Power PUFs: Strengthening SRAM PUFs against Fault Injection on Low-Cost IoT Devices

Abhinav Komanduri and Alexander H. Nelson
University of Arkansas
Department of Electrical Engineering and Computer Science
{abhinavk, ahnelson}@uark.edu

Introduction

Physically Unclonable Functions (PUFs) utilize manufacturing variability to generate entropic identifiers

Can be used to generate digital hardware **"fingerprints"**

Static Random Access Memory (SRAM) PUFs use the memory address and the start-up values as CRP

Attacker Model

We consider adversaries that are:

- In **physical proximity** of the target device
- In a **non-privileged** position
- Able to inject faults at a **coordinated time**

Methods

Extracted SRAM PUF and applied SECDED **Hamming ECC**

Simulated bit flipping prob.

Used CWLite to inject **crowbar faults**

Modified ESP32 PCB for target prep.

Measured HD_{intra} to show **low reliability**

Methods (Cont.)

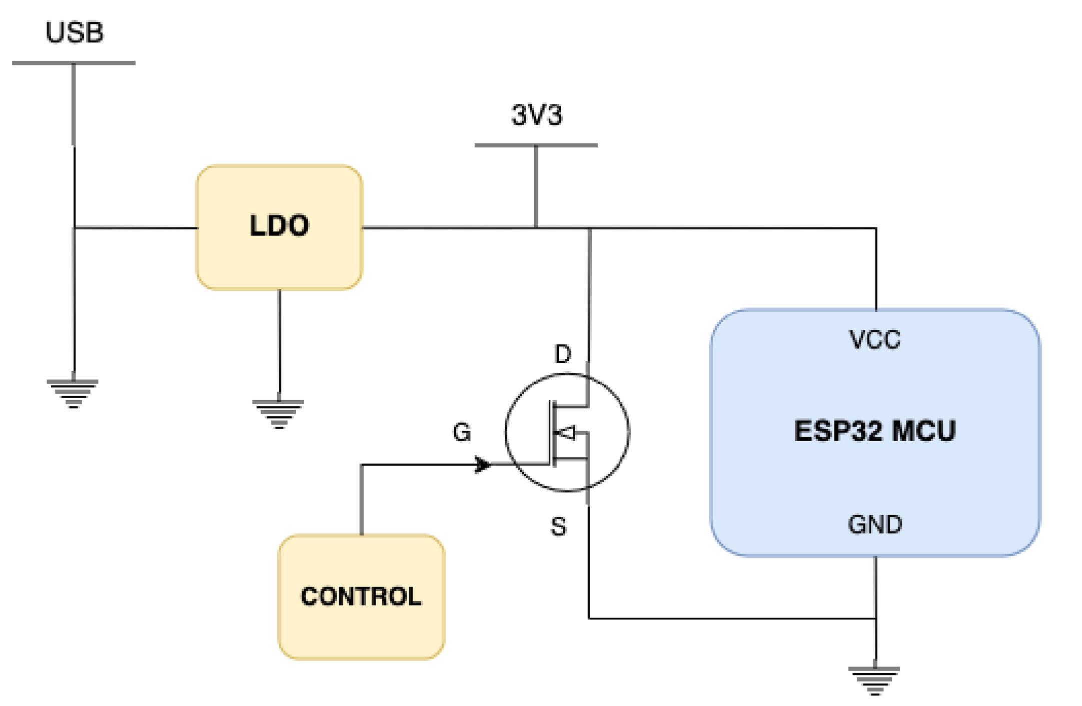

Fig 1. Block schematic of Crowbar Voltage Glitching on target devices

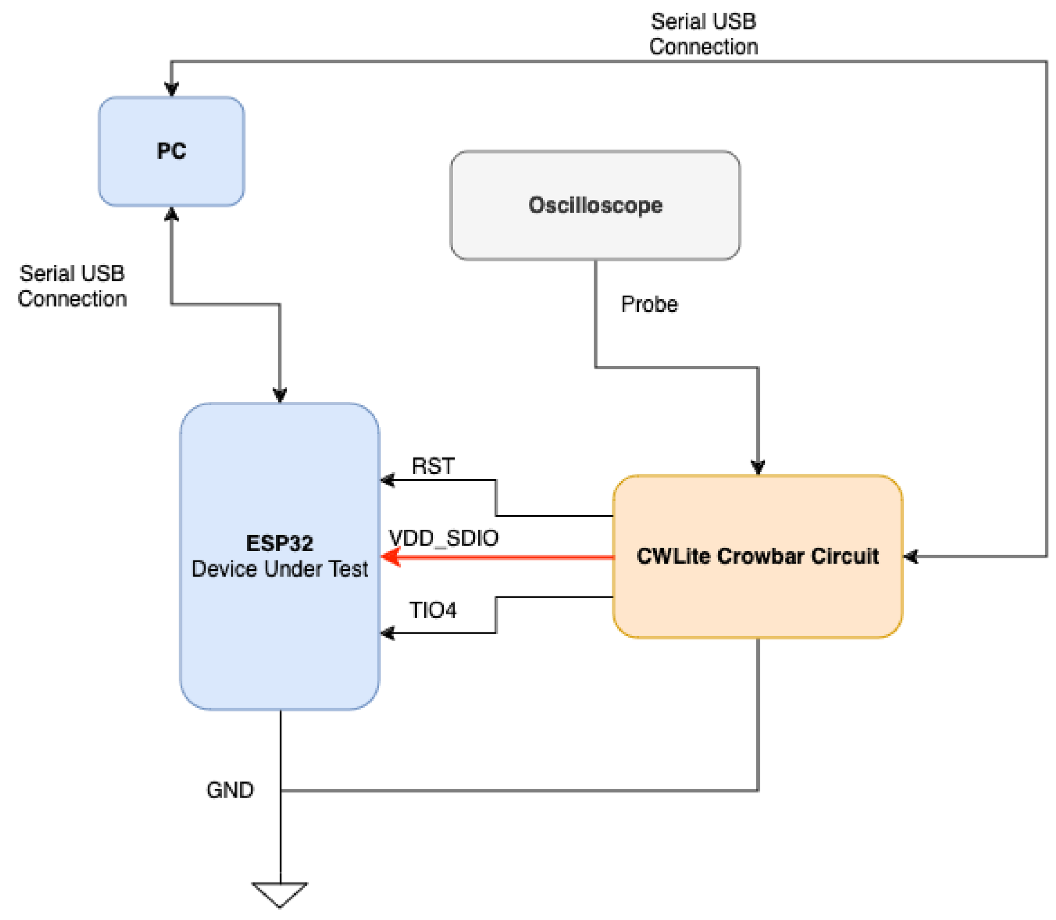

Fig 2. Setup schematic for testing with CW connected to DUT with data collected via serial communication with PC.

Preliminary Results

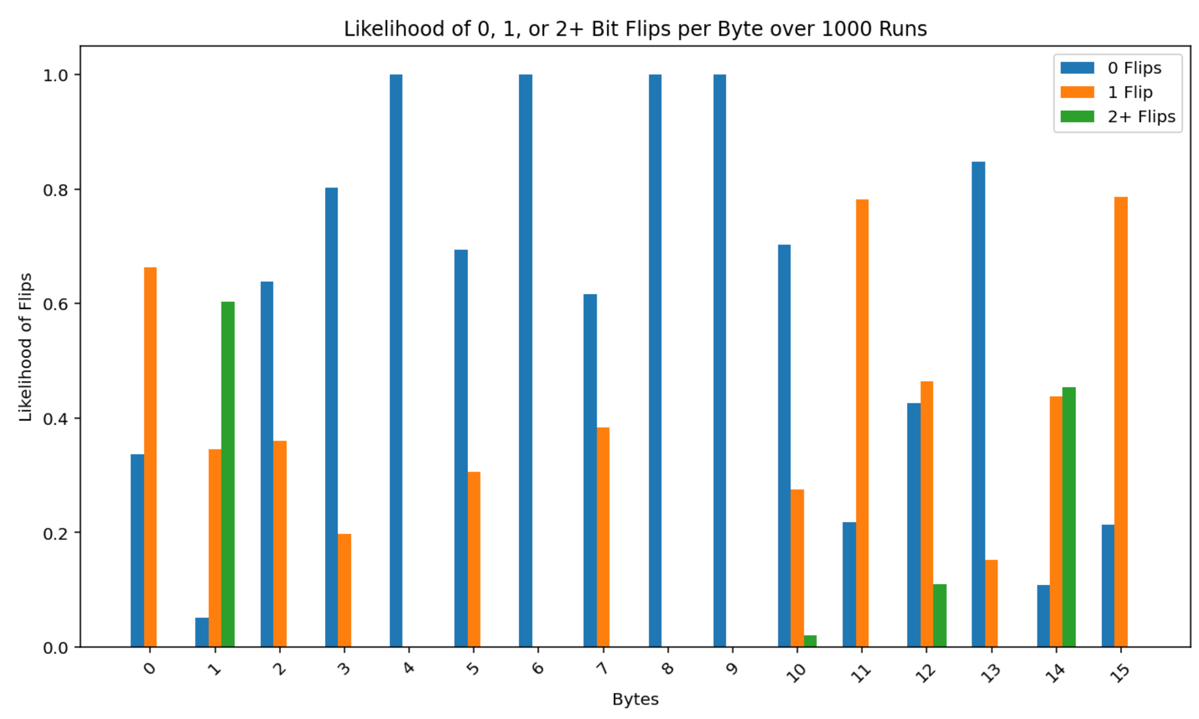

Fig 3. Simulation of bit stability for 16 bytes (128 bits) of ESP32 SRAM for PUFs

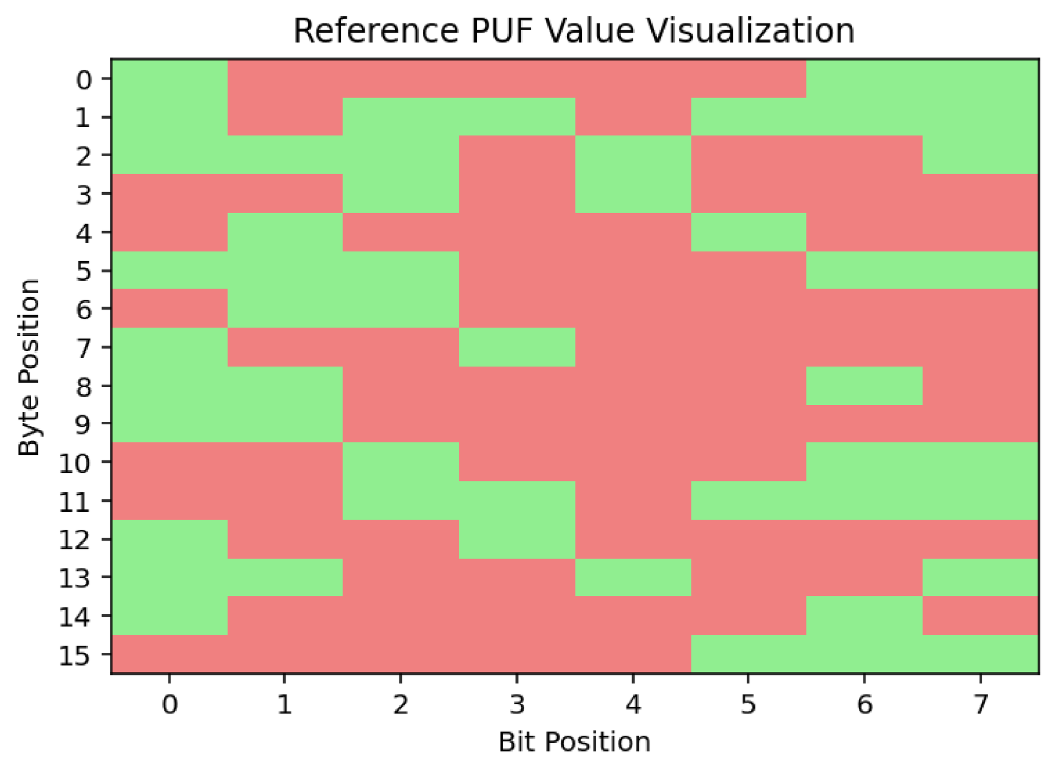

Fig 4. Visualization of reference PUF value generated where green and red represent bit states 1 or 0, respectively.

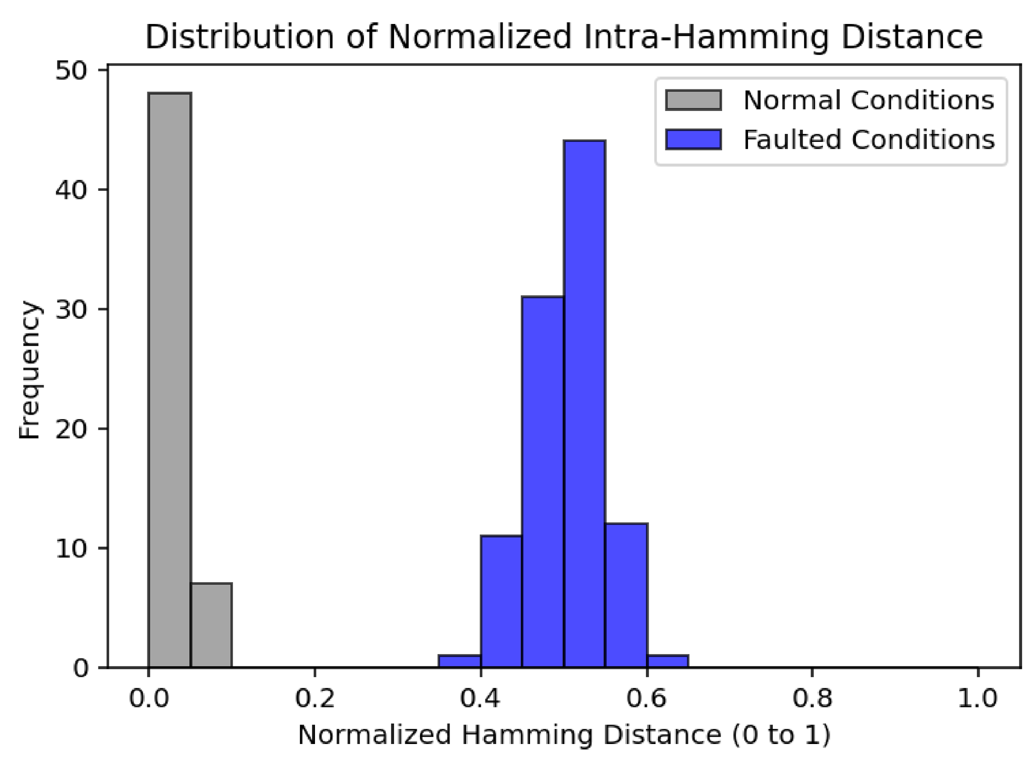

Fig 5. Distribution of HD_{intra} over 100 PUF iterations.

Discussion and Future Work

Reliability from 0.963 to 0.531 drop

Future work includes EM, clock glitching, and laser fault attacks

Alternate PUF arch. (i.e., latch, flip-flop, FPGA)

Conclusion

SRAM PUFs offer a lightweight security solution

Vulnerable to voltage fault injections, showing for mitigation strategies, alternative architectures, and robust error correction.

Acknowledgements

This work is based upon work supported by the National Science Foundation under Grant No. 2237945. This work is also supported by the University of Arkansas Honors College Research Grant and Travel Grant.

References

J. Dreyer, R. Tönjes and N. Aschenbruck, "ESPuF - Enabling SRAM PUFs on Commodity Hardware," *2023 16th International Conference on Signal Processing and Communication System (ICSPCS)*, Bydgoszcz, Poland, 2023, pp. 1-10, doi: 10.1109/ICSPCS58109.2023.10261156.

O. Stancek, "Physical unclonable functions on ESP32", Ph.D. dissertation, Czech Technical University, Prague, Czech Republic, May 5, 2022, 69 pp. [Online].

Y. Xiao, Y. He, X. Zhang, et al., "From hardware fingerprint to access token: Enhancing the authentication on IoT devices", in Proceedings 2024 Network and Distributed System Security Symposium, San Diego, CA, USA: Internet Society, 2024, isbn: 978-1-891562-93-8.4 doi: 10.14722/ndss.2024.241231. [Online].

J. v. Woudenberg and C. O'Flynn, The hardware hacking handbook: breaking embedded security with hardware attacks. San Francisco, CA: No Starch Press, 2022, 479 pp., isbn: 978-1-59327-874-8.

PerCom Pervasive Computing 2025

YOUR STORY. YOUR HONORS.