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

Type of project: Strategic research project, 4 years, Start: Jan 2022

PROTECTION THROUGH INTRINSIC MEMORY FEATURES

EXPLORING TEMPERATURE LIMITS OF SRAM-BASED PHYSICAL UNCLONABLE FUNCTIONS

A major part of the DEPS project is the securing of individual software components, so that the software itself can determine if it is running on its designated target machine. It should be discernable if the software is executed on hardware that is simply using the same components or on the original machine.

The typical approach to determine this is the use of a physical unclonable function (PUF). These PUFs often use hardware manufacturing tolerances inherent in all semiconductors to generate a unique fingerprint of a device. On desktop systems, DRAM is available in abundance and a PUF can be extracted from it by using the RowHammer procedure. In this procedure bit flips are forced in the DRAM. The pattern of the bit flips varies between DRAM chips like fingerprints between humans.

On embedded systems, DRAM is not present most of the time, and if it is, the feasibility of the RowHammer procedure to produce bit flips is reduced. This is due to the lower frequency of memory reads that can be achieved on an embedded system [2].

With RowHammer PUFs being a suboptimal solution to implemented PUFs on embedded systems, SRAM PUFs were evaluated for this purpose instead [3]. SRAM PUFs use the initial value of SRAM cells after power-up to generate a unique fingerprint. The benefits of using an SRAM PUF on embedded systems is twofold: nearly every embedded system contains SRAM and the frequency restrictions do not impact the ability to create a fingerprint, as the PUF is only dependent on the initial state of the SRAM.

In our research [1] we compared two similar on-board SRAMs from the same vendor and evaluated

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

Federal Ministry
Republic of Austria
Labour and Economy

FFG
Promoting Innovation.

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

their usability for PUFs, especially regarding different temperature ranges.

Methodology

The three main factors based on which we can evaluate the usability of a PUF are the reproducibility of a reference fingerprint of the PUF, the reliability of the PUF and the uniqueness of the PUF. To gather significant information about these properties, we collected data from 14 chips for each of the compared SRAMs. The fingerprint was taken at three different temperatures: 10°C, 25°C and 50°C. To ensure consistent temperatures at each measurement point, a self-made low-cost climate chamber was used. For each chip and temperature, a total of 50 measurements was taken.

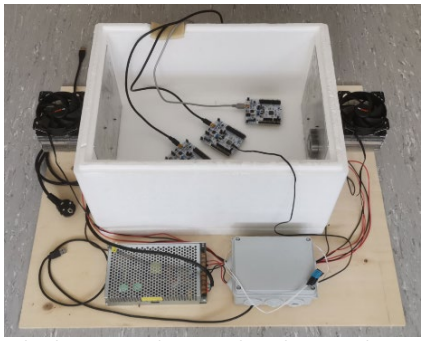

Fig. 1: The low-cost climate chamber used to ensure a stable temperature.

Results

Based on our measurements we could determine that the reproduction of a reference fingerprint taken at 25°C relies heavily on the specific model used, with one model showing a Hamming distance of up to 12 % to the reference at 50°C. The other model only showed a Hamming distance of up to 7 % to the reference at 50°C. At 10°C the Hamming distance to the reference was generally below 8 % for both models and at the same temperature as the reference measurement of 25°C it was at about 4-6 %.

The absolute reliability of the PUF denotes the noise between measurements under the same operating conditions. This was observed to be lowest under colder operating conditions, with a maximum Hamming distance of 5 % between samples on both SRAM models. With increasing temperature one model proofed to be much less reliable with a Hamming distance of more than 12 % while the other model stayed below 8 % at 50°C.

The uniqueness – the difference between the fingerprints of different chips of the same model – was higher on the model showing lower reliability. Optimal uniqueness is at a value of 50 %. The less reliable model achieved this almost perfectly, while the more reliable model has a uniqueness of around 48 %. Interestingly, the less reliable model offered a much higher variance in uniqueness with increasing temperature compared to the reliable model that showed generally lower variance, which was also largely independent of temperature.

Conclusion

Going by the results of our research, we noted that a sturdy error correction scheme is necessary to solve this problem of large Hamming distances between measurements of the fingerprint. The basis for such error correction could be a fuzzy extractor. We are currently evaluating approaches to make the concept feasible on embedded systems.

Related DEPS Publications

[1] M. Zeinzinger, J. Langer, F. Eibensteiner, P. Petz, L. Drack, D. Dorfmeister, R. Ramler: Comparative Analysis of SRAM PUF Temperature Susceptibility on Embedded Systems. ICECT 2023.

[2] M. Wurzer: DRAMA in Embedded Systems – Determining the Address Mapping Function.

[3] L. Drack: SRAM based Physical Unclonable Functions for Low-Cost Embedded Systems.

Contact:
Florian Eibensteiner, University of Applied Sciences Upper Austria, T +43 5 0804-22425, florian.eibensteiner@fh-ooe.at

Consortium:
scch { software competence center hagenberg }
CODE RI Research Institute Cyber Defence Universität der Bundeswehr München
EPFL
JKU LIT Secure and Correct Systems Lab
Symflower
framag
Plasser&Theurer
KU LEUVEN
EMBEDDED SYSTEMS LAB FH OÖ / CAMPUS HAGENBERG

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

Federal Ministry
Republic of Austria
Labour and Economy

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