Detecting Recycled Commodity SoCs:
Exploiting Aging-Induced SRAM PUF Unreliability

Yansong Gao\textsuperscript{a,∗}, Hua Ma\textsuperscript{b}, Said F. Al-Sarawi\textsuperscript{a}, Derek Abbott\textsuperscript{a}, Damith C. Ranasinghe\textsuperscript{b}

\textsuperscript{a}School of Electrical and Electronic Engineering, The University of Adelaide, Adelaide, SA 5005, Australia
\textsuperscript{b}School of Computer Science, The University of Adelaide, SA 5005, Australia

Abstract

A physical unclonable function (PUF), analogous to a human fingerprint, has gained an enormous amount of attention from both academia and industry. SRAM PUF is among one of the popular silicon PUF constructions that exploits random initial power-up states from SRAM cells to extract hardware intrinsic secrets for identification and key generation applications. The advantage of SRAM PUFs is that they are widely embedded into commodity devices, thus such a PUF is obtained without a custom design and virtually free of implementation costs. A phenomenon known as ‘aging’ alters the consistent reproducibility—reliability—of responses that can be extracted from a readout of a set of SRAM PUF cells. Similar to how a PUF exploits undesirable manufacturing randomness for generating a hardware intrinsic fingerprint, SRAM PUF unreliability induced by aging can be exploited to detect recycled commodity devices requiring no additional cost to the device. In this context, the SRAM PUF itself acts as an aging sensor by exploiting responses sensitive to aging. We use SRAMs available in pervasively deployed commercial off-the-shelf micro-controllers for experimental validations, which complements recent work demonstrated in FPGA platforms, and we present a simplified detection methodology along experimental results. We show that less than 1,000 SRAM responses are adequate to guarantee that both false acceptance rate and false rejection rate are no more than 0.001.

Keywords: Anti-counterfeiting, Recycled SoCs, SRAM PUF, hardware security

1. Introduction

Electronic components are increasingly integrated and introduced into every domain of our lives. They are pervasively employed in Internet of Thing (IoT) devices such as wireless sensors in smart homes and health-care applications in civilian use cases to military and aerospace components in defense. However, over the past decade, counterfeit electronic components or integrated circuits (ICs) have flooded into every aspect of supply chains \[1\]. Counterfeit ICs pose great concerns for: i) governments, threatening national security or civilian safety due to their poor quality leading to lower performance or malfunctions that may result in critical system failures—e.g., transportation, hospital and power-station facilities, in addition, to tax revenue losses; ii) industry, they cause direct revenue loss and further ruin brand value; iii) consumers, they can induce potential safety concerns when they are employed in security or health critical applications due to the low quality and reliability issues \[2\].

∗Corresponding author

Email addresses: yansong.gao@adelaide.edu.au (Yansong Gao), mary.ma@adelaide.edu.au (Hua Ma), said.alasarawi@adelaide.edu.au (Said F. Al-Sarawi), derek.abbott@adelaide.edu.au (Derek Abbott), damith.ranasinghe@adelaide.edu.au (Damith C. Ranasinghe)

Combating counterfeit ICs involves securing untrusted supply chains resulting from the globalization of the semiconductor industry; one needs to trace, check and detect counterfeits along the supply chain within their lifecycles. Among various countermeasures, the physical unclonable function (PUF) is one promising lightweight hardware security primitive that assigns each IC with a unique identifier upon its creation, similar to fingerprints of humans \[3, 4, 5, 6\]. Since PUF exploits manufacturing randomness, it is impossible for the counterfeiter to physically clone such instance-specific identifiers in the atom-by-atom level. Thus, the PUF is able to prevent counterfeiting ICs from several sources including cloned and overproduced ones. However, they were not considered to detect remarked or recycled counterfeit ICs \[2\] until recent work from \[7\]. Extending PUF’s functionality to detect remarked or recycled ICs is considerably valuable, as they contribute to more than 80% of reported counterfeit incidents \[8\].

Previous PUF applications focused on identification or authentication and key generation applications \[9, 10\]. In both, it is desirable for a PUF to regenerate the same response (output) when queried by the same challenge (input). However, in practice, the reliability of responses corresponding to certain challenges are affected by variations in environmental factors and aging effects. In typical PUF-based applications, for instance, cryptographic key genera-
Figure 1: SRAM cell [19]. $V_{th}$ difference in the transistors results into repeatable random power-up states either in ‘1’ or ‘0’.

In contrast, we take advantage of unavoidable unreliability of responses resulting from aging effects to provide a high degree of assurance to sense the period of aging experienced by PUF integrated ICs. In particular, we consider exploiting SRAM PUFs that are available in most commodity electronic systems or system on chips (SoCs), where neither additional area cost nor custom modification is required, to detect recycled commodity SoCs. The SRAM PUF is more suitable in this context in comparison with other popular silicon PUF structures such as Arbiter PUFs (APUF) and Ring Oscillator PUFs (ROPUFs) [10, 17, 18] do requiring additional cost such as adding logic circuitry into existing electronic components using customized designs. Our work complement the recent work in [7] utilizing SRAM PUFs to detect recycled devices demonstrated on FPGA platforms. We summarize our contributions below:

1. We evaluate and validate detection of recycled SoCs by using ubiquitously deployed micro-controllers that are commonly embedded with SRAM memories.
2. We develop a simplified aging sensitive response (ASR) selection methodology and detail how to systemically evaluate and quantify the detection capability. The detection is cost-free to the commodity SoCs since all the computations are left to the resource-rich verifier that carries out the detection.
3. Our investigations with experimental results demonstrate that the aging-induced unreliability of SRAM PUFs in SoCs can effectively detect recycled SoCs with very high accuracy. Our ASR methodology allows to use less than 1,000 SRAM responses to ensure that both false rejection rate (FRR) and false acceptance rate (FAR) are less than 0.001. In addition, experimental results validate that the detection accuracy increases with prolonged aging periods.

The rest of the paper is organized as follows. Related work is introduced in Section 2. In Section 3 we detail the simplified ASR selection methodology and how to systematically evaluate the detection capability. The simplified response selection approach during the provisioning phase is introduced in order to improve the detection efficiency in the recycled hardware detection phase by employing responses that are more sensitive to aging effects. Then comprehensive experimental results from off-the-shelf commodity microcontrollers embedded SRAM PUFs are given in Section 4. In Section 5 we conclude this article.

2. Background and Related Work

2.1. SRAM PUF

Unlike the other two popular silicon PUF constructions, ROPUFs and APUFs that exploit time delay differences [5] to extract secrets, SRAM PUFs [20, 19] leverage the threshold voltage $V_{th}$ mismatch between two cross-coupled inverters of a SRAM cell resulting from manufacturing randomness. As a memory cell, a write operation forces the SRAM cell to transition into one of two digital states, e.g., ‘0’ or ‘1’. When a cell is powered up or no write operation is occurred, the SRAM cell tends to prefer a repeatable power-up state—also referred as a response—either being ‘1’ (AB=01) or ‘0’ (AB=10). As an example, if the $V_{th,P1}$ is slightly smaller than $V_{th,P2}$, at power-up, $M_1$ starts conducting before $M_2$, thus, $A=1$. This in turn prevents $M_2$ switching on. As a consequence, the SRAM cell at power-up prefers to be ‘0’ (AB=10). Larger $|V_{th,P1} - V_{th,P2}|$ leads to more repeatable power-up states or more reliable responses when the cell is used to regenerate the response. Such a repeatable power-up state differs from cell to cell and chip to chip as well, thus, a map of the power-up states of a set of SRAM cells can be treated as a unique identifier, or the SRAM memory array can be treated as a PUF. In particular, the readout SRAM power-up state is referred to as the response, while the address of the SRAM cell is referred to as the challenge.

2.2. Sensing Aging with SRAM PUFs

However, some of SRAM PUF responses are not reproducible due to that fact that the $V_{th}$ difference of a selected cell is not dominant in the presence of noise from environmental factors such as supply voltage and temperature variations and aging effects. In elementary PUF-oriented identification and authentication applications, those unreliable responses are undesirable. In contrast, and just as undesirable fabrication randomness is extracted to create instance-specific PUFs to derive a physical inseparable trust anchor for a hardware device, a PUF response’s sensitivity to environmental factors and aging can also be utilized to secure sensing. In this context, sensing functionality is derived from a PUF and the PUF lends itself as a sensor to guarantee the veracity of sensed data [21, 22, 23, 7, 24].
Detecting recycled devices using SRAM PUFs by considering those PUF responses sensitive to aging effects was recently received attention and initially investigated in [7]. Guo et al. used SRAM cells in FPGA platforms for experimental validations. We complement this initial investigation using SRAM memory in pervasively deployed off-the-shelf micro-controllers as they are commonly deployed in many SoCs ranging from home appliances to various sensors in the Internet of Things (IoT) era. We present a simpler methodology of selecting aging sensitive response bits and detail a systematic approach to evaluate and quantify recycled SoC detection capability supported by experimental data.

2.3. SRAM Aging

Silicon ICs performance deteriorates gradually over time attributing to various factors such as hot carrier injection (HCI), time-dependent dielectric breakdown (TDDB) and bias temperature instability (BTI) [23, 7]. The negative BTI (NBTI) plays dominant aging effect in modern ICs, especially for switched-on pMOS transistors [25].

The NBTI effect increases the threshold voltage of pMOS transistors when a transistor is ‘on’. Considering the example in Section 2.1 where the SRAM is powered up without a write operation. Consider that we already knew AB = 10, where the M1 is ‘on’ and experiences a gradually increased $V_{th,P1}$ due to the NBTI, while the $V_{th,P2}$ remains or changes negligibly with respect to $V_{th,P1}$. Hence, over time, $V_{th,P1} > V_{th,P2}$. As a consequence, the regenerated responses over the life of such cells tend to shift from being reliably generated ‘0’ to ‘1’. Though anti-aging strategies are possible [25], its expensive time and monetary cost prohibit a counterfeiter to do so, especially for low-end ICs. The bit flipping over time caused by the response sensitivity to aging is undesirable for conventional PUF applications, but can be exploited to detect recycled commodity SoCs widely embedded with SRAM memories.

Before delving into detailed descriptions, we give a number of useful definitions to ease the following descriptions, especially the systematic detection capability evaluations.

3. Detection Methodology

3.1. Preliminaries

**Definition 1. InterA-distance.** The interA-distance is a random variable describing the distance between two PUF responses $R^{PreA}$, $R^{PostA}$ produced before aging and after aging by applying the same challenge—address in case of a SRAM PUF—to the same PUF, hence,

$$D_{interA} = \text{dist}(R^{PreA}, R^{PostA}) \quad (1)$$

where $R^{PreA}$, $R^{PostA}$ are two responses generated before and after aging by applying the same challenge to the same PUF.

**Definition 2. IntraA-distance.** The intraA-distance is a random variable describing the distance between two PUF responses $R^{A}$, $R^{A'}$ re-evaluated on the same PUF, using the same challenge before aging.

$$D_{intraA} = \text{dist}(R^{A}, R^{A'}) \quad (2)$$

where $R^{A}$, $R^{A'}$ are two responses obtained from the same PUF using the same chosen challenge before aging.

The dist(;) can be any well-defined and appropriate distance metric over the responses. In this paper, responses are always bit vectors and the used distance metric is Hamming distance (HD) or fractional Hamming distance formally defined below:

**Definition 3. Hamming distance.** For bit vectors $X_1$ and $X_2$ with the same length $l$, the HD between them is defined as:

$$f_{HD}(X_1, X_2) = \sum_{i=1}^{l} X_1 \oplus X_2 \quad (3)$$

**Definition 4. Fractional Hamming distance.** Built upon Eq. (3), the fractional Hamming distance (FHD) is defined as:

$$f_{FHD}(X_1, X_2) = \frac{f_{HD}(X_1, X_2)}{l} \quad (4)$$

Readers who are familiar with PUFs will notice that the definition of the interA-distance is similar to the inter-distance of PUFs that measures the difference between two responses from two distinct PUF instances given the same challenge. The difference is that the interA-distance is evaluated across differing aging periods subject to the same PUF instance, the inter-distance is, however, evaluated across different PUF instances.

The intraA-distance is similar to the intra-distance of PUF responses that measures the difference between two responses reproduced from two distinct evaluations by applying the same challenge to the same randomly chosen
3.2. Detecting Capability

PUF instance. The main difference is that the intra-distance does not consider the source of aging, it simply treats any environmental fluctuation, e.g., supply voltage, temperature and also aging effects as noise sources. However, in this work, we are able to finely fix the supply voltage and temperature, only thermal noise is treated as a noise source. The aging effects is not a noise source but is exploited to detect aging devices.

Similar to the inter-distance and intra-distance distribution of PUFs explained in detail in [26], both of the interA-distance and intraA-distance can be assumed to follow a binomial distribution $B(n, p)$. The binomial probability estimator of interA-distance and intraA-distance distributions are referred to as $\hat{p}_{\text{interA}}$ and $\hat{p}_{\text{intraA}}$, respectively. In general, the $\hat{p}_{\text{interA}}$ is the probability that $R^{\text{PreA}} \neq R^{\text{PostA}}$, see Definition 1, and the $\hat{p}_{\text{intraA}}$ is the probability that $R^{A} \neq R^{A}$, see Definition 2.

### 3.2. Detecting Capability

Based on (5) and (6), we can see that the FRR and FAR depend on the $\hat{p}_{\text{intraA}}$ and $\hat{p}_{\text{interA}}$, the threshold $n_{th}$, and the number of employed CRPs $n$. For example, supposing $n$ is 64 as shown in Fig. 2, a large $n_{th}$ benefits the false rejection rate but aggravates the false acceptance rate, and vice versa for a small $n_{th}$. We want to minimize both FAR and FRR in practice. There exists a threshold value to make both FAR and FRR equal. We refer this interested threshold value as equal error threshold, termed $n_{\text{EER}}$. Consequently, when both error rates are equal, we refer this equal rate as equal error rate (EER) following Roel’s work [26]. For a discrete distribution, there may not be an $n_{\text{EER}}$ for which FAR is equal to FRR, and in that case, $n_{\text{EER}}$ and EER are defined as in [26]:

$$n_{\text{EER}} = \arg\min\{\max\{\text{FAR}(n_{th}), \text{FRR}(n_{th})\}\}$$  \hspace{1cm} (7)

$$\text{EER} = \max\{\text{FAR}(n_{\text{EER}}), \text{FRR}(n_{\text{EER}})\}$$  \hspace{1cm} (8)

Given binomial probability estimator $\hat{p}_{\text{interA}}$ and $\hat{p}_{\text{intraA}}$, the task is to find minimal number of CRPs, $n$, for ensuring an acceptable EER that meets desired requirements.

To increase the capability of distinguishing recycled devices from new ones and minimize both FAR and FRR, it is imperative to increase the difference between $\hat{p}_{\text{intraA}}$ and $\hat{p}_{\text{interA}}$. We can visually observe this in Fig. 2. For example, when the interA-distance distribution shifts to right and intraA-distance distribution keeps same, it is clear that both FAR and FRR will be reduced as the overlapped area becomes small. Therefore, we introduce an approach to select SRAM responses that are of higher sensitivity to aging to increase the difference between $\hat{p}_{\text{intraA}}$ and $\hat{p}_{\text{interA}}$.

### 3.3. Selecting ASRs

It has been shown when a SRAM cell is under high temperature, $V_{th}$ increases in a similar manner to that caused by aging [7]. Therefore, during provisioning phase, the SRAM PUF responses can be re-evaluated under room temperature (RT) and high temperature (HT), respectively, to select aging sensitive responses (ASRs). Notably, the high temperature setting is only necessary during the provisioning phase and is not required during the detection phase. The ASR selection follows Algorithm 1.

The proposed ASR selection method is straightforward and simpler in comparison with [7]. During the provisioning phase, the response $r$ is regenerated $N$ times under RT.
Algorithm 1 Selecting ASRs

1: procedure selection (PUF, RT, HT)
2: for $i = 1 : N$ do
3: generating response $r_{RT}$, under RT using PUF;
4: end for
5: for $i = 1 : N$ do
6: generating response $r_{HT}$, under HT using PUF;
7: end for
8: if (all $r_{RT}$ same) && (all $r_{HT}$ same) && ($r_{RT} \neq r_{HT}$) then
9: select aging sensitive response $r$;
10: return
11: else
12: discard response $r$;
13: return
14: end if
15: end procedure

and HT respectively. The $r$ is selected as an ASR when all regenerated $r$ are same under RT and HT, respectively, but exhibit opposite values. For example, the regenerated $r$ exhibits ‘1’ for all $N$ evaluations under RT and ‘0’ for all $N$ evaluations under HT. Then this $r$ is selected as a ASR. Otherwise, it is discarded and will not be utilized for detecting aging SoCs in the afterward detection phase.

When ASRs are selected, there $\hat{p}_{\text{intraA}}$ and $\hat{p}_{\text{interA}}$ can be heuristically evaluated. We assume $\hat{p}_{\text{intraA}}$ is less than $\hat{p}_{\text{interA}}$, and this is true as we will show in Section 4.

4. Experimental Results

4.1. Experiment Setup

SRAM PUF CRP dataset is collected from three chip-KIT Pro MX7 microcontroller boards. From each board, we read power-up states from 262,144 SRAM cells as SRAM PUF responses. The nominal power supply voltage is 3.25 V. We are able to change the voltage from 3.125 V to 3.50 V. We found that the voltage, however, has negligible effects on the SRAM PUF reliability under test, which agrees with other experimental results [24]. Therefore, we focus on SRAM PUF reliability performance as shown in Fig. 3 that is $\hat{p}_{\text{intraA}}$ before aging under nine different temperature corners: −5°C, 15°C, 25°C, 35°C, 45°C, 55°C, 65°C, 75°C, 85°C. The room temperature 25°C is treated as the nominal or reference corner. We are mostly interested in the $\hat{p}_{\text{intraA}}$ under RT, which is approximately 6% as shown in Fig. 3.

To test the aging influence on the SRAM PUF response’s reliability, we put the microcontroller board in the oven of 80°C to accelerate the aging. For expected NBTI aging, the acceleration factor (AF) is expressed [25]:

$$AF = \left( \frac{V_{\text{stress}}}{V_{\text{nominal}}} \right) ^ \alpha \cdot \exp \left( \frac{E_{\text{aa}}}{k} \left( \frac{1}{T_{\text{stress}}} - \frac{1}{T_{\text{nominal}}} \right) \cdot \frac{1}{m} \right), \quad (9)$$

where the parameters setting are: the gate voltage exponent $\alpha = 3.5$; the time exponent $m = 0.25$; the apparent activation energy $E_{\text{aa}} = -0.02\, eV$; and Boltzmann’s constant $k = 8.62 \times 10^{-5} eV/K$. We only consider temperature resulted stress, where $V_{\text{stress}} = V_{\text{nominal}}, T_{\text{stress}} = 80°C, T_{\text{nominal}} = 25°C$. As a consequence, we are able to obtain AF=11.03.



![Figure 3: $\hat{p}_{\text{intraA}}$ of three SRAM PUFs across three microcontrollers under nine temperature corners, reference temperature is 25°C.](image)

Figure 3: $\hat{p}_{\text{intraA}}$ of three SRAM PUFs across three microcontrollers under nine temperature corners, reference temperature is 25°C.

After 48 hours of accelerated aging that is equal to 22.1 days of effective NBTI device aging under normal working conditions in the field, we calculate the $\hat{p}_{\text{interA}}$ under RT using a strategy of randomly selecting responses. Results in Fig. 4 imply that $\hat{p}_{\text{interA}}$ is only slightly higher than $\hat{p}_{\text{intraA}}$. More specifically, the difference between $\hat{p}_{\text{interA}}$ and $\hat{p}_{\text{intraA}}$ is only around 1%. This indicates that only a small fraction of responses are sensitive to aging. We can see from our analyses in Section 3.2 that using a random response selection strategy for recycled SoCs detection is cumbersome.

Next, we first implement the ASR selection approach outlined in Algorithm 1 and then demonstrate the significantly improved difference between $\hat{p}_{\text{interA}}$ and $\hat{p}_{\text{intraA}}$ that consequently facilitates the detection capability.

4.2. ASR Detection Capability Results

We apply the ASR selection according to Algorithm 1. Noting that both $\hat{p}_{\text{intraA}}$ and $\hat{p}_{\text{interA}}$ are a function of $N$, which is number of a response reevaluated under a given
RT and HT. The purpose of the selection process is to increase the difference between \( \hat{p}_{\text{inter}} \) and \( \hat{p}_{\text{intra}} \) whilst also making sure that the \( \hat{p}_{\text{intra}} \) is small as well. Mean of \( \hat{p}_{\text{inter}} \), \( \hat{p}_{\text{intra}} \), and \( \hat{p}_{\text{inter}} - \hat{p}_{\text{intra}} \) as a function of \( N \) settings for those selected ASRs are depicted in Fig. 5 (a).

We can see that \( \hat{p}_{\text{intra}} \) when ASR is implemented, is always larger than the \( \hat{p}_{\text{intra}} \) of around 6% without ASR selection, see Fig. 4 this is because the ASRs are also tending to be erroneous when they are regenerated under RT before aging. However, the \( \hat{p}_{\text{inter}} \) is increased faster, therefore, larger \( \hat{p}_{\text{inter}} - \hat{p}_{\text{intra}} \) is achieved. In addition, the \( \hat{p}_{\text{intra}} \) decreases as the \( N \) increases with slightly improved \( \hat{p}_{\text{inter}} - \hat{p}_{\text{intra}} \). Overall, as we shall see in Table 1 a larger \( N \) yields a higher detection capability.

In Fig. 5 (b), the number of selected ASRs out of 262,144 responses are depicted. We can expect that the number of ASRs to decrease as \( N \) increases because less number of responses are able to satisfy the selection criterion in Algorithm 1. Therefore, a larger \( N \) leads to less number of selected ASRs but higher sensitivity to aging for those selected ASRs.

In Table 1 we give results of quantitatively evaluations of \( n \)—minimal bit length of the response to meet the EER, and \( n_{\text{th}} \) or \( n_{\text{EER}} \) of SRAM PUF being used to detect recycled SoCs under different \( \hat{p}_{\text{inter}} \) and \( \hat{p}_{\text{intra}} \). We can see from Table 1 the necessary bit length of \( n \) decreases as \( N \) is increasing. For example, \( n \) is reduced by more than 63% by increasing \( N \) from three to nine whilst both FAR and FRR are guaranteed to be less than 0.001. This validates the high efficacy of the presented ASR selection methodology. Using ASRs that are more sensitive to aging expedite the detecting of recycled commodity SoCs as less response bits need to be acquired during an evaluation. In addition, the volume needed to securely store reference ASRs in database is reduced or relaxed.

Besides the above 48 hrs accelerated aging period, we also test the detection capability given two other accelerated aging periods: 18 hrs and 108 hrs—equal to 8.3 and 49.6 days of SoC operation in the field. The evaluated detection capability is detailed in Table 2. We set \( N = 9 \) for all evaluations. We can see that longer aging periods are easier to detect with fewer number of ASRs while guaranteeing the same detection capability, e.g., EER threshold.

In practice, given the same \( n \), if the FAR is more critical than FRR—this maybe the case as FAR poses a security concern by mistakenly accepting recycled SoCs, a smaller \( n_{\text{th}} \) can be adopted.

5. Conclusion

In this study, we experimentally validate the use of embedded SRAMs in off-the-shelf microcontrollers to detect the periods that SoCs work in the field. It is validated that both FAR and FRR can be less than \( 10^{-4} \) when the SoCs experiences only nine days aging. The simplified ASR selection method considerably reduces the necessary number of SRAM PUF response bits to achieve the required detection capability by employing responses that exhibit higher sensitivity to aging effects. In addition, adding the ability of aging sensing to the popular SRAM PUF extends its function to secure IC supply chains by not only preventing cloned and overproduced ICs but also from recycled ones. Most importantly, detection of recycled commercial SoCs embedded with SRAM memories requires no modification to the original design, and thus cost-free is achieved.

Acknowledgment

This research was supported by the Australian Research Council Discovery Program (DP140103448). We acknowledge support from China Scholarship Council (201306070017). We thank the help from Dr Alex Dimitriou for oven setup and Mr Danny DiGiacomo for experiment setup. We also thank useful discussions with Mr. Zimu Guo and Dr. Domenic Forte.

References

[1] K. M. Gregory, Counterfeit electronic parts flood U.S. market, accessed: 2017-02-05.
[2] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, Y. Makris, Counterfeit integrated circuits: a rising threat in the global semiconductor supply chain, Proceedings of the IEEE 102 (8) (2014) 1207–1228.
[3] G. E. Suh, S. Devadas, Physical unclonable functions for device authentication and secret key generation, in: Proc. Design Automation Conf. (DAC), 2007, pp. 9–14.
[4] C. Jin, M. van Dijk, Secure and efficient initialization and authentication protocols for SHIELD, IEEE Transactions on Dependable and Secure Computing.
[5] Y. Gao, D. C. Ransinghe, S. F. Al-Sarawi, O. Kavehei, D. Abbott, Emerging physical unclonable functions with nanotechnology, IEEE Access 4 (2016) 61–80.
Table 1: Quantitative evaluation of necessary bit length of the response for successful detection under different \( \hat{p}_{\text{intra}} \) and \( \hat{p}_{\text{inter}} \) that are determined by \( N \).

| Aging period (Days) | \( \hat{p}_{\text{inter}} - \hat{p}_{\text{intra}} \) | \( n \) | EER < \( 10^{-2} \) | EER < \( 10^{-3} \) | EER < \( 10^{-4} \) |
|---------------------|-----------------|-----|-----------------|-----------------|-----------------|
| 8.3                 | 3.32 %           | 1870 199  −2.00 −2.01 | 3294 350  −3.00 −3.01 | 4764 506  −4.00 −4.01 |
| 22.1                | 6.52 %           | 551 68  −2.01 −2.00 | 974 120  −3.01 −3.04 | 1406 173  −4.01 −4.03 |
| 49.6                | 8.61 %           | 330 43  −2.02 −2.01 | 584 76  −3.01 −3.04 | 840 109  −4.01 −4.02 |

Note: the * symbol indicates \( \log_{10}(\cdot) \) of the value.

Table 2: Quantitative evaluation of necessary bit length of the response for successful detection under different \( \hat{p}_{\text{inter}} \) and \( \hat{p}_{\text{intra}} \) that are related to aging period, where \( N = 9 \).

| Aging period (Days) | \( \hat{p}_{\text{inter}} - \hat{p}_{\text{intra}} \) | \( n \) | EER < \( 10^{-2} \) | EER < \( 10^{-3} \) | EER < \( 10^{-4} \) |
|---------------------|-----------------|-----|-----------------|-----------------|-----------------|
| 3                   | 20.70%          | 1706 393  −2.01 −2.01 | 3005 692  −3.01 −3.00 | 4347 1001  −4.01 −4.01 |
| 4                   | 17.55%          | 1251 252  −2.01 −2.00 | 2191 441  −3.00 −3.01 | 3171 638  −4.00 −4.01 |
| 5                   | 14.98%          | 914 163  −2.01 −2.00 | 1611 287  −3.01 −3.00 | 2330 415  −4.00 −4.01 |
| 6                   | 13.07%          | 746 120  −2.00 −2.01 | 1314 211  −3.00 −3.01 | 1906 306  −4.00 −4.01 |
| 7                   | 11.54%          | 603 89  −2.02 −2.02 | 1052 155  −3.00 −3.01 | 1528 225  −4.01 −4.02 |
| 8                   | 10.30%          | 606 81  −2.01 −2.01 | 1065 142  −3.00 −3.01 | 1546 206  −4.00 −4.01 |
| 9                   | 9.26%           | 551 68  −2.01 −2.01 | 974 120  −3.01 −3.04 | 1406 173  −4.01 −4.03 |

Note: the * symbol indicates \( \log_{10}(\cdot) \) of the value.

[6] A. B. Alvarez, W. Zhao, M. Alioto, Static physically unclonable functions for secure chip identification with 1.9–5.8% native bit instability at 0.6–1 V and 15 fJ/bit in 65 nm, IEEE J. Solid-State Circuits 51 (3) (2016) 763–775.

[7] Z. Guo, M. T. Rahman, M. M. Tehranipoor, D. Forte, A zero-cost approach to detect recycled SoC chips using embedded SRAM, in: Proc. Symp. Hardware Oriented Security and Trust (HOST), IEEE, 2016, pp. 191–196.

[8] U. Guin, D. Forte, M. Tehranipoor, Design of accurate low-cost on-chip structures for protecting integrated circuits against recycling, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 24 (4) (2016) 1233–1246.

[9] Y. Gao, G. Li, H. Ma, S. F. Al-Sarawi, O. Kavehei, D. Abbott, D. C. Ranasinghe, Obfuscated challenge-response: A secure lightweight authentication mechanism for PUf-based pervasive devices, in: Proc. Int. Conf. Pervasive Computing and Communication (Percom) Workshops, 2016, pp. 1–6.

[10] M.-D. M. Yu, S. Devadas, Pervasive, dynamic authentication of physical items, Queue 14 (6) (2016) 70.

[11] R. Maes, A. Van Herreweghe, I. Verbauwhede, PUFKey: A fully functional PUF-based cryptographic key generator, in: Cryptographic Hardware and Embedded Systems (CHES), 2012, pp. 302–319.

[12] D. C. Ranasinghe, P. H. Cole, Confronting security and privacy threats in modern RFID systems, in: Proc. Fortieth Asilomar Conf. Signals, Systems and Computers, 2004, pp. 2058–2064.

[13] D. Lim, Extracting secret keys from integrated circuits, Master’s thesis, Massachusetts Institute of Technology (2004).

[14] U. Rührmair, J. Solter, F. Sehle, X. Xu, A. Mahmoud, V. Stoyanova, G. Dorr, J. Schmidhuber, W. Burleson, S. Devadas, PUF modeling attacks on simulated and silicon data, IEEE Trans. Inf. Forensics Security 8 (11) (2013) 1876–1891.

[15] G. T. Becker, The gap between promise and reality: On the insecurity of XOR Arbiter PUFs, in: Cryptographic Hardware and Embedded Systems (CHES), 2015, pp. 535–555.

[16] C. Herder, M.-D. Yu, F. Koushanfar, S. Devadas, Physical unclonable functions and applications: A tutorial, Proceedings of IEEE 102 (2014) 1126–1141.

[17] J.-L. Zhang, G. Qu, Y.-Q. Lv, Q. Zhou, A survey on silicon PUFs and recent advances in ring oscillator PUFs, Journal of Computer Science and Technology 29 (4) (2014) 664–678.

[18] Y. Cao, L. Zhang, C.-H. Chang, S. Chen, A low-power hybrid RO PUF with improved thermal stability for lightweight applications, IEEE Trans. Comput.-Aided Design Integr. Circuits Syst. 34 (7) (2015) 1143–1147.

[19] D. E. Holcomb, W. P. Burleson, K. Fu, Initial SRAM state as a fingerprint and source of true random numbers for RFID tags, in: Proceedings of the Conference on RFID Security, 2007.

[20] Y. Su, J. Holleman, B. Otis, A 1.6 pJ/bit 96% stable chip-id cost approach to detect recycled SoC chips using embedded SRAM, in: Proc. Symp. Hardware-Oriented Security and Trust (HOST), IEEE, 2014, pp. 148–153.

[21] K. Rosenfeld, E. Gavas, R. Karri, Sensor physical unclonable functions, in: Proc. IEEE. Int. Symp. Hardware Oriented Hardware-Oriented Security and Trust (HOST), 2010, pp. 112–117.

[22] U. Rührmair, J. Martinez-Hurtado, X. Xu, C. Kraeh, C. Hilgers, D. Kononchuk, J. J. Finley, W. P. Burleson, Virtual proofs of reality and their physical implementation, in: Proc. IEEE Symp. Security and Privacy (S&P), 2015, pp. 70–85.

[23] K. C. Baby, S. Aung, N. Schwesinger, Finite element analysis of differential capacitive PUF sensors, in: Sensors Applications Symposium (SAS), IEEE, 2016, pp. 1–6.

[24] H. Ma, Y. Gao, O. Kavehei, D. C. Ranasinghe, A PUF sensor: Securing physical measurements, in: Proc. Int. Conf. Pervasive Computing and Communication (Percom) Workshops, 2017.

[25] R. Maes, V. van der Leest, Countering the effects of silicon aging on SRAM PUFs, in: Proc. Symp. Hardware-Oriented Security and Trust (HOST), IEEE, 2014, pp. 148–153.

[26] M. Roel, Physically unclonable functions: Constructions, properties and applications, Ph.D. thesis, Ph. D. thesis, Dissertation, University of KU Leuven (2012).

[27] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, S. Devadas, Extracting secret keys from integrated circuits, IEEE 102 (2014) 1126–1141.
