

DEPS - <https://deps.scch.at>
Dependable Production Environments with Software Security

Host: SCCH, www.scch.at

Programme: COMET – Competence Centers for Excellent Technologies

Programme line: COMET-Module



LEVERAGING ROWHAMMER FOR PHYSICALLY UNIQUE AND NON-TAMPERABLE DEVICE IDENTIFICATION

ENSURING DEVICE SECURITY AND INTEGRITY THROUGH INNOVATIVE HARDWARE-BASED IDENTIFICATION

In the context of industrial control systems, ensuring the security and integrity of devices is crucial. Traditional methods often require additional hardware, which is not feasible for legacy and embedded systems. The challenge is to develop a cost-effective, secure method for device identification that can be implemented on existing hardware without the need for additional components. By providing a unique and non-tamperable identifier, the method could serve as a trust anchor for secure device authentication, key generation, and binding software to specific hardware, preventing unauthorized access and software piracy.

Solution

We have developed a novel approach using the Rowhammer effect on DRAM, which is a type of memory

widely used, to implement a Physically Unclonable Function (PUF). Our method leverages the unique bit flip patterns induced by Rowhammer to generate a statistical fingerprint of each device, providing a secure and non-tamperable identifier. Our approach operates in two phases, depicted in Figure 1:

During the *enrollment phase*, we induce bit flips in the DRAM to create a unique fingerprint, which is stored for future reference. The Mahalanobis distance is used to analyze the distribution of bit flips, enhancing identification accuracy. In the *identification phase*, the device is re-identified by inducing bit flips and comparing the new fingerprint with the stored reference using the Mahalanobis distance. This ensures accurate and robust identification by filtering out noise and focusing on consistent patterns.

SUCCESS STORY 2024/1

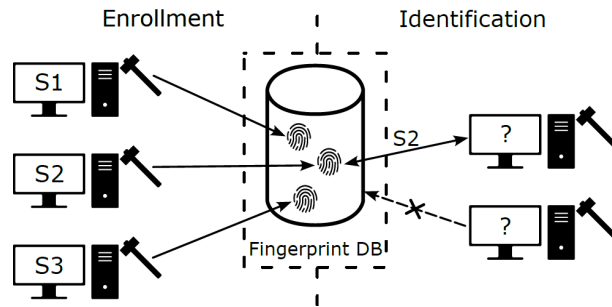


Figure 1: The two phases of our approach.

Key Innovations

Our solution innovates on prior device identification mechanisms in several aspects:

- **Rowhammer PUFs:** Using the inherent properties of DRAM to create unique, unclonable identifiers.
- **Statistical Fingerprinting:** Employing the Mahalanobis distance to compare error distributions, enhancing identification accuracy.
- **Legacy System Compatibility:** Demonstrating the method's applicability on widely available consumer PCs with DDR4 memory, ensuring broad compatibility.

Scientific Contributions

Our research [1,2] contributes the following to the state of the art:

- **Empirical Analysis of Bit Flips:** We provide an in-depth empirical analysis of the repeatability and distribution of bit flips caused by Rowhammer on DDR4 memory. This analysis is crucial for understanding the stability and reliability of the generated PUFs.
- **Overcoming Noise in Bit Flips:** One of the significant challenges we address is the noise in bit flips, which can affect the reliability of PUFs. We introduce the use of the Mahalanobis distance, a statistical measure that considers the variance and covariance of the bit flip distributions. This approach allows for more accurate and robust identification by filtering out noise and focusing on the consistent patterns unique to each device.

- **System Identification:** Our method not only identifies individual DRAM modules but also the systems they are used in. This is possible due to the influence of other hardware components, such as the memory controller, on the bit flip patterns. This capability ensures that the PUF cannot be transferred to another system simply by swapping memory modules.
- **Practical Implementation:** We demonstrate the practical implementation of Rowhammer-based PUFs on widely available consumer PCs, highlighting our method's feasibility and applicability to existing hardware without the need for additional components.

Impact

This breakthrough offers a significant advancement in device security, particularly for industrial control systems. By enabling secure device identification without additional hardware, it provides a cost-effective solution to protect against unauthorized access and tampering. Our method's compatibility with legacy systems ensures it can be easily integrated into existing infrastructures, enhancing overall security.

Related DEPS Publications

[1] B. Fischer, D. Dorfmeister, H. Lampesberger, and E. Hermann. "Leveraging Rowhammer for Physically Unique and Non-tamperable Device Identification." ISM 2024.

[2] B. Fischer. "Design of a Rowhammer-Based Unique Hardware Identification Mechanism." Master's thesis, University of Applied Sciences Upper Austria, 2023.

Contact: Juliana Küster Filipe Bowles, DEPS Coordinator, SCCH, T +43 50 343 900, juliana.bowles@scch.at

Consortium:

scch {
software
competence
center
hagenberg



RI
Research Institute
Cyber Defence
Universität der Bundeswehr München

EPFL

JYU
LIT Secure and Correct
Systems Lab

Symflower

framag

SIGMATEK

Plasser & Theurer

KU LEUVEN

EMBEDDED SYSTEMS LAB
FH 00 / CAMPUS HAGENBERG

pwc

Federal Ministry
Republic of Austria
Climate Action, Environment,
Energy, Mobility,
Innovation and Technology

Federal Ministry
Republic of Austria
Digital and
Economic Affairs



Austrian Research Promotion Agency
Sensengasse 1, A-1090 Vienna
P +43 (0) 5 77 55 - 0
office@ffg.at
www.ffg.at