University of Passau

Faculty of Computer Science and Mathematics

Chair for Secure Intelligent Systems

M.Sc Mobile and Embedded Systems

Machine Learning Attack Resistant DRAM - Based Physically unclonable functions

Reshmi Suragani
suraga01@ads.uni-passau.de

Supervisor: Prof. Dr. Elif Bilge Kavun
Date: November 18, 2020

1 Introduction

Over the last decades, there has been an exponential increase in the usage of smart devices. These hardware devices often contain secure information [Her+14]. Physical Unclonable Function (PUF) is the most powerful way to secure semiconductor devices from attacks like data tampering or access to a secret key. PUFs generate random keys that can be used in the generation of cryptographic keys, based on the device's manufacturing variations. They act as a digital fingerprint which serves as an identifier. PUFs use Challenge-Response Pairs (CRP) for device authentication. Based on CRPs, PUFs can be classified as strong and weak PUFs. The number of unique CRPs is the major difference between a strong PUF and a Weak PUF. Usually a strong PUF consists of a large number of CRPs, whereas a weak PUF consists of one or few CRPs [Her+14]. Memory-Based PUFs have gained attention over a period of time as they are present in almost every embedded device[HBF08; Sut+17; Kim+18]. Memory components like SRAM, DRAM and Flash can be utilised for secure key generation. They are also cost-effective and does not need any additional hardware.

Dynamic random-access memory (DRAM) cell is designed using a capacitor and two transistors. Practically every cell should be similar, but they exhibit differences among cells because of their manufacturing variations [Teh+15]. The cells are arranged as a two-dimensional matrix. The bit value stored in the cell is based on the charging status of the capacitor. It denotes logic '1' when the capacitor is charged, and logic '0' once it is discharged. To prevent data getting faded away due to leakage of capacitor over a time, most of the devices are integrated with the self-refresh module. The self refresh rate is disabled for DRAM PUF and the cells are initialized to value '1' and few cells leak to '0' after some time [SRR16]. This randomness can be used to construct a fingerprint.

The use of the DRAMs remanence property is another possible technique. DRAM can retain the data for a few minutes even without power supply for long intervals at a room temperature. In this PUF method, power is switched off rather than turning of refresh rate [Gut01]. The DRAM PUF is an example of a strong PUF as it contains more number of challenge-response pairs [Tan+17].

While PUF is the most promising approach to device authentication and cryptographic algorithms, recent studies have shown that even PUFs are vulnerable to attacks ranging from semi-invasive to non-invasive. The most common non-invasive attack is machine learning [Gan+16]. By training a machine learning model with a large number of challenge-response pairs, the model can accurately predict the response. Studies have shown that even strong PUFs, such as Arbiter PUFs, can be targeted using a machine learning model [Rüh+10]. In this study, we will investigate DRAM PUF vulnerability against machine learning attacks, as memory-based PUF considered to be powerful enough against attacks [Rüh+10].

2 Problem Statement

The goal of the thesis is to investigate whether DRAM PUF is robust against machine learning attacks [PKT19]. To achieve this, we create a Machine Learning model by using DRAM startup values as input data. The following hypothesis are evaluated

a) The data is collected from DRAM PUF. The dataset is split into training data and test data by using K-fold cross-validation.

b) The dataset is evaluated on a different machine learning algorithms like Support Vector Machine (SVM), Logistic Regression (LR), Naive Bayes (NB) and Convolutional Neural Network (CNN).

c) Finally, we will check whether the responses of DRAM can be predicted by a machine learning model.

2.1 Implementation

Fatemeh et al. tested on-board MIRA P3R1GE3EGF G8E DDR2 DRAM on the Diligent Atlys board to test machine learning attacks. But we will test the hypothesis on 1 MBit Hitachi HM51100AL CMOS DRAM in DIP package. The DRAM is wired to the Xilinx Spartan-6 FPGA on the Digilent Atlys board to collect data. We are planning to use Python programming language in Google Colab platform for machine learning algorithms as mentioned in the previous section.

Bibliography

[Gan+16] Fatemeh Ganji et al. "Strong machine learning attack against PUFs with no mathematical model". In: *International Conference on Cryptographic Hardware and Embedded Systems*. Springer. 2016, pp. 391–411.

[Gut01] Peter Gutmann. "Data Remanence in Semiconductor Devices." In: *USENIX Security Symposium*. 2001, pp. 39–54.

[HBF08] Daniel E Holcomb, Wayne P Burleson, and Kevin Fu. "Power-up SRAM state as an identifying fingerprint and source of true random numbers". In: *IEEE Transactions on Computers* 58.9 (2008), pp. 1198–1210.

[Her+14] C. Herder et al. "Physical Unclonable Functions and Applications: A Tutorial". In: *Proceedings of the IEEE* 102.8 (2014), pp. 1126–1141. DOI: 10.1109/JPROC.2014.2320516.

[Kim+18] Jeremie S Kim et al. "The DRAM latency PUF: Quickly evaluating physical unclonable functions by exploiting the latency-reliability tradeoff in modern commodity DRAM devices". In: *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*. IEEE. 2018, pp. 194–207.

[PKT19] Anugayathiri Pugazhenthi, Nima Karimian, and Fatemeh Tehranipoor. "DLA-PUF: deep learning attacks on hardware security primitives". In: *Autonomous Systems: Sensors, Processing, and Security for Vehicles and Infrastructure 2019*. Vol. 11009. International Society for Optics and Photonics. 2019, 110090B.

[Rüh+10] Ulrich Rührmair et al. "Modeling attacks on physical unclonable functions". In: *Proceedings of the 17th ACM conference on Computer and communications security*. 2010, pp. 237–249.

[SRR16] S. Sutar, A. Raha, and V. Raghunathan. "D-PUF: An intrinsically reconfigurable DRAM PUF for device authentication in embedded systems". In: *2016 International Conference on Compliers, Architectures, and Sythesis of Embedded Systems (CASES)*. 2016, pp. 1–10. DOI: 10.1145/2968455.2968519.

[Sut+17] Soubhagya Sutar et al. "D-PUF: An intrinsically reconfigurable DRAM PUF for device authentication and random number generation". In: *ACM Transactions on Embedded Computing Systems (TECS)* 17.1 (2017), pp. 1–31.

[Tan+17] Q. Tang et al. "A DRAM based physical unclonable function capable of generating >1032 Challenge Response Pairs per 1Kbit array for secure chip authentication". In: *2017 IEEE Custom Integrated Circuits Conference (CICC)*. 2017, pp. 1–4. DOI: 10.1109/CICC.2017.7993610.

[Teh+15] Fatemeh Tehranipoor et al. “DRAM Based Intrinsic Physical Unclonable Functions for System Level Security”. In: *Proceedings of the 25th Edition on Great Lakes Symposium on VLSI*. New York, NY, USA: Association for Computing Machinery, 2015. URL: https://doi.org/10.1145/2742060.2742069.