

Unlocking Hidden Secrets: Leveraging SRAM Aging Imprints for Sensitive Data Recovery

Zakia Tamanna Tisha[†], Gaines Odom[†], Biswajit Ray^{*}, and Ujjwal Guin[†]

[†]Department of Electrical and Computer Engineering, Auburn University

^{*}Department of Electrical and Computer Engineering, Colorado State University

Email: {zakia.tisha, gaines.odom, ujjwal.guin}@auburn.edu, biswajit.ray@colostate.edu

Abstract—Long-term data remanence in SRAMs can pose serious security risks when ICs containing sensitive information are discarded at the end of their operational life. Sensitive information can fall into unauthorized hands if these ICs are not sanitized properly. Traditionally, data remanence has been addressed primarily in DRAM and flash memories, while SRAMs have been overlooked due to very short retention periods. Hovanes et al. [1] demonstrated that SRAMs are vulnerable to data remanence attacks, which can retrieve static data, such as firmware and keys. Their method exploits aging-induced imprints on power-up states, enabling partial recovery by comparing aged states with the originals. Although effective, this method requires maintaining records of all initial power-up states. In this paper, we propose a data recovery approach that does not require access to prior information. Our method also exploits data imprinting in SRAMs, but instead of using actual initial power-up states, we employ controlled aging to reconstruct them. Experiments on SRAM chips storing a binary image demonstrated near-complete recovery after 12 hours of controlled aging at 100°C using 32 copies.

Index Terms—data remanence, data recovery, SRAM power-up state, process variation, aging.

I. INTRODUCTION

Driven by the rapid expansion of artificial intelligence applications, the demand for advanced and secure integrated circuits (ICs) has reached unprecedented levels. Meeting this demand has expanded the IC supply chain in both scale and complexity, introducing new interdependencies and broadening the attack surface. Hardware trust and data protection stand at the core of modern security concerns. The growing adoption of cyber-physical systems in defense, healthcare, and transportation further heightens the need to safeguard sensitive data throughout the electronics life cycle.

The electronics life cycle extends beyond design, manufacturing, ATP (assembly, test, and packaging), distribution, and deployment. Adversaries now exploit post-deployment phases, notably component harvesting from recycled systems [2], [3]. Post-retirement recycling introduces vulnerabilities such as residual data retention. Static random access memory (SRAM), though volatile, can retain sensitive information long after power-down [1], enabling attackers to reconstruct system states or bypass authentication. While sanitization standards exist for non-volatile memories (e.g., NIST SP 800-88 Rev. 1 [4]), volatile memories like SRAM, widely used in caches and FPGAs, have not received comparable attention. The assumption that SRAM loses data once powered off [5] has contributed to neglect in developing strict sanitization protocols.

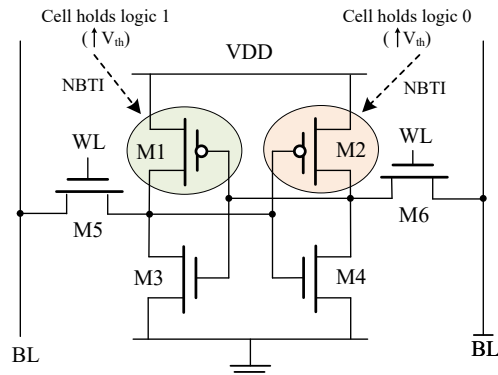


Figure 1: A 6-transistor (6T) SRAM cell under NBTI stress.

Recent studies highlight data privacy risks in aged SRAMs. Hovanes et al. [1] showed that aging biases power-up states toward historical data, enabling partial recovery after power-down. Subsequent work examined instability under temperature [6], active attack models [7], radiation-induced imprinting [8], [9], and low-temperature retention [10].

While prior work [1] has shown that aging-induced bias in power-up states can reveal historical data, it critically relies on access to the initial power-up state as a reference for comparison. In most practical scenarios, such reference states are unavailable, making this requirement a key limitation. To overcome this, we propose controlled aging to emulate initial behavior. By exploiting negative bias temperature instability (NBTI) in PMOS transistors, our method recovers the original data with near-complete accuracy. We demonstrate recovery of 20.98% from a single chip and over 99% when aggregating 32 copies. During cryptographic key recovery, even when only a single chip enables partial recovery, the overall key strength is significantly reduced, as the proposed approach explicitly identifies the locations of the recoverable bits. This knowledge provides a substantial advantage to an attacker, effectively shrinking the entropy of the underlying cryptographic key. In contrast, complete firmware reconstruction becomes feasible when multiple chips are available, as many of them retain identical or highly similar values.

II. PROPOSED APPROACH

NBTI effects are most pronounced during the early phase of device operation, where the resulting increase in V_{th} appears as aging degradation and gradually saturates under continued

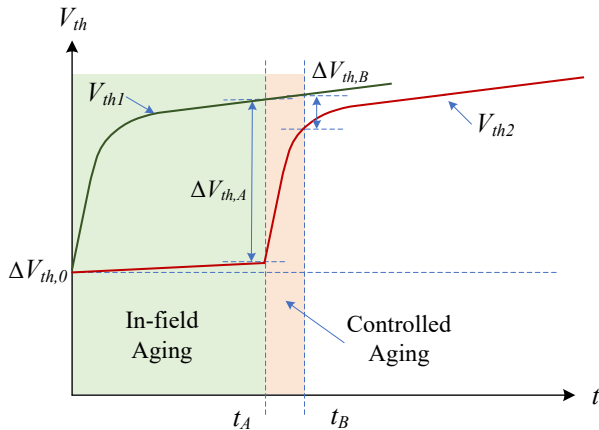


Figure 2: Variation of V_{th} of PMOS transistors of a 6T SRAM cell under in-field and controlled aging conditions.

stress [11]. In a 6T SRAM cell (see Figure 1), NBTI induces asymmetric degradation, with one PMOS transistor aging while the other remains close to its fresh state, depending on the stored logic value. For example, when the cell stores a logic ‘1’, transistor M_1 undergoes aging, whereas M_2 remains largely unaffected. This asymmetric degradation leaves a persistent data imprint in the cell, biasing subsequent power-up states toward the value stored during long-term operation [12].

Figure 2 illustrates asymmetric aging behavior, where the y-axis denotes the threshold voltage (V_{th}) of the two PMOS transistors and the x-axis denotes the aging time, t , with the green and red curves corresponding to transistors M_1 and M_2 , respectively. Under prolonged logic ‘0’ gate bias during in-field operation, the V_{th} of M_1 (V_{th1}) increases and saturates at time t_A , while the V_{th} of M_2 (V_{th2}) remains near its initial value, increasing the imbalance between the two transistors. We propose controlled aging to restore the initial imbalance between the PMOS transistors. In this process, the previously unstressed M_2 is deliberately aged by alternating all-1 and all-0 patterns at fixed intervals until V_{th2} also reaches saturation like V_{th1} . As shown in the figure, this approach approximately restores the initial V_{th} difference ($\Delta V_{th,0}$) by achieving $\Delta V_{th,B}$ at time t_B , thereby reestablishing conditions close to the IPS. Consequently, the cell reflects its inherent V_{th} difference, and the aging-induced imprint is removed, explaining why the approximation behaves similarly to the actual IPS.

The proposed recovery approach without using IPS begins by measuring the final power-up state (FPS) of each device under test. Controlled aging is then applied by stressing the cells with all 1s and 0s for fixed durations to yield the approximate initial power-up state (AIPS). The FPS and AIPS are compared to achieve partial data recovery. Finally, a majority voting is employed across devices to improve recovery using Algorithm 1 in [1].

III. EXPERIMENTAL RESULTS

To validate the proposed approach, we conduct an experiment on 23A1024-SN serial SRAM chips. Each 1-Mbit chip is logically partitioned into 16 segments, all of which are treated as independent chips. Binary test images are generated using custom Python scripts and written to

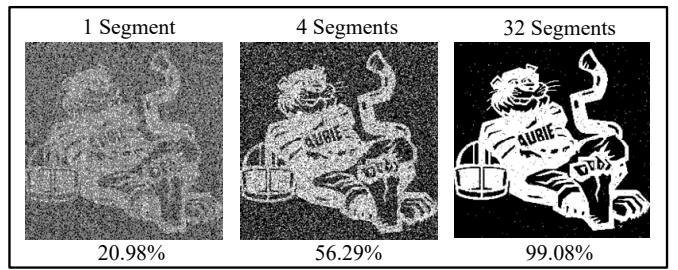


Figure 3: Data recovery results for the proposed data recovery approach (without IPS).

all SRAM segments, followed by accelerated aging using a Temprotronic ThermoSpot system at $100^\circ C$ (within the operating temperature range of the selected ICs). A Raspberry Pi is used to program the chips and collect post-aging data.

The results of our experiments are presented in Figure 3. Two chips with aging degradation are used to evaluate the proposed approach. We obtain a total number of 32 segments from two aged chips. At first, twenty power-up states are recorded to form the FPS dataset. The segments then undergo controlled aging under thermal stress at $100^\circ C$ for 2 hours. All memory addresses are first written with all 1s and stressed at $100^\circ C$ for 2 hours. The step is followed by overwriting with 0s and repeating the aging procedure for another 2 hours. An all-1 followed by an all-0 stress pattern defines one cycle. The cycle is repeated three times to ensure uniform degradation, resulting in a total duration of 12 hours. After aging, twenty power-up states are recorded again to form the AIPS dataset, which is then compared with the FPS for partial data recovery. Finally, majority voting is applied across the chips, with segments randomly selected from the 32 available. With a single segment, the recovered image achieves partial recovery of 20.98%. Although recovery is partial with a single chip, it can substantially reduce adversarial uncertainty in key retrieval, lowering the number of unknown bits in AES from 128 to approximately 100. This demonstrates that even limited visibility into stored states diminishes the intended security strength of keys and directly weakens resistance to key-recovery attacks [13]. Using four segments improves recovery to 56.29%, and majority voting across all 32 segments achieves 99.08%, signifying that full firmware reconstruction is achievable.

IV. CONCLUSION

The proposed approach shows that aging-induced degradation in SRAMs can be systematically exploited to recover stored data without requiring initial power-up states. Controlled aging enables partial recovery even from a single device, reducing key-bit uncertainty and weakening resistance to key-recovery attacks. Aggregating results across multiple devices achieves near-complete firmware reconstruction, making full recovery a realistic threat for end-of-life SRAM-based systems.

ACKNOWLEDGMENT

This work was supported by the National Science Foundation under Grant Numbers CNS-2423248 and CNS-2423249.

REFERENCES

- [1] J. Hovanes, Y. Zhong, and U. Guin, "Beware of Discarding Used SRAMs: Information is Stored Permanently," in *IEEE Physical Assurance and Inspection of Electronics (PAINE)*, pp. 1–7, 2022.
- [2] U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, vol. 102, pp. 1207–1228, Aug 2014.
- [3] M. Tehranipoor, U. Guin, and D. Forte, *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer International Publishing, 2015.
- [4] A. R. Regenscheid, L. Feldman, G. A. Witte, *et al.*, "NIST Special Publication 800-88, Revision 1: Guidelines for Media Sanitization," 2015.
- [5] 2014. NSA/CSS Storage Device Sanitization Manual, NSA/CSS Policy Manual 9-12, 2014, <https://www.nsa.gov/portals/75/documents/resources/everyone/media-destruction/storage-device-declassification-manual.pdf>.
- [6] J. Mahmood and M. Hicks, "SRAM Has No Chill: Exploiting Power Domain Separation to Steal On-Chip Secrets," in *Proceedings of the 27th ACM International Conference on Architectural Support for Programming Languages and Operating Systems*, pp. 1043–1055, 2022.
- [7] J. Mahmood and M. Hicks, "UnTrustZone: Systematic Accelerated Aging to Expose On-chip Secrets," in *2024 IEEE Symposium on Security and Privacy (SP)*, pp. 4107–4124, IEEE, 2024.
- [8] U. Surendanathan, A. S. Vellankanni, A. Milenkovic, U. Guin, and B. Ray, "Ionizing Radiation-Induced Data Imprinting Effects in SRAM Arrays," *IEEE Transactions on Nuclear Science*, 2025.
- [9] J. Cui, Q. Zheng, Y. Li, and Q. Guo, "Impact of High TID Irradiation on Stability of 65 nm SRAM Cells," *IEEE Transactions on Nuclear Science*, vol. 69, no. 5, pp. 1044–1050, 2022.
- [10] F. Hoque, I. Halseide, A. Milenkovic, and B. Ray, "Data Remanence Vulnerabilities in Commercial SRAM at Low Temperature," in *2024 IEEE Physical Assurance and Inspection of Electronics (PAINE)*, pp. 1–7, IEEE, 2024.
- [11] S. Mahapatra, N. Goel, S. Desai, S. Gupta, B. Jose, S. Mukhopadhyay, K. Joshi, A. Jain, A. Islam, and M. Alam, "A comparative study of different physics-based nbt1 models," *IEEE transactions on electron devices*, vol. 60, no. 3, pp. 901–916, 2013.
- [12] U. Guin, W. Wang, C. Harper, and A. D. Singh, "Detecting Recycled SOCs by Exploiting Aging Induced Biases in Memory Cells," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 72–80, 2019.
- [13] E. Barker and Q. Dang, "Nist special publication 800-57 part 1, revision 4," *NIST, Tech. Rep.* vol. 16, p. 51, 2016.