-chip SRAM using accelerated transistor wear-out. **Outcome**: two top-tier conference publications.

- **Defenses leveraging SRAM data remanence**: Designed data hiding & SoC anti-counterfeit systems utilizing SRAM's analog behavior, specifically circuit aging. **Invisible bits** is a steganography scheme that creates a covert, cryptographically secure but plausibly deniable information transfer channel in the hardware. Further applied imprinting and data retention voltage techniques for detecting and avoiding recycled, remarked, and cloned chips. **Outcome**: Three papers [Invisible bits, Retain-the-date, SKU-RAM (under review)]
- **Cloud FPGA localization**: Developed a cloud FPGA localization system using dynamic timing faults in functionally valid circuits, circumventing AWS security restrictions on hardware DNA access. This entirely **on-chip** signature extraction method achieves >**99% accuracy**, **operates 13X faster**, and **costs 92% less** than the state-of-the-art (under review).
- **Hardware-assisted firmware obfuscation**: Developed a custom MIPS core featuring a reorder cache in the instruction fetch unit, enabling dynamic and transparent reconstruction of control flow from obfuscated firmware. **Outcome**: a journal paper.

*Graduate course projects*

- **Hardware/Software Co-Design**:
  – Machine learning inference: Developed a NIOS-II-based ML accelerator, focusing on resource-efficient heterogeneous computing through custom instruction & hardware/software co-design. Achieved **2500x** speed boost compared to baseline software-only implementation using ARM-FPGA system.
  – Crypto acceleration engines: Implemented RSA hardware engine using Radix-2 Montgomery multiplication and Chinese remainder theorem. AES Engine: Crafted for Hardware Trojan demonstrations.
- **Linux kernel programming**:
  – Intra-Process isolation: Utilized Intel's *Memory Protection Key (MPK)* and *libmpk* to explore user-space memory permission control at page granularity.
  – Distributed shared memory synchronization: Implemented MESI protocol to synchronize shared pages across multiple Linux processes/machines using user-space page-fault handling (userfaultfd).

## PRESENTATION & TALKS

**Invisible Bits: Hiding Secret Messages in SRAM's Analog Domain.** (ASPLOS) 2022
**SRAM Has No Chill: Exploiting Power Domain Separation to Steal Onchip Secrets.** (ASPLOS) 2022
**SRAM PUF-based device authentication protocol hardware demo.** (HOST) 2019
**Graduate Research Showcasing.** Auburn University 2018
**Hardware Trojan showcasing (hardware & poster)** NAE Grand Challenges Scholars Program 2018

## AWARDS

| | | |
|---|---|---|
| NSF travel grant | ASPLOS, Switzerland | 2022 |
| NSF travel grant | Symposium on Hardware Oriented Security & Trust | 2019 |
| Graduate school tuition fellowship | Auburn University | 2017-19 |
| Best project award | Tensilica Xtensa Embedded-DSP design contest, India | 2016 |
| Dean's List award | BUET | |

## SERVICE

**Reviewer:**
– IEEE Internet of Things Journal 2022
– Journal of Hardware and Systems Security 2023

**External Reviewer:**
• ASPLOS'24 • IEEE Transactions on Circuits and Systems I'21 • VLSID'19 • DAC'19 • GLSVLSI'19 • Journal of Hardware and Systems Security'19 • IEEE Transactions on Very Large Scale Integration Systems'17 &'18 • VLSI Test Symposium'18 • Transactions on Multi-Scale Computing Systems'18