Probabilistic Identification of SRAM PUFs Using Selective Weak-Bit Masking

Łukasz Makowski
Faculty of Electrical Engineering
Warsaw University of Technology
Warsaw, Poland
https://orcid.org/0000-0002-4586-6890

***Abstract*—This work investigates probabilistic fingerprinting of SRAM startup states, focusing on cells that do not settle reproducibly across repeated power-up cycles. Instead of discarding such variable bits, their startup behavior is modeled probabilistically and a heuristic masking algorithm is used to select reduced fingerprints for likelihood-based device identification. Successful identification across all evaluated mask sizes indicates that device-specific information is preserved under substantial fingerprint reduction. This demonstrates that SRAM startup variability can itself provide useful information for device fingerprinting rather than merely being a source of instability.**

***Index Terms*—Physical unclonable function, microcontrollers, authentication.**

I. Introduction

Physical unclonable functions (PUFs) can provide a foundation for device-specific identifiers without requiring secret values to be stored in non-volatile memory [1]. In particular, SRAM-based PUFs are attractive for embedded and IoT systems because SRAM is already available in most microcontrollers [2].

During power-up, each SRAM cell passes through a brief transient state and then settles into one of two stable states representing a binary value. Individual SRAM cells can be classified according to the reproducibility of their startup states. Stable cells consistently settle to either logic 0 or logic 1 across repeated power-up cycles. Other cells exhibit less reproducible startup behavior and may reach either steady state according to their characteristic probabilities [3]. The corresponding memory positions are commonly referred to as unstable or "weak" cells and are usually considered problematic for reliable device identification. Often, these uncertainties are mitigated using fuzzy extractors and error-correcting codes to generate a stable identifier [4], [5].

This work, however, investigates whether the startup variability of SRAM cells can instead be treated as a source of device-specific information. Instead of compensating for this instability to improve reproducibility, the proposed approach embraces it as a useful property. To this end, selective weak-bit masking is combined with probabilistic modeling of startup states for device identification.

II. Experimental Methodology

For further numerical investigation, an experimental dataset of startup-state snapshots was collected from a 4-kB SRAM region of eight STM32L152RE microcontroller boards. The snapshots were acquired under stable environmental conditions in a laboratory at 22 °C. To minimize manual intervention, the acquisition process employed automated power cycling of the USB ports supplying the microcontroller boards. The power-cycling procedure was consistent across all acquisitions in terms of the time the devices remained powered down and the time they remained powered up before a snapshot was obtained through the debugging interface.

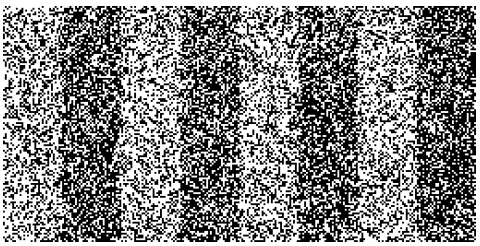

Fig. 1. Example of an SRAM startup-state snapshot.

Each snapshot is represented as a vector of bit values. For initial visual inspection of the SRAM startup state, this vector can be reshaped into a rectangular matrix of arbitrary dimensions and displayed as a binary image. An example of such a snapshot is shown in Fig. 1, where binary values of 1 and 0 are represented by black and white pixels, respectively. Although the SRAM startup state might be expected to appear random, Fig. 1 reveals clearly visible bands where one of the binary values occurs more frequently. This observation is consistent with results reported by other researchers for this particular microcontroller [6].

A total of 120 snapshots were acquired from each of the eight microcontrollers, resulting in a dataset of 960 samples for further analysis. In a subsequent acquisition campaign, an additional 50 snapshots were collected from each device and reserved exclusively for validation of the identification method described later in the paper.