Power-up control techniques for reliable SRAM PUF

Juyun Lee1, Dong-Woo Jee2, and Dongsuk Jeon1(a)

Abstract Physically unclonable function (PUF) is a widely used hardware-level identification method. SRAM PUFs are the most well-known PUF topology, but they typically suffer from low reproducibility due to non-deterministic behaviors and noise during power-up process. In this work, we propose two power-up control techniques that effectively improve reproducibility of the SRAM PUFs. The techniques reduce undesirable bit flipping during evaluation by controlling either evaluation region or power supply ramp-up speed. Measurement results from the 180 nm test chip confirm that native unstable bits (NUBs) are reduced by 54.87% and bit error rate (BER) decreases by 55.05% while reproducibility increases by 2.2x.

Keywords: physically unclonable function, power-up control, SRAM

Classification: Integrated circuits

1. Introduction

Implementing secure hardware is one of the key issues in IoT (Internet of Things) devices such as wearable platforms and autonomous vehicles. Physically unclonable functions (PUFs) are frequently adopted in those IoT devices as identification and other security measures. Typically, PUF circuits generate die-specific unique key values using process variations such as threshold voltage mismatch of MOSFET transistors. Process variations occur innately during fabrication process, and hence a unique fingerprint can be assigned to each die at a low cost [1].

In the last decade, studies on PUFs have been carried out extensively in various ways. For instance, authors in [2] propose a PUF based on the resistance variations in the power grids. At the circuit level, different PUF cell circuit topologies have been proposed, e.g., static random-access memories (SRAMs) [3, 4, 5], proportional to absolute temperature (PTAT) voltage generators [6], NAND gates [7], current mirrors [8], analog amplifiers [9], ternary content addressable memory (TCAM) [10], sub-threshold current array [11], and leakage-based PUF [12]. In [3], delay variation is used in the clock path to generate PUF outputs, and a post processing circuit is exploited to improve robustness further. In [4], the authors propose a modified SRAM with additional reset transistors, which achieves higher stability than a typical SRAM. In [9], a sub-threshold amplifier-based PUF cell is presented, demonstrating good reproducibility with smaller area and power consumption. Among a number of PUF cell designs, SRAM bit cell is still widely used since it has a wide operation region and can be easily incorporated into the standard digital design flow. Also, SRAMs can easily provide enough number of PUF output values to generate keys long enough for devices that are produced in large quantities [13].

Despite of the simple design process, SRAM PUFs have a reliability issue since they exhibit proneness to evaluation errors, causing native unstable bits (NUBs) in the array. Various post processing methods have been proposed to resolve this issue. For instance, the temporal majority voting (TMV) is a method to take the majority of the results of multiple evaluations using a counter [3, 6, 9]. In [13], the authors propose a bit selection algorithm that utilizes the spatial correlation in the SRAM cell array, whereas the authors in [14] propose an algorithm to select uncorrelated bits under various environment conditions. In [15], SRAM blocks are tested under different long-term storage scenarios to capture the effect of the negative-bias temperature instability (NBTI) on the PUF reliability and data-dependent operations are proposed to mitigate this issue. In [16, 17], temperature compensation scheme is exploited to improve stability for PUF.

In this work, we investigate the vulnerability of SRAM PUF cells during the initialization process and propose to enhance reliability by adopting power-up sequence control schemes. The proposed schemes effectively suppress evaluation errors and improves PUF reliability with minimal circuit and system overheads.

The rest of this paper is organized as follows. In Section II, we briefly describe and analyze the terms and metrics necessary to understand the reliability of the SRAM PUF cells. Section III introduces the proposed power-up control techniques to improve reproducibility. Section IV analyzes measurement results from the test chip. Finally, Section V summarizes the work.

2. SRAM PUF

A typical 6T SRAM bit cell consists of two cross-coupled inverters and two access transistors as shown in Fig. 1. When a bit cell is powered on or reset, the internal nodes start evaluation through positive feedback of the inverter loop. If the transistors in the cross-coupled inverters are not perfectly balanced due to transistor mismatch, each internal node is skewed toward either 0 or 1. Since transistor threshold voltage mismatch generally follows a well-de-
For the responses of the PUFs to be used as a fingerprint, each instance must produce a unique value. Uniqueness refers to the degree of the dissimilarity of responses from different PUFs for the same challenge. Inter-chip Hamming distance (inter-HD) measures the Hamming distance between the responses of two chips for the same input. Assuming an ideal random distribution, inter-HD should approach 50%.

2.2 Reproducibility
Ideally, PUFs must generate the same fingerprint for the same input across different operating conditions for reliable operation. Reproducibility refers to the degree of response variation when evaluating the response from a PUF module, which is typically computed as the intra-chip Hamming distance (intra-HD). Intra-HD captures how many bits are altered when the responses are measured multiple times for a single PUF instance. For ideal error-tolerant PUF devices, intra-HD should be zero.

2.3 Hold static noise margin (SNM)
The hold SNM is a metric for measuring the static stability of cross-coupled inverters in the SRAM [19, 20]. The hold SNM is defined as the maximum amount of noise that can be tolerated in the SRAM without flipping the state when noise interferes with the bit cell. Fig. 2 shows the voltage transfer curves (VTCs) of the inverters (INV0, INV1). The hold SNM is calculated as the largest square that fit inside of each eye in the VTC. If INV0 and INV1 are identical, two squares will have the identical size. In practice, however, due to transistor mismatch the squares possess different areas and the internal node tends to converge towards 0 or 1.

2.4 Bit error rate (BER)
BER is the average ratio of bit errors occurring in each sampling [21]. BER is generally tightly coupled with native unstable bits (NUBs); for instance, as NUBs decrease BER also tends to be reduced.

Post processing such as TMV [3] and error correction code (ECC) [22] is often employed to correct errors in the final response. However, the higher BER there exist in the PUF, the more cost required for post processing.

2.5 PUF static noise margin ratio (PSNM\text{ratio})
The authors in [23] analyze the SRAM start-up behavior and suggest another metric, PUF static noise margin (PSNM) to quantify the degree of skewness of an SRAM bit cell. PSNM\text{ratio} determines the direction and degree of skewness, where the value larger than 1 implies the power-up state tendency of 1. PSNM\text{ratio} can be acquired by noise margins (NM and \overline{NM}) of the VTC. The NM and \overline{NM} are calculated using the values at four points of the VTC where \frac{dv_{out}}{dv_{in}} = -1 in the VTC of the SRAM as follows:
\begin{equation}
NM = \min(V_{OH} - V_{HI}, V_{IL} - V_{OL})
\end{equation}
\begin{equation}
\overline{NM} = \min(V_{OH} - V_{HI}, V_{IL} - V_{OL})
\end{equation}

For INV1, which is the right side inverter of the SRAM cell in Fig. 1, the output is \(V_{OH}\) and \(V_{OL}\) when the input is \(V_{IL}\) and \(V_{HI}\), respectively. Similarly, the output voltages \(V_{OH}\) and \(V_{OL}\) of INV0 are obtained when the input is \(V_{IL}\) and \(V_{HI}\). PSNM\text{ratio} is defined as the ratio of the two noise margins.
\begin{equation}
PSNM\text{ratio} = NM/\overline{NM}
\end{equation}

3. Improving reliability through power-up control
As an SRAM array is turned on by raising power supply voltage, each bit cell starts evaluation when it reaches its minimum operating point where hold SNM becomes large enough to skew toward 0 or 1 and hold the value. If the ramp up speed of the SRAM power supply is not well defined, the PUF cell may be exposed to varying amount of noise during each evaluation.

This issue has been studied in various ways in prior works. The authors in [24] suggests an SRAM test methodology that identifies unreliable bit cells during power-up using additional test circuitry in the SRAM array. In [25], SRAMs in microcontroller ICs are tested under several power supply conditions, but the work does not provide detailed experiments solely focused on the power-up sequences.

In [26], it was hinted that increasing supply voltage very slowly would make each bit cell evaluate at its expected state.
minimum operating voltage where the SNM is skewed most and the lowest bit error rate is achieved, and the authors in [27] suggest to use different supply voltage change speeds and directions to detect unreliable cells. The authors in [28] propose to manipulate the ramp-up speed to cancel out the effect of the variation of operating temperature. The ramp-up speed was controlled by programming an external power supply, and it was shown that the PUF cell produce results similar to the ones obtained at nominal temperature by altering the ramp-up speed.

Alternatively, here we propose simple power-up control schemes to improve the reproducibility of SRAM PUFs that can be fully integrated on chip, and confirm their effectiveness both in simulation and measurements. In this section, two power-up sequence control techniques are proposed: 1) utilizing the characteristics of the transistors in the sub-threshold region, and 2) manipulating the voltage ramp-up speed during the power-up sequence. Both techniques minimize the effect of circuit noise on the evaluation process and achieve an optimal operating point in terms of PUF cell reliability.

### 3.1 Scheme 1: developing fingerprint in sub-threshold region

In the sub-threshold region, the effect of transistor mismatch is exaggerated compared to the near- or super-threshold regions [29], and consequently the butterfly curve of an SRAM bit cell shows more asymmetric hold SNMs as shown in Fig. 2(b). Since the state with smaller hold SNM is highly prone to upset, the bit cell in such a state ultimately exits the state and settles into the opposite one where the hold SNM is significantly larger [30].

To analyze the relationship between the PUF reliability and the operating voltage, we simulated the switching point voltage ($V_{\text{switch}}$) variation of a minimum sized inverter while sweeping the supply voltage using Monte-Carlo simulations. $V_{\text{switch}}$ is the voltage where the output is equal to the input voltage. If $V_{\text{switch}}$ deviates from the half-$V_{\text{DD}}$ point more, the probability of large relative skewness of the cross-coupled inverter increases since the skewness of hold SNM is proportional to the difference between $V_{\text{switch}}$ values of the back-to-back inverters. In simulation, the $V_{\text{DD}}$ is swept from 300 mV to 1.8 V in 300 mV steps, and the results are shown in Table I. Although the absolute amount of skewness is proportional to $\sigma$, at lower operating voltages other factors such as circuit speed and power supply-related noises including $Ldi/dt$ and IR drop are decreased as well due to reduced current draw. Therefore, we calculate the $\sigma/V_{\text{DD}}$ to compare the amount of $V_{\text{switch}}$ variation with respect to $V_{\text{DD}}$. In the sub-threshold region, the variation is significantly larger than the near- or super-threshold regions, so we achieve a larger relative skewness in the sub-threshold region.

We also obtained the $\text{PSNM}_{\text{ratio}}$ from 1 K Monte-Carlo simulations while varying the $V_{\text{DD}}$ of the SRAM PUF from 300 mV to 1.8 V. Fig. 3 shows the simulated histogram of $\text{PSNM}_{\text{ratio}}$. In the histogram (Fig. 3), the x-axis represents the PSNM ratio value, and the y-axis represents the normalized count. Table II shows the standard deviation and mean of $\text{PSNM}_{\text{ratio}}$ with respect to $V_{\text{DD}}$. The results show that the variation of $\text{PSNM}_{\text{ratio}}$ is larger at lower $V_{\text{DD}}$. This means that the relative skewness is greater at low voltages. In other words, a cell with a low amount of transistor mismatch can still exhibit reliable operation at a low $V_{\text{DD}}$, due to the enlarged relative skewness. Consequently, the reproducibility is improved if the response of the PUFs is developed in the sub-threshold regime for both enrollment and reconstruction phases. Note that an SRAM bit cell can be susceptible to noise when it operates at minimum possible operating voltage ($V_{\text{min}}$) where its hold margin is almost zero. However, for higher voltages still in sub-threshold regime, it can stay for a long time without losing stored values. Therefore, it is important to develop the SRAM responses at an optimal voltage.

### 3.2 Scheme 2: controlling voltage ramp-up speed

The effect of the developing response in the sub-threshold region can be also realized by making the ramp-up speed of $V_{\text{DD}}$ very slow. The SRAM bit cells are stabilized immediately after the $V_{\text{DD}}$ arrives at the minimum operation voltage $V_{\text{min}}$ of the SRAM, which is typically well below the super-threshold region. However, the hold SNM becomes very small near $V_{\text{min}}$ and hence the operation becomes unreliable if the $V_{\text{DD}}$ stays there for a long time, which implies that the SRAM would be susceptible to noise if the ramp-up speed is very slow, which disagrees with the prediction from [26]. This also explains the observations in [28], where the authors show that the slowest

| $V_{\text{DD}}$ (V) | $\mu$ (mV) | $\sigma$ (mV) | $\sigma/V_{\text{DD}}$ |
|-------------------|------------|--------------|----------------------|
| 0.3               | 98.78      | 19.76        | 0.066                |
| 0.6               | 240.4      | 20.94        | 0.035                |
| 0.9               | 386.2      | 23.04        | 0.026                |
| 1.2               | 517.5      | 25.02        | 0.021                |
| 1.5               | 630.0      | 26.68        | 0.018                |
| 1.8               | 734.6      | 27.88        | 0.015                |

| $V_{\text{DD}}$ (V) | $\mu$ | $\sigma$ |
|-------------------|------|---------|
| 0.3               | 1.0841 | 0.7173  |
| 0.4               | 1.0209 | 0.1554  |
| 1.7               | 1.0030 | 0.0348  |
| 1.8               | 1.0030 | 0.0349  |
ramp-up speed is not necessarily an optimal operating point to suppress errors. Therefore, to maximize the PUF reliability one needs to finely control the ramp-up speed and operate the design at an optimal point while minimizing circuit overheads.

To achieve this goal, we propose a digitally-controlled ramp-up manipulation circuit depicted in Fig. 4. The proposed circuitry consists of two parts, the binary-weighted power gates along with additional gate transistors biased by $V_B$ and the control transistors which takes digital signals for finer speed control. While the lower power transistors are binary-weighted, the amount of current flowing through each control transistor can be further adjusted through $V_B$.

4. Measurement results

A test chip incorporating SRAM PUFs along with the proposed circuitry is fabricated in 180 nm CMOS process. Fig. 5 shows the die photo of the fabricated chip. The proposed power-up control schemes are tested on 20 chips in total. Each chip includes a 256-bit SRAM cell array with a readout circuitry and the power gates shown in Fig. 4. The total area is 17,181 µm², where the proposed power control circuit occupies 2,158 µm² (66,604 F²).

The measurement setup is shown in Fig. 5. An external digital-to-analog converter (DAC) generates the supply voltage of the SRAM cell array, and an FPGA board controls both the DAC output voltage and the on-chip power gate control signals. We used MCP4725 DAC with the driving current of 210 µA and settling time of 6 µs.

First of all, the fingerprints are captured from each chip with $V_B = 0$ V and $\text{Ramp}[7:0] = 255$ to obtain the fastest ramp-up speed. These results are used as baseline in the experiments since this represents a typical SRAM case where no power gate exists.

To evaluate scheme 1, we control the initialization voltage ($V_i$) of the SRAM. The DAC output voltage first moves from 0 V to the desired $V_i$ instantly as shown Fig. 6. Since the ramp-up speed of DAC is fast enough (0.55 V/µs in datasheet), the bit cells evaluate the fingerprints at this $V_i$ and we can determine the effect of evaluation voltage of the SRAM PUF on the bit error rates. We measured NUBs and BER when the supply voltage is directly increased to 1.8 V and when the supply is initialized to a lower starting point that varies from 100 mV to 900 mV with 100 mV step size. Fig. 7 illustrates measurement results obtained from a single die. The results confirm that both NUBs and BER drop noticeably in the deep sub-threshold region which is below 300 mV.

For scheme 2, we measure those metrics while changing the control signals of the ramp-up speed control circuit ($V_B$ and $\text{Ramp}[7:0]$). The control signals $V_B$ and $\text{Ramp}[7:0]$ enable coarse and fine tuning of the ramp-up speed, respectively. As anticipated in the previous section, there exists an optimal point in terms of reliability as shown in Fig. 8.

Using the measurement procedure above, the proposed power control schemes are tested across 20 dies in total.
Fig. 8. Measurement results for Scheme 2. X-axis represents the control values of the power gates in Fig. 4.

Fig. 9. Measured NUB ratio and BER across 20 chips.

Fig. 9 shows the ratio of NUBs of the baseline and the case when the scheme 1 is applied, where the number of NUBs decreases after applying the scheme 1 for all 20 dies. Likewise, BER is also reduced when compared to the baseline. The number of NUBs and BER averaged over all dies are reduced by 35.11% and 38.27%, respectively.

For each die, we find the optimal ramp-up speed at which NUBs and BER are minimized by sweeping Ramp[7:0]. In Fig. 9, the values representing scheme 2 are obtained from the optimal points. The measurements confirm that BER and NUBs are lowered for all chips when scheme 2 is applied. NUBs are reduced by 54.87% and BER decreases by 55.05%, suggesting that scheme 2 is more effective technique than scheme 1 in mitigating evaluation errors. The BER improvements under different temperatures across 10 dies are shown in Fig. 10, which confirms both scheme are effective at all temperatures. At higher temperatures, the scheme 1 exhibits larger improvements, whereas the scheme 2 is more effective at lower temperatures.

Fig. 11(a) represents the distribution of the normalized Hamming distance (HD). For the baseline, inter-chip HD has $\mu = 0.475$ and $\sigma = 0.030$ while intra-chip HD shows $\mu = 0.064$ and $\sigma = 0.014$. The value exhibits 7.4x mean separation between intra and inter-chip HD. With scheme 1, the separation becomes 15.7x that is 2.12x higher than the baseline. In the case of scheme 2, 16.3x mean separation is achieved, exhibiting 2.2x higher value than the baseline. The measurement results confirm that the proposed schemes improve both the reproducibility and the uniqueness of the SRAM PUFs. Fig. 11(b) shows the distribution of the bit-aliasing, which represents the correlation of each cell across multiple dies. The value should be 0.5 in the ideal case without biasness. The average bit-aliasing is improved from 0.39 to 0.49 for scheme 1 and to 0.43 for scheme 2.

5. Conclusion

This paper presents power-up sequence control techniques to reduce the evaluation errors of SRAM PUF. We first propose a method of developing responses in the sub-threshold region, which intentionally skews SNM more for reliable evaluation. The second scheme controls the power supply voltage ramp-up speed and operates the PUFs at the optimal operating point. The on-chip power control circuitry provides coarse grain tuning based on the bias voltage and fine grain tuning by digital control signals.

We demonstrate the validity of the two proposed schemes with both SPICE simulations and measurements from 180nm test ICs. The proposed schemes successfully reduce both BER and NUBs, and hence improve the reliability of the SRAM PUFs without additional post processing circuitry.

Acknowledgments

This work was supported by the National Research Foundation of Korea under Grants NRF-2019R1C1C1004927 and NRF-2016R1C1B2016072, and by the Information Technology Research Center Support Program Supervised by the Institute for Information and Communications Technology Promotion under Grants IITP-2019-0-01421. This work was also supported by the Technology Innovation Program (10074267, Development of the Miniaturized Sensor Module Technology for 3D Finger Vein Recognition using Ultrasound based on 500dpi Class High Resolution) funded by the MOTIE, Korea.

References

[1] G. E. Suh and S. Devadas: “Physical unclonable functions for device authentication and secret key generation,” DAC (2007) 9.

[2] R. Helinski, et al.: “A physical unclonable function defined using power distribution system equivalent resistance variations,” DAC (2009) 676 (DOI: 10.1145/1629911.1630089).
[3] S. K. Mathew, et al.: “A 0.19 pJ/bit PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22 nm CMOS,” ISSCC Dig. Tech. Papers (2014) 278 (DOI: 10.1109/ISSCC.2014.6757433).

[4] Y. Su, et al.: “A digital 1.6 pJ/bit chip identification circuit using process variations,” IEEE J. Solid-State Circuits 43 (2008) 69 (DOI: 10.1109/JSSC.2007.910961).

[5] G. Li, et al.: “High performance bistable weak physical uncloneable function for IoT security,” IEICE Electron. Express 15 (2018) 20180879 (DOI: 10.1587/exle.15.20180879).

[6] J. Li and M. Seok: “Ultra-compact and robust physically uncloneable function based on voltage-compensated proportional-to absolute temperature voltage generators,” IEEE J. Solid-State Circuits 51 (2016) 2192 (DOI: 10.1109/JSSC.2016.2586498).

[7] B. Karpinsky, et al.: “Physically uncloneable function for secure key generation with a key error rate of 2E-38 in 45 nm smart-card chips,” ISSCC Dig. Tech. Papers (2016) 158 (DOI: 10.1109/ISSCC.2016.7417955).

[8] A. Alvarez, et al.: “15 fJ/static physically uncloneable functions for secure chip identification with <2% native bit instability and 140x inter/intra PUF hamming distance separation in 65 nm,” ISSCC Dig. Tech. Papers (2015) 256 (DOI: 10.1109/ISSCC.2015.7063023).

[9] K. Yang, et al.: “A 553F2 2-transistor amplifier-based physically uncloneable function (PUF) with 1.67 native instability,” ISSCC Dig. Tech. Papers (2017) 146 (DOI: 10.1109/ISSCC.2017.7870303).

[10] N. Tumuganti, et al.: “Novel TCAM-based PUF with improved reliability for hardware-entangled security,” IEICE Electron. Express 14 (2017) 20170716 (DOI: 10.1587/exle.14.20170716).

[11] X. Xi, et al.: “Strong subthreshold current array PUF with 2E5 challenge-response pairs resilient to machine learning attacks in 130 nm CMOS,” VLSI-C (2017) C268 (DOI: 10.23919/VLSIC.2017.8008503).

[12] J. Lee, et al.: “A 445F2 leakage-based physically uncloneable Function with lossless stabilization through remapping for IoT security,” ISSCC Dig. Tech. Papers (2018) 132 (DOI: 10.1109/ISSCC.2018.8310219).

[13] K. Xiao, et al.: “Bit selection algorithm suitable for high-volume production of SRAM-PUF,” HOST (2014) 101 (DOI: 10.1109/HST.2014.6855578).

[14] M. T. Rahman, et al.: “Systematic correlation and cell neighborhood analysis of SRAM PUF for robust and unique key generation,” J. Hardware and System Security 1 (2017) 137 (DOI: 10.1007/s41635-017-0012-3).

[15] R. Maes and V. van der Leest: “Countering the effects of silicon aging on SRAM PUFs,” HOST (2014) 148 (DOI: 10.1109/HST.2014.6855586).

[16] S. Tao and E. Dubrova: “An ultra-energy-efficient temperature-stable physical uncloneable function in 65 nm CMOS,” Electron. Lett. 52 (2016) 805 (DOI: 10.1049/el.2016.0292).

[17] S. Taneja, et al.: “Fully synthesizable PUF featuring hysteresis and temperature compensation for 3.2% native BER and 1.02 D/°b in 40nm,” IEEE J. Solid-State Circuits 53 (2018) 2828 (DOI: 10.1109/JSSC.2018.2865584).

[18] Y. Cai, et al.: “Threshold voltage distribution in MLC NAND flash memory: Characterization, analysis, and modeling,” DATE (2013) 1285 (DOI: 10.7873/DAT.2013.266).

[19] E. Seevinck, et al.: “Static-noise margin analysis of MOS SRAM cells,” IEEE J. Solid-State Circuits 22 (1987) 748 (DOI: 10.1109/JSSC.1987.1052809).

[20] C. M. R. Prabhhu and A. K. Singh: “Low-power reliable SRAM cell for write/read operation,” IEICE Electron. Express 11 (2014) 20140913 (DOI: 10.1587/exle.11.20140913).

[21] I. Batimore, et al.: “Improved generation of identifiers, secret keys, and random numbers from SRAMs,” IEEE Trans. Inf. Forensics Security 10 (2015) 2653 (DOI: 10.1109/TIFS.2015.2471279).

[22] M.-D. Yu and S. Devadas: “Secure and robust error correction for physical uncloneable functions,” IEEE Des. Test Comput. 27 (2010) 48 (DOI: 10.1109/MDT.2010.25).

[23] M. Cortez, et al.: “Modeling SRAM start-up behavior for physical uncloneable functions,” DFT (2012) 1 (DOI: 10.1109/DFT.2012.6378190).

[24] E. I. Vatajelu, et al.: “Towards a highly reliable SRAM-based PUFs,” DATE (2016) 273.

[25] M. Barbareshi, et al.: “Testing 90 nm microcontroller SRAM PUF quality,” DTIS (2015) 1 (DOI: 10.1109/DTIS.2015.7127360).

[26] D. E. Holcomb, et al.: “Power-up SRAM state as an identifying fingerprint and source of true random numbers,” IEEE Trans. Comput. 58 (2009) 119 (DOI: 10.1109/TC.2008.212).

[27] W. Wang, et al.: “Exploiting power supply ramp rate for calibrating cell strength in SRAM PUFs,” LATS (2018) 1 (DOI: 10.1109/LATSW.2018.834685).

[28] M. Cortez, et al.: “Intelligent voltage ramp-up time adaptation for temperature noise reduction on memory-based PUF systems,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst. 34 (2015) 1162 (DOI: 10.1109/TCAD.2015.2422844).

[29] B. H. Calhoun and A. P. Chandrakasan: “Static noise margin variation for sub-threshold SRAM in 65-nm CMOS,” IEEE J. Solid-State Circuits 41 (2006) 1673 (DOI: 10.1109/JSSC.2006.873215).

[30] A. Neale and M. Sachtjev: “A low energy SRAM-based physically uncloneable function primitive in 28 nm CMOS,” CICC (2015) 1 (DOI: 10.1109/CICC.2015.7338478).