Jubayer Mahmod

Security Engineer @ AWS
Ex-Sr. Security Engineer@Lucid Motors (Red Team)
Hardware Security PhD @ Virginia Tech

www.jubayer.io
jubayeramahmod@gmail.com
https://www.linkedin.com/in/jubayer0175/

SUMMARY Hardware security researcher with 8 years of experience in the security of silicon, firmware, and cloud platforms. My doctoral work encompass developed attacks and defenses to systems via SRAM remanence, including secure-boot/TEE design, side-channel & fault attacks, cloud-FPGA provenance, and anti-counterfeit silicon.

EDUCATION

PhD, Computer Engineering, Virginia Tech, USA 04/24
Thesis: The Art of SRAM Security: **Advisor:**Dr. Matthew Hicks
Tactics for Remanence-based Attack and Strategies for Defense

MS, Electrical & Computer Engineering, Auburn University, AL, USA 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

PROFESSIONAL EXPERIENCE

Amazon	Security Engineer	WA	09/2024 - present
Lucid Motors	Senior Security Engineer (Red Team)	CA	04/2024-09/2024
Virginia Tech	Research Assistant	VA	08/2019-04/2024
Auburn University	Research Assistant	AL	08/2017-08/2019

TECHNICAL SKILLS

• Hardware/software co-design • Applied Cryptography • ARM SoC/Cloud FPGA security (aws F1)
• TEE: ARM TrustZone, SGX • Linux kernel, Coreboot, Secure debug, Threat modeling
• C, Assembly (x86 & ARM), Verilog, Python • Cadence Design Tools, Ghidra.

RESEARCH SUMMARY

First authored publications in top-tier venues (4): **Oakland(x1), ASPLOS(x3)**
Other publications (6)

SELECTED PUBLICATIONS

1. **Jubayer Mahmod** & Matthew Hicks. *PhasePrint: Exposing Cloud FPGA Fingerprints by Inducing Timing Faults at Runtime*. International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2025) [Acceptance rate: 20%]
2. **Jubayer Mahmod** & Matthew Hicks. *UnTrustZone: Systematic Accelerated Aging to Expose On-chip Secrets.* IEEE Symposium on Security and Privacy (SP 2024) [Acceptance rate: 12%].
3. **Jubayer Mahmod** & Matthew Hicks. *SRAM Imprinting for System Protection and Differentiation.* (ACM AsiaCCS 2024) [Acceptance rate: 20%]
4. **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 2022) [Acceptance rate: 20%]
5. **Jubayer Mahmod** & Matthew Hicks. *SRAM Has No Chill: Exploiting Power Domain Separation to Steal On-chip Secrets.* International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2022)[Acceptance rate: 20%]
6. **Jubayer Mahmod** & Matthew Hicks. *Retain The Date: Purging Recycled Chips from the Supply Chain through SRAM's Data Retention Behavior (under submission)*
7. **Jubayer Mahmod** & Ujjwal Guin. *A Robust, Low-Cost and Secure Authentication Scheme for IoT Applications*. Cryptography 4.1 (2020)
8. **Jubayer Mahmod**, Millican Spencer, Ujjawal Guin, & Vishwani Agrawal. *Delay Fault Testing: Present and Future*. IEEE VLSI Test Symposium (VTS'19).
9. 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)

SELECTED PROJECTS

- **Platform Security Architecture:** Led security design for an AWS embedded platform, spanning SoC-level evaluation and cloud integration. Defined security requirements, performed threat modeling, and conducted black-box testing of hardware-backed features. Delivered architectural recommendations that balanced robustness, performance, and cost. Collaborated cross-functionally across silicon, firmware, and cloud teams to ensure end-to-end security.
- **Exploiting SRAM data remanence to design attacks**: Demonstrated artificial data retention with 100 % accuracy on multiple SoCs (Volt Boot), then evolved the technique to bypass ARM TrustZone and exfiltrate code/data with >98% accuracy via accelerated transistor aging (UnTrustZone). The work exposed limitations of on-chip cryptographic defenses under data remanence threats.
- **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 demonstrated that imprinting and data retention voltage techniques can be applied for detecting and avoiding recycled, remarked, and cloned chips.
- **Cloud FPGA localization**: Developed an on-chip timing-fault technique that fingerprints cloud FPGAs with $>$ 99% accuracy, 13$\times$ speedup, and 92 % lower cost—eliminating reliance on restricted hardware-DNA interfaces.

TALKS

PhasePrint: Exposing Cloud FPGA Fingerprints by Inducing Timing Faults at Runtime. (ASPLOS, Netherlands) 2025

Exploring Dual Edges of SRAM Data Remanence in SoCs: Covert Storage and Exfiltration Risks in TEE. (Hardwear.io, California) 2024

UnTrustZone: Systematic Accelerated Aging to Expose On-chip Secrets. (IEESP, San Francisco) 2024

Invisible Bits: Hiding Secret Messages in SRAM's Analog Domain. (ASPLOS, Switzerland) 2022

SRAM Has No Chill: Exploiting Power Domain Separation to Steal Onchip Secrets. (ASPLOS, Switzerland) 2022

SRAM PUF-based device authentication protocol hardware demo. (HOST, Washington DC) 2019

AWARDS

PhD Dissertation finalist (top 5)	Symposium on Hardware Oriented Security & Trust	2024
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:

- Computer Architecture letter 2025
- International Conference on Computer Design (ICCD) 2024
- Journal of Hardware and Systems Security 2023
- IEEE Internet of Things Journal 2022

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