Design Dependent SRAM PUF Robustness Analysis

Mafalda Cortez Said Hamdioui
Delft University of Technology
Faculty of EE, Mathematics and CS
Mekelweg 4, 2628 CD Delft, The Netherlands
{A.M.M.O.Cortez, S.Hamdioui}@tudelft.nl

Ryoichi Ishihara
Delft University of Technology
Delft Institute of Microsystems and Nanoelectronics (DIMES)
Feldmannweg 17, 2600 GB Delft, The Netherlands
R.Ishihara@tudelft.nl

***Abstract*—In this paper we evaluate and compare the robustness (i.e., repeatability and uniqueness) of two SRAM PUF designs, General Purpose (GP) and Low-Power (LP), by means of both circuit simulations and industrial measurements. Circuit simulations are performed on both designs while considering two technology nodes (45nm and 32nm), three temperatures and three voltage ramp-up times. Industrial measurements are performed to validate the simulation results. The simulation results as well as industrial measurements demonstrate that GP devices provide better repeatability for all investigated cases (up to 4.5× better) while the uniqueness is design independent.**

Keywords: PUF-based system, SRAM PUF, Robustness

I. Introduction

Physical Unclonable Functions (PUFs) are the embodiment of random and unique, but repeatable, mapping of challenges to responses in physical structures such as integrated circuits (ICs) [1]. The *uniqueness* and *repeatability* of this mapping, known as *fingerprint*, enables unambiguous identification of ICs making PUFs efficient hardware security primitives. Moreover, PUFs are hard to clone due to their random, uncontrollable, inherent, device-unique and deep-submicron process variations. Combined with proper post-processing, a PUF is able to generate secret keys of cryptographic strength, and reliably store them in a highly secure manner without the need for conventional on-chip *non-volatile memory* [2, 3]. However, PUF fingerprints have two main drawbacks. First, they are noisy; when the same challenge is consecutively applied to the same device, the mapped responses are slightly different even under the same operating conditions, resulting in lower repeatability. Second, the fingerprints of any two random devices might be slightly correlated, resulting in lower uniqueness.

To tackle PUF challenges and to guarantee robustness, i.e., uniqueness and repeatability, PUF-based systems use fuzzy extractors for both privacy amplification (to improve uniqueness) and error correction (to improve repeatability) [4]. However, the usage of fuzzy extractors comes at a cost which scales up with less robust bare PUF responses; reduced uniqueness is compensated with larger PUF footprints and reduced repeatability is compensated with *error-correcting code* (ECC) having larger error correction capability, resulting in an overall larger silicon area overhead [4, 5]. Numerous PUF constructions have been proposed and implemented (see [6] for an overview); however, SRAM PUFs are one of the most popular as they are standard IC components and CMOS technology compatible [7–9]. Our work focuses on the robustness analysis of this PUF type.

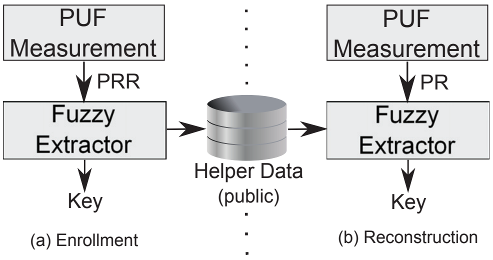
Much work has been published regarding the robustness of SRAM PUF technology [7–13]. In [7], the authors studied the mismatch root-cause in SRAM cells; the work validated only SRAM repeatability for 65nm node low-power. In [8], the authors theoretically analyzed the impact that external factors have on the fingerprint uniqueness and repeatability. In [9], [10] and [11] the authors addressed techniques to improve fingerprints' statistical characteristics, such as fuzzy extractors and helper data algorithms. In [12], the authors presented a technique called stable-PUF-marking to identify robust SRAM cells; they proposed to use only these cells for cryptographic key generation as an alternative for error correction code of those which are non-robust. They assumed that the cells mismatch is based on threshold voltage only. No silicon results were presented to validate the findings. In [13], the authors presented a comparison between SRAM PUFs and Flip-Flop PUFs repeatability and uniqueness based on 65nm silicon results. This study focused on a single technology node.

The state-of-the-art clearly shows that although the robustness of SRAM PUF is quite addressed, limited silicon results were reported. Moreover, robustness for different SRAM PUF designs in cryptographic systems is not investigated yet; understanding this will allow the integration of the best design in cryptographic systems, resulting in better robustness and overall reduced cost.

In this paper, we evaluate and compare the robustness of two different SRAM PUF designs, general purpose (GP) and low-power (LP), for different technology nodes and under varying operation conditions, such as temperature and voltage ramp-up time. The paper has the following contributions:

- Repeatability and uniqueness evaluation for two SRAM PUF design based on circuit simulations; the analysis is performed for two different technology nodes (45nm and 32nm) while considering three temperatures and three voltage ramp-up times.
- Repeatability and uniqueness measurements performed on silicon devices (both GP and LP), manufactured using different technology nodes. Also here, the impact of different stress conditions is investigated.

The rest of this paper is organized as follows. Section II provides some preliminaries on PUF-based systems, including the SRAM cell, the two different designs under consideration and introduces the metrics used to evaluate the PUF robustness. Section III discusses the simulation setup, the performed experiments and the simulation results. Section IV provides the industrial analysis, including the characteristics of the devices measured, the performed measurements, the results, a comparison with simulation results and a discussion. Finally, Section V concludes this paper.



(a) Enrollment

(b) Reconstruction

Fig. 1: PUF-based Key Generation and Storage System [7,17]

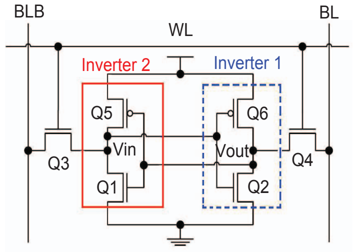


Fig. 2: 6T CMOS SRAM cell [7]

II. PUF-BASED SYSTEMS

In this section, we provide background information on PUF-based systems. First, we discuss their main operations. Second, we briefly provide some preliminaries on the basic operation of SRAM PUFs. Third, we summarize the main differences between general purpose and low-power devices. Finally, we introduce the robustness evaluation metrics.

A. PUF-based Key Generation and Storage

Fig. 1 shows the flow of a PUF-based key-storage system [3, 11] implemented with a *fuzzy extractor* (FE) [4, 14], which typically consists of two phases:

Enrollment: a key is generated from a *PUF Reference Response* (PRR). First, a PUF measurement produces the PRR. Next, the PRR is processed by the FE into a cryptographically strong *Key*, and helper data is generated as a FE byproduct. Finally, the helper data is stored in an external non-volatile memory (hence, becomes public information).
Reconstruction: the earlier enrolled *Key* is reliably recovered from a noisy *PUF Response* (PR) and the stored helper data. First, a PUF measurement produces the PR. Some bits of PR are different from original PRR; hence, PR is a noisy version of PRR. Next, PR is processed by the FE in combination with the helper data which is retrieved from the external memory. If the noisy PR is close enough to the PRR obtained during enrollment (i.e., the PUF response is repeatable up to a limited amount of noise), then the FE succeeds in reliably reconstructing the enrolled *Key*.

B. SRAM PUF

Fig. 2 shows the popular six-transistor SRAM cell. An SRAM cell is a bistable circuit, i.e., it has two possible states denoted as logic ’0’ and ’1’ and it comprises two cross-coupled inverters at its core, respectively formed by (*Q1*, *Q5*) and (*Q2*, *Q6*). The peripheral circuitry used to access the cell is comprised by two pass transistors (*Q3* and *Q4*), the bitline (*BL*), the complement bitline (*BLB*) and the wordline (*WL*).

When powered-up, the cross-coupled inverters start driving electric current, hence, increasing the voltages at their gates (V_{in} and V_{out}). The first inverter that builds enough gate voltage to drive its NMOS will pull-down its output, forcing the other inverter to pull-up and causing the SRAM cell to settle in one of both stable states. Since both inverters are designed to be nominally identical, the outcome (the states in which a cell settles) is entirely determined by the effect of random process variations. Hence, an SRAM power-up state, known as a *start-up value* (SUV), is a PUF response, and this construction is called an SRAM PUF.

C. SRAM Design

There are four designs that are optimized for different application requirements; they are *High-Performance* (HP) optimized for speed, *Low-Operating Dynamic Power* also known as *General Purpose* (GP) optimized for dynamic dissipation power, *Low-Standby Static Power* also known as *Low-Power* (LP) optimized for static power dissipation and *III-VGe* optimized for both low dynamic power and high speed operation. In our work, we focus on GP and LP devices, which are the ones manufactured for measurements. These designs differ on various parameters; a non-exhaustive list is summarized in Table I [15], comparing GP and LP devices. The table highlights the different configurations of both physical and electrical parameters for the same technology node, but different designs; V_{DD} is the supply voltage, L_{eff} is the effective gate length, t_{ox} is the thickness oxide, I_{on} is the leakage current during operation and I_{off} is the leakage current during idle. Comparing the two designs reveals that GP has a lower supply voltage, a shorter channel length and thickness oxide (hence, smaller threshold voltage), a similar operational current and two orders of magnitude higher leakage current. Our goal is to investigate the impact that these differences have on the robustness of SRAM PUFs, hence, on the overall cost of SRAM PUF-based systems.

D. PUF robustness metrics

PUF robustness in general, and of SRAM PUF in particular, can be evaluated by the repeatability and by the uniqueness of its fingerprint. Fingerprint’s repeatability is the ability of a device to generate the same fingerprint every time it is powered-up. The higher the number of bits that always have the same SUV, the higher the repeatability of that device. Uniqueness is the ability of a fingerprint to be distinguished from other devices fingerprint. The higher the fingerprint randomness, the less the correlation between any two given devices (assuming same fingerprint lengths).

To evaluate our experiments impact on both repeatability and uniqueness, we rely on two widely used metrics; they are *Fractional Hamming Distance* (FHD) and *Fractional Hamming Weight* (FHW) [13]. A brief explanation of the metrics and how these are used to evaluate the robustness parameters is given next.

FHD is used to evaluate both repeatability and uniqueness. FHD calculates the percentage of bits that are different between two different PUF responses; e.g., the FHD between ’0010’ and ’0110’ is 25%. When FHD is used for repeatability, per device, each of the measured PUF responses (PR) is compared with the enrollment PUF response (PRR) and then

TABLE I: Different configurations of physical and electrical parameters

	45nm					32nm				
	V_{DD} (V)	L_{eff} (nm)	t_{ox} (nm)	I_{on} (μA/μm)	I_{off} (nA/μm)	V_{DD} (V)	L_{eff} (nm)	t_{ox} (nm)	I_{on} (μA/μm)	I_{off} (nA/μm)
GP	0.7	22	0.9	754.0	6.80E+0	0.6	16	0.8	750.3	9.53E+0
LP	1.0	25	1.3	752.2	5.78E-2	0.9	18	1.1	888.9	7.77E-2

normalized to the response length, see Fig. 1. An FHD per device close to 0% indicates a high repeatability. When FHD is used for uniqueness, the measured enrollment PUF response (PRR) of each PUF device is compared with that of all other PUF devices and then normalized to the response length. An FHD between devices close to 50% is a good indicator of uniqueness. Moreover, the metric' statistical significance increases with the number of PRs considered to calculate FHD per device (for repeatability) and with the number devices considered per FHD between devices (for uniqueness).
FHW is used to evaluate uniqueness; it computes the percentage of bits that are *not* zero; e.g. the FHW of '0010' is 25%. An FHW close to 50% indicates a balanced distribution of zeros and ones in the PUF responses. However, this metric is blind to logic values clustering.

III. Simulation based analysis

To analyze the repeatability and uniqueness of SRAM PUFs both for general purpose and low-power, a memory system comprising a cell and peripheral circuitry is synthesized and simulated using HSPICE and PTM models [19]. In this section, first, we present the PUF fingerprint generation. Thereafter, we describe the simulation experiments and results.

A. SRAM PUF Response Setup

Each bit of an SRAM PUF response is generated by an individual SRAM cell. Fig. 3 shows the SRAM fingerprint generation schematic used in our simulations. It has been shown in [7, 8] that the threshold voltage V_{th} of NMOS transistors is the technology parameter with the most impact on the SRAM cell start-up value. Hence, Monte Carlo is used to generate 300 V_{th} random values for *Q1* (see Fig. 2) according to the distribution presented in [16], i.e., mean μ = standard NMOS V_{th} and deviation σ = $9\% \cdot \mu$. These 300 SRAM cells combined create an SRAM cell array that generates a unique and random 300-bit response after power-up.

B. Performed Experiments

PUF-based systems are designed to reconstruct the enrolled key under extreme operation conditions. Hence, it is crucial to test fingerprint repeatability for extreme temperatures and voltage ramp-up times. However, it is only during enrollment that the devices uniqueness might be vulnerable due to the helper data. Therefore, uniqueness is only evaluated for enrollment condition.

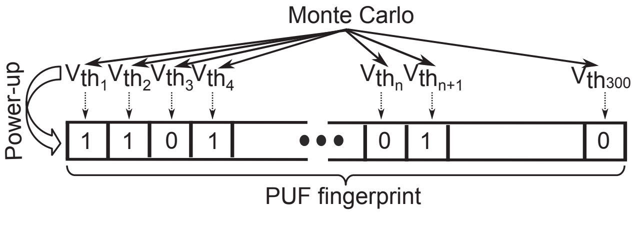

Monte Carlo
Power-up
V_{th_1} V_{th_2} V_{th_3} V_{th_4}
V_{th_n} $V_{th_{n+1}}$
$V_{th_{300}}$
1 1 0 1
0 1
0
PUF fingerprint

Fig. 3: SRAM PUF simulation [17]

To investigate the impact that technology scaling, temperature *Temp* and voltage ramp-up time t_{ramp} have on the repeatability and uniqueness, we simulated the power-up of the SRAM cell array for two experiment groups: repeatability experiments and uniqueness experiments.

Repeatability experiments: for each combination of design, technology node, *Temp* and t_{ramp}, we simulated the power-up of the SRAM cell array 20 times and evaluated its response. The transient noise during power-up is randomly generated by the simulation tool; hence, five variable parameters are used for the simulation:

- Design (GP, LP)
- Technology node (45nm, 32nm)
- Temperature (*Temp*) (-40^{o}C, 25^{o}C, 85^{o}C)
- Voltage ramp-up time (t_{ramp}) (10μs, 50μs, 90μs)
- Transient noise (different for each of the 20 power-ups)

Hence, a total of 720 simulations are performed (2 designs $\times$ 2 technology nodes $\times$ 3 *Temp* $\times$ 3 t_{ramp} $\times$ 20 transient noise).

Uniqueness experiments: at enrollment conditions (*Temp* = 25^{o}C and t_{ramp}= 10μs) for the considered designs and technology nodes, we analyzed a subset of the performed simulations results in the previous experiments with focus on uniqueness. Three variable parameters are used for the analysis:

- Design (GP, LP)
- Technology node (45nm, 32nm)
- Transient noise (different for each of the 20 power-ups)

Note that the simulations were carried out with the technology nodes mentioned above (45nm and 32nm) as the PTM models are available for both considered designs (GP and LP) and technology nodes.

C. Simulation Results

Fig. 4 and Table II show the simulation results for repeatability and uniqueness, respectively.

Repeatability: Fig. 4 shows the impact on FHD, hence, on SRAM fingerprint repeatability. The vertical axis (y axis) represents the FHD over the 20 measurements; the mean value is plotted in a gray box, the maximum value (max) over the 20 measurements in a white box and the standard deviation (std) as a black line in the center of the boxes. In the horizontal axis (x axis), the information is grouped first per *Temp* and thereafter per t_{ramp}. Each device is assigned a letter; a - 45nm GP, b - 32nm GP, c - 45nm LP and d - 32nm LP. Moreover, the enrollment conditions are highlighted in yellow (light gray if printed in black and white). From the figure, we can observe

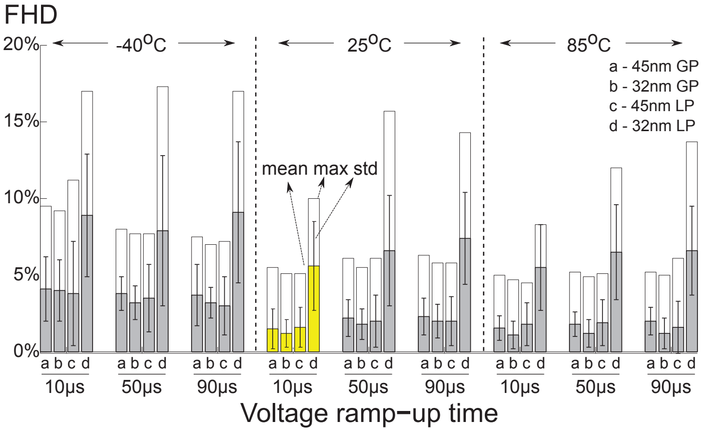


Fig. 4: Repeatability results - simulations

TABLE II: Uniqueness results - simulations

	45nm GP	32nm GP	45nm LP	32nm LP
FHW	48% ± 2.3%	53% ± 2.9%	49% ± 2.6%	54% ± 3.5%

that GP and LP devices are impacted by *Temp*, t_{ramp} and technology scaling as follows:

Temperature impact at constant t_{ramp} (10μs): Regardless of the design, FHD (noise) is higher for extreme temperatures; e.g., for 45nm GP, mean FHD at -40^oC is 2.7× higher than that of 25^oC and 2.5× than that of 85^oC. Moreover, -40^{o}C has the highest max and std FHD.

Voltage ramp-up time at constant *Temp* (25^{o}C): GP devices are less sensitive to t_{ramp} variations than LP devices; e.g., 32nm GP FHD increases marginally for all different t_{ramp}, while 32nm LP max FHD increases 1.5×. Low-Power devices vulnerability to t_{ramp} variations can be explained by the slow response of these devices to frequency variation, as they have higher threshold voltage to minimize the leakage current.

Temperature and Voltage Ramp-Up Time Combined: Regardless of the design, for *Temp* lower than enrollment, a noise reduction is observed for t_{ramp} longer than enrollment; however, for *Temp* higher than enrollment, short t_{ramp} are the least noisy. For example, 45nm GP at -40^{o}C FHD is the lowest for 90μs, but for 85^{o}C FHD is lowest for 10μs. These results reveal a correlation between *Temp* and t_{ramp} that can be used to decrease noise by appropriate selection of t_{ramp} to the *Temp*. These results are in line with [17].

Technology scaling: LP devices are more sensitive to both *Temp* and t_{ramp} variations. Moreover, technology scaling reduces noise for GP designs, while it increases for LP designs. For example, GP FHD reduces by 0.93× with technology scaling while LP increases by 2×.

Uniqueness: Table II shows the impact that design type and technology node have on the uniqueness of an SRAM fingerprint. Note that uniqueness is evaluated only at enrollment condition. The table shows the FHW average over 20 measurements with its respective standard deviation. FHD between devices is not calculated as only one device per combination of design and technology node is simulated. The table reveals that, regardless of the technology node, both designs have a balanced distribution of 0s and 1s, indicating good uniqueness; e.g., 45nm GP has an FHW of 48% ± 2.3%.

IV. Industrial based analysis

The simulation results are validated using silicon devices. For this purpose, we perform measurements on two SRAM designs manufactured in two technology nodes (SRAM module providers not disclosed due to IP constrains). In this section, first, we introduce the devices and thereafter the measurements carried out. Finally, we present the repeatability and uniqueness results, compare them with the simulation results and discuss the differences between the two designs.

A. Devices under consideration

To study the variation of repeatability and uniqueness of SRAM fingerprints, 100 SRAM devices distributed over two designs (65nm GP, 45nm GP, 65nm LP and 40nm LP), are evaluated. This information is summarized in Table III. Note that the simulated technology nodes and measured ones are not exactly the same; this because the available simulation models are limited. Nevertheless, the correlation and trends between simulations and silicon data can still be derived from them.

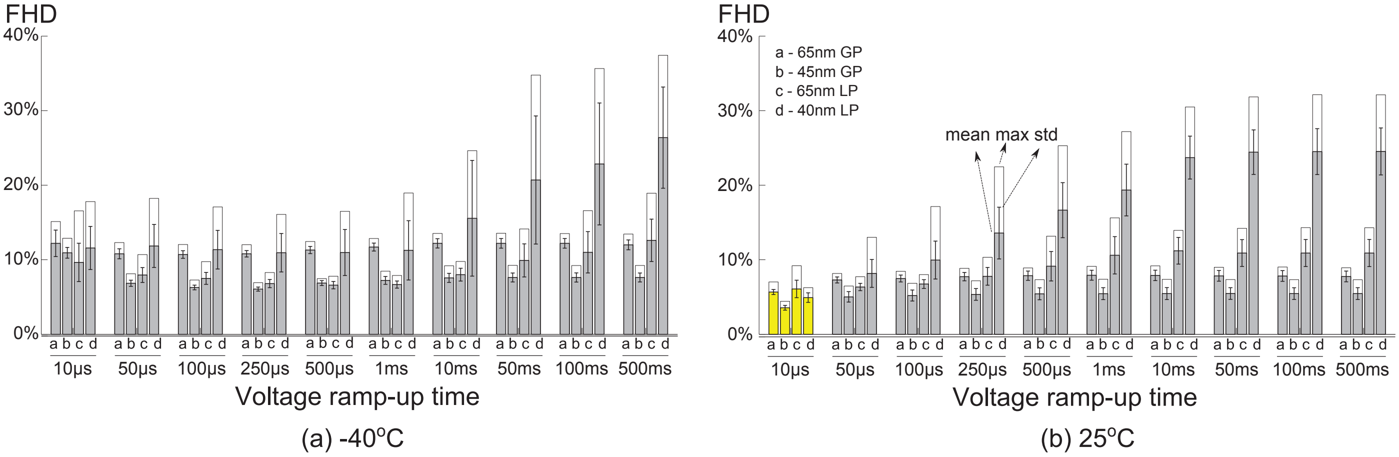
B. Performed Measurements

Similarly to the simulation experiments, we evaluate the repeatability and uniqueness of each of the SRAM devices (GP and LP), considering various temperatures, voltage ramp-up times and temperature and voltage ramp-up combined, as follows. Note that we consider only the first 2k bits of each device, as this is the typical size required to deploy a secure *Key* [22].

Temperature: we evaluate SRAM PUF repeatability for a wide range of *Temp* (-40^{o}C, 25^{o}C and 85^{o}C). The devices are placed in a climate chamber at 25^{o}C. Then, *Temp* is decreased to -40^{o}C. Next, *Temp* is increased to 25^{o}C and 85^{o}C. Finally, *Temp* is decreased to 25^{o}C. This is repeated twice. When the devices reach the temperatures of interest, 50 measurements are performed per device, making a total of 250 measurements per device. Between measurements, there is a power-off time of 1 sec, to make sure that all capacitances are discharged and hence prevent the impact on the new PUF response. Every temperature increase/decrease is performed at a speed of 3^{o}C/min. The settling time on desired temperature is 5 mins.

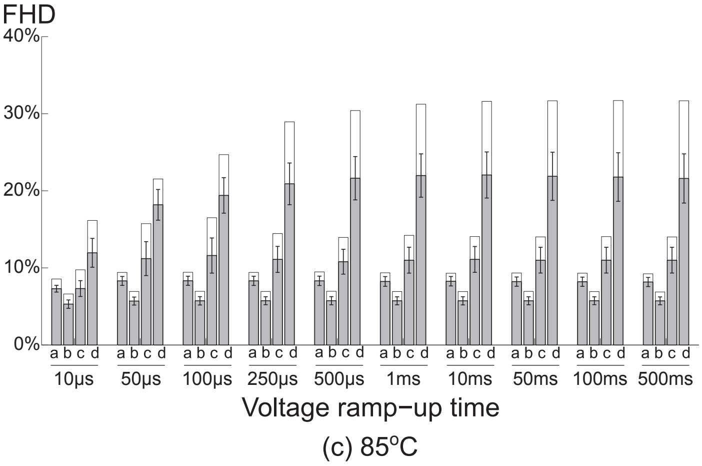
TABLE III: SRAM devices under test characteristics

Technology	#	Geometry	Size (Bytes)
65nm	30	128×128	2048
65nm LP	6	2048×16	4096
	4	1024×160	20480
	4	4096×64	32768
	4	4096×320	163840
	4	4096×80	40960
	4	128×128	2048
	4	512×128	8096
45nm	5	16384×8	16384
	5	32×320	1280
	5	128×128	2048
	5	1024×128	16384
40nm LP	5	16384×8	16384
	5	32×320	1280
	5	1024×8	1024
	5	8×256	256



(a) -40^{o}C

(b) 25^{o}C



(c) 85^{o}C

Fig. 5: Repeatability results - industrial experiments

Voltage ramp-up time: we evaluate SRAM PUF repeatability for a wide range of t_{ramp} (10μs, 50μs, 100μs, 250μs, 500μs, 1ms, 10ms, 50ms, 100ms, 500ms). The devices are placed in a test setup which is suitable for varying ramp-up time of the IC core voltage. At each t_{ramp} the devices are powered-up, read, powered-off for 1 sec and powered on again. There are 20 measurements taken per t_{ramp}.

Temperature and voltage ramp-up time combined: we repeat the voltage ramp-up test for each of the considered temperatures.

All measurement results are stored in a binary dump. These binary dump files are analyzed using MATLAB.

C. Measurement Results

Repeatability: Fig. 5 shows the repeatability results. From the figure, the following observations can be made.

Temperature impact at constant t_{ramp} (10μs): Regardless of the design, FHD is higher for extreme temperatures, in particular for -40^{o}C; e.g., FHD at -40^{o}C for 65nm GP is 2.2× higher than that of enrollment and 1.7× higher than that of 85^{o}C.

Voltage ramp-up impact at constant *Temp* (25^{o}C): GP devices are negligibly impacted by t_{ramp}; e.g., 65nm GP FHD mean increases by 1.3× when t_{ramp} is increasing from $10\mu s$ to 500ms. However, LP devices are more sensitive to t_{ramp} variations; e.g., 65nm LP FHD mean increases by 2.4× when t_{ramp} increases from $10\mu s$ to 500ms. Hence, almost 2× more sensitive. Moreover, the same trend is also valid for the standard deviation. Finally, regardless of the design, FHD increases with t_{ramp} until saturation.

Temperature and voltage ramp-up combined: Regardless of the design, FHD is lower at -40^{o}C for t_{ramp} longer than the one used for enrollment, while at 85^{o}C FHD is lower if a short t_{ramp} is used. For example, at -40^{o}C the FHD mean for 65nm GP is the lowest for 50μs, while at 85^{o}C the mean FHD is the lowest for 10μs.

Technology scaling: FHD for GP improves with technology scaling, while it deteriorates for LP. For example, at 85^{o}C and 10μs, FHD reduces by 1.2× for GP, while it increases by 1.6× for LP. The difference is further emphasized with longer t_{ramp}; e.g., at 85^{o}C and 500ms, HD reduces by 1.4× with GP design, while it increases by 2.0× with LP design.

Uniqueness: Table IV shows the uniqueness results. From the table, two main observations can be made:

1) Regardless of the design, FHD between devices shows a good distance between fingerprints at enrollment for all devices; e.g., 65nm GP has an FHD of 50% ± 0.42% between devices.

2) Both designs and technology node present a good distribution of 0's and 1's, which is a good uniqueness indicator; e.g, 65nm GP has an FHW of 50% ± 1%.

D. Comparison: Simulation vs. Silicon

Repeatability: simulation results show that GP devices are less sensitive to varying operation conditions, keeping FHD virtually constant, and that technology scaling reduces its FHD by 0.93×. Silicon measurements show the same trend, however with even more severe values; varying operation conditions impact FHD up to 1.3× while technology scaling reduces FHD by 1.4×. Overall, GP is up to 4.5× better than LP; e.g., at 25^{o}C for 500ms max FHD is 4.5× higher for 40nm LP than for 45nm GP.

Uniqueness: simulation results indicate a good FHW, however the other metrics were not conclusive due to the limited amount of simulated PUF bits and number of devices simulated. The industrial measurements show good uniqueness values for for all investigated devices, therefore, revealing that uniqueness is not impacted by design (GP or LP).

TABLE IV: Uniqueness results - industrial experiments

	65nm GP	45nm GP	65nm LP	40nm LP
FHD (between devices)	50% ± 0.42% (min = 48.73%)	49.85% ± 0.63% (min = 48.54%)	49.90% ± 0.51% (min = 47.30%)	49.23% ± 1.05% (min = 46.74%)
FHW (at enrollment)	50% ± 1%	50% ± 0.5%	50% ± 2.5%	50% ± 0.5%

E. Discussion

The superior performance of GP devices over LP devices for PUF purpose can be explained as follows. GP devices have lower threshold voltages to enhance speed when compared with LP devices. This lower threshold voltage makes them more vulnerable to process variation. While in most applications vulnerability to process variation is a concern, in PUF applications it enhances the asymmetry of the cross-coupled inverters of the SRAM cell; hence putting the SRAM cell in a repeatable state rather than in a random state on power-up. Therefore making the SRAM PUF cell more robust. However, with technology scaling, despite at enrollment condition the previous statement holding true, for the remaining stress conditions LP devices become more vulnerable. Increased LP vulnerability is particularly evident with respect to t_{ramp} variations, as LP devices respond poorly to frequency variations.

The validity of our results holds across the investigated designs, despite the discrete number of devices available. However, the absolute noise values may vary when other technology nodes and manufacture process are considered, the trends are solid. This is due to the very nature of the designs. GP devices, when compared with LP devices will always perform better with varying voltage ramp-up times, due to their intrinsic lower V_{th}.

Regarding the cost of each design in terms of power consumption and area overhead. As PUF-based systems are active only during the start-up of a device to generate the key, delay and power consumption play very minor roles. Therefore, we consider the area overhead to be the main design constrain. With this respect, GP devices have a lower footprint when compared with LP devices (see Table I) [15]. Moreover, the lower the noise in PUF responses, the smaller the PUF size required to design a robust PUF system [5,18]. As SRAM PUF GP devices are less noisy and more robust when compared with its LP counterparts, we can predict that PUF systems based on GP SRAMs will result in a significant overall smaller area. More specifically, according to [5,9], when the system is designed to correct a maximum noise of 15%, SRAM corresponds from 585B (or 77% out of 6.1k gates) up to 1kB (or 92% out of 9.3k gates) of the overall area overhead of a PUF-based system, depending on the ECC type. When a higher error correction capability is required, e.g., error correction up to 30%, SRAM footprint increases from 585B to 2kB and from 1kB up to 3.5kB, depending on the ECC type. This simple analysis shows the potential of choosing appropriate memory design, e.g., 45nm GP over 40nm LP, as it reduces the footprint of the PUF-based system circa 3×.

From a security point of view, due to higher electrical currents, GP devices might be more vulnerable to being cloned according to [21]. However, the complexity and required tools to perform the attack are not accessible for the average attacker.

V. Conclusion

In this paper we demonstrated SRAM PUF robustness for both GP and LP designs, by evaluating their repeatability and uniqueness for a wide range of temperatures and voltage ramp-up times, using circuit simulations and industrial measurements. The results show that GP designs are up to 2× less sensitive to varying operating conditions. Moreover, GP designs improve their robustness with technology scaling by 1.4× while LP deteriorates by 2.0×. Overall, using GP SRAM PUFs will result in more robust and cheaper PUF-based systems.

Acknowledgments

The authors would like to thank Intrinsic-ID B.V. for providing the silicon data used in this work.

References

[1] R. Pappu, *Physical One-Way Functions*, Ph.D. Thesis, 2001.

[2] J. Guajardo et al., *FPGA Intrinsic PUFs and Their Use for IP Protection*, CHES, 2007.

[3] B. Skoric et al, *Robust Key Extraction from Physical Unclonable Functions*, Applied Cryptography and Network Security, 2005.

[4] Y. Dodis, L. Reyzin, and A. Smith, *Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data*, Advances in Cryptology - Eurocrypt, 2004.

[5] M. Cortez et al., *Intelligent Voltage Ramp-up Time Adaptation for Temperature Noise Reduction on Memory-based PUF Systems*, to appear in: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 2015.

[6] R. Maes and I. Verbauwhede, *Physically Unclonable Functions: A Study on the State of the art and Future Research Directions*, Towards Hardware-Intrinsic Security, Information Security and Cryptography, 2010.

[7] M. Cortez et al., *Modeling SRAM Start-Up Behavior for Physical Unclonable Functions*, DFT, 2012.

[8] D.E. Holcomb et al., *Power-up SRAM State as an Identifying Fingerprint and Source of True Random Number*, IEEE Trans. on Computers **vol.58** (2009), no. 9, 1198–1210.

[9] R. Maes et al, *A Soft Decision Helper Data Algorithm for SRAM PUFs*, IEEE Int. Symp. on Information Theory, 2009.

[10] J. Guajardo et al., *Physical Unclonable Functions and Public-key Crypto for FPGA IP Protection*, FPL, 2007.

[11] J. Guajardo et al., *FPGA Intrinsic PUFs and Their Use for IP Protection*, CHES, 2007, pp. 63–80.

[12] M. Hofer and C. Boehm, *An Alternative to Error Correction for SRAM-like PUFs*, CHES, 2010.

[13] M. Claes, V. vd Leest, and A. Braeken, *Comparison of SRAM and FF PUF in 65nm Technology*, NordSec, 2011.

[14] J.-P. Linnartz and P. Tuyls, *New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates*, AVBPA, 2003.

[15] ITRS, *MASTAR*, 2013.

[16] W. Zhao et al., *Rigorous Extraction of Process Variations for 65nm CMOS Design*, European Solid State Device Research, 2007.

[17] B. Preneel V. vd Leest E. vd Sluis, *Soft Decision Error Correction for Compact Memory-Based PUFs using a Single Enrollment*, CHES, 2012.

[18] M. Cortez et al., *Adapting voltage ramp-up time for temperature noise reduction on memory-based PUFs*, HOST, 2013.

[19] Y. Cao W. Zhao, *New generation of Predictive Technology Model for sub-45nm early design exploration*, IEEE Trans. on Electron Devices, 2006.

[20] Y. Dodis et al., *Fuzzy extractors: How to generate strong keys from biometrics and other noisy data*, SIAM Journal on Computing, 2008.

[21] C. Helfmeier et al., *Cloning Physically Unclonable Functions*, HOST, 2013.

[22] R. Maes et al., *Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs*, CHES, 2009.