REAP-NVM: Resilient Endurance-Aware NVM-based PUF against Learning-based Attacks

Hassan Nassar*, Ming-Liang Wei†, Chia-Lin Yang†, Jörg Henkel*, Kuan-Hsun Chen‡

*Karlsruhe Institute of Technology (KIT), Chair for Embedded Systems (CES), Germany
†National Taiwan University, Taiwan ‡University of Twente, the Netherlands
*{nassar, henkel}@kit.edu, †d04943004@ntu.edu.tw, †yangc@csie.ntu.edu.tw, ‡k.h.chen@utwente.nl

***Abstract*—NVM-based PUFs offer secure authentication and cryptographic applications by exploiting NVMs' MLC to generate diverse, ML-attack-resistant responses. Yet, frequent writes degrade these PUFs, lowering reliability and lifespan. This paper presents a model to assess endurance effects on NVM PUFs, guiding the creation of more robust PUFs. Our novel NVM PUF design enhances endurance by evenly distributing writes, thus mitigating cell stress, achieving a $62\times$ improvement over current solutions while preserving security against learning-based attacks.**

***Index Terms*—Non-Volatile Memory, Physical Unclonable Functions, Security, Endurance**

I. Introduction

Physical Unclonable Functions (PUFs) are vital in security systems, creating unique identifiers through intrinsic device variations and using a challenge-response protocol. A trusted third party initially conducts an enrollment phase, where challenge-response pairs (CRPs) are collected for PUF authentication. PUFs produce unique, random responses to identical challenges, preventing cloning. However, PUFs are vulnerable to machine learning attacks, where attackers gather enough CRPs to predict responses to new challenges, compromising PUF security. Attackers collect CRPs through means such as man-in-the-middle attacks during deployment, unlike the controlled third-party enrollment.

Recent studies on NVM-based PUFs show they mitigate learning-based attacks by exploiting NVM cells' gradual state changes via iterative pulsing, complicating ML predictions and enhancing resistance [1], [2]. Despite this, NVMs face durability issues due to repeated writes, impacting their quality and reliability. While wear leveling helps distribute writes when NVM is used as main memory [3], it doesn't prevent changes in individual cell behavior, crucial for reproducible responses of PUFs. Such changes lead to PUF noise, causing mismatches between deployment and enrollment responses, resulting in authentication failures. Therefore, addressing endurance issues is essential for the practical use of NVM-based PUFs.

Our Contributions: Most works on NVM-based PUFs consider general solutions for delay-based silicon PUFs that would work for NVM-PUFs. However, since these PUFs are significantly different, such an assumption must be examined. To the best of our knowledge, this is the first work to address the endurance of NVM-based PUFs to address this pressing issue.

This work is supported in part by the German Research Foundation (DFG) as part of the priority program "SPP 2377: Disruptive Memory Technologies" under project: (ARTS-NVM) and in part by the German Federal Ministry of Education and Research (BMBF) through grant 01IS23066 as part of the Software Campus Project "HE-Trust". We thank DFG (Project Number: 405422836, NVM-OMA).

II. NVM-PUF Endurance Analysis

We developed a Markov chain-based endurance analysis to predict PUF failure probability after N challenges. The probabilities are updated via a transition matrix applied to the state vector, starting with a one-hot vector in the "Receive Challenge" state. The system converges to a terminal state, ceasing updates when this state's probability is $1 - 10^{-5}$. For each state s, the probability $P_m(t, s)$, shows the likelihood of being visited at iteration t, informing the distribution of accumulated visit times.

To assess the endurance of the PUF system, it is crucial to calculate the cumulative set/reset operations. We first determine the visit count distribution for each state during a challenge, then derive the final set/reset state distribution. This is done by converting recorded transition probabilities into total visit counts.

We treat the set and reset counts for a challenge as random variables from the mentioned distribution, allowing us to determine these counts after N challenges. The total set and reset operations after N challenges are found by summing N independent random variables from each challenge's distribution. This gives us the time-varying distribution of these operations, helping to determine the system's lifetime.

The cycling endurance of a PCM cell is 1000 cycles [4]. Any cell exceeding this is considered dead. A PUF with M cells is dead when 15% of its cells are dead, a common reliability threshold [1]. We aim to calculate the PUF failure probability using these definitions and the set and reset operation distribution. For each challenge, a single cell is dead if its set and reset operations exceed the endurance limit. Each cell operates independently, so the distribution of dead cells among a set of cells follows a binomial distribution. Lastly, we determine the probability of the PUF being dead by summing the probabilities of having k dead cells.

III. Endurance-Aware PUF: REAP-NVM

REAP-NVM uses NVM's multilevel cells to thwart ML modeling attacks, providing a strong PUF with many CRPs for authentication and key generation. It limits endurance

978-3-9826741-0-0/DATE25/© 2025 EDAA

degradation by writing to one cell pair per challenge, reducing cell aging without sacrificing security. Inspired by interpose PUF [5], it improves security by changing a single challenge bit with minimal overhead.

Our PUF design is an Arbiter PUF (APUF) with 128 stages, incorporating NVM cells between switches. Each challenge has three parts: a 128-bit value controlling switch configurations, 7 bits selecting an NVM cell pair for configuration, and 3 bits setting a resistance level with 8 options [6]. This resistance variation complicates ML model predictions of REAP-NVM behavior. Only one cell pair is adjusted per challenge, with a $\frac{1}{128}$ chance of being set, a $\frac{1}{128}$ chance of needing a reset from prior use, and a $\frac{126}{128}$ chance of remaining unaffected, distributing usage evenly and minimizing damage.

We then evaluate REAP-NVM to know whether it achieves desirable behavior or not. We build a SPICE/Matlab simulation environment using PCM and get the model parameters from [1]. We simulate two REAP-NVM PUFs and generate 102,400 CRPs from each of them. Moreover, we simulate a normal APUF with 128 stages to compare against it as a baseline.

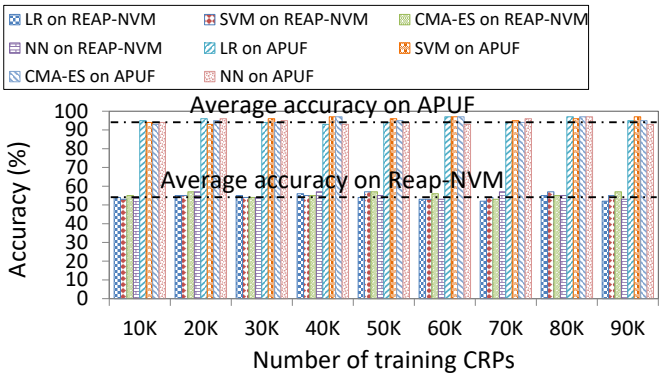

Figure 1. Performance of learning-based attacks on REAP-NVM

Next, we evaluate the security of REAP-NVM against learning-based attacks. We use the same attacks as those from [7]. We increase the training set from 10,000 to 90,000 CRPs with a step 0f 10,000 CRPs. As a baseline, we compare the prediction accuracy with APUF. As Fig. 1 shows, REAP-NVM remains resilient to learning-based attacks with a prediction accuracy of around 55%, that is, in a range similar to flipping a coin. However, APUF is easily predictable, having already been in the range of 95% from the lowest training dataset.

After ensuring that REAP-NVM is unique, uniform, and mitigates the learning-based attacks, we analyze its endurance in comparison to the state-of-the-art. In addition to REAP-NVM, we also analyze A-MPUF [2] and ICR-PUF [8], Light-PUF [9], and PCM-PUF [10].

Based on the probabilities of the lifetime for PUFs we evaluate the half-life of each PUF, i.e., when the probability of PUF being dead is 50%. Figure 2 shows the half-life evaluation. ANV-PUF [1] has a very low half-life, making it barely usable. Other state-of-the-art PUFs are better, but not comparable to REAP-NVM. Overall, compared to the next best PUF, REAP-NVM has 62× improvement.

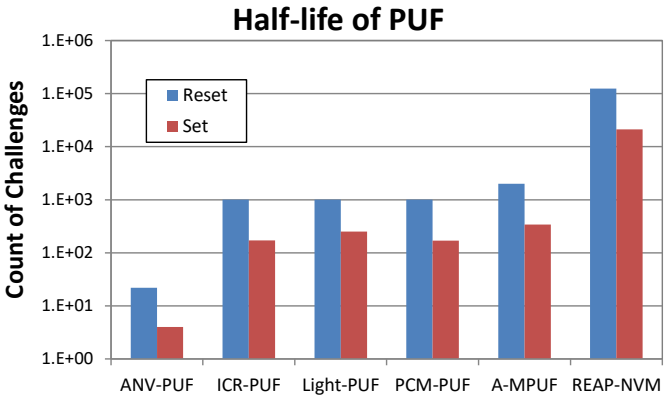

Figure 2. Half-Life of PUF affected by Set and Reset

IV. Conclusions

NVM technologies offer a promising avenue for designing PUFs to counter learning-based attacks. A key issue with NVM-based PUFs is their endurance problem; frequent writes cause wear and reduce reliability and lifespan. We tackle these issues by providing a model to predict endurance degradation and exploring advanced PUF designs. Our new design, REAP-NVM, reduces learning-based attacks and addresses endurance issues. Experiments show REAP-NVM improves endurance over the state-of-the-art without compromising security.

References

[1] H. Nassar *et al.*, "ANV-PUF: Machine-Learning-Resilient NVM-Based Arbiter PUF", *ACM Trans. Embed. Comput. Syst.*, vol. 22, no. 5s, sep 2023.

[2] R. Ali *et al.*, "A Reconfigurable Arbiter MPUF With High Resistance Against Machine Learning Attack", *IEEE Transactions on Magnetics*, vol. 57, no. 10, pp. 1–7, 2021.

[3] N. Hölscher *et al.*, "Memory Carousel: LLVM-Based Bitwise Wear-Leveling for Non-Volatile Main Memory", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 42, no. 8, pp. 2527–2539, 2023.

[4] A. Anand *et al.*, "Cycle test stability and corrosion evaluation of phase change materials used in thermal energy storage systems", *Journal of Energy Storage*, vol. 39, p. 102664, 2021.

[5] P. H. Nguyen *et al.*, "The Interpose PUF: Secure PUF Design against State-of-the-art Machine Learning Attacks", *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2019, no. 4, p. 243–290, Aug. 2019. [Online]. Available: https://tches.iacr.org/index.php/TCHES/article/view/8351

[6] F. Zahoor *et al.*, "Resistive Random Access Memory (RRAM): an Overview of Materials, Switching Mechanism, Performance, Multilevel Cell (MLC) Storage, Modeling, and Applications", *Nanoscale Research Letters*, vol. 15, no. 1, p. 90, Apr 2020.

[7] L. Wu *et al.*, "FLAM-PUF: A Response–Feedback-Based Lightweight Anti-Machine-Learning-Attack PUF", *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 41, no. 11, pp. 4433–4444, 2022.

[8] L. Zhang *et al.*, "Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 6, pp. 921–932, 2014.

[9] B. Hajri *et al.*, "A lightweight reconfigurable rram-based puf for highly secure applications", in *2020 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)*. Esrin, Italy: IEEE, 2020, pp. 1–4.

[10] L. Zhang *et al.*, "Leakage-resilient memory-based physical unclonable function using phase change material", in *2014 International Carnahan Conference on Security Technology (ICCST)*. Rome, Italy: IEEE, 2014, pp. 1–6.