Long-term Continuous Assessment of SRAM PUF and Source of Random Numbers

Rui Wang, Georgios Selimis, Roel Maes, Sven Goossens
Intrinsic-ID, Eindhoven, The Netherlands
Email: {rui.wang, georgios.selimis, roel.maes, sven.goossens}@intrinsic-id.com

***Abstract*—The qualities of Physical Unclonable Functions (PUFs) suffer from several noticeable degradations due to silicon aging. In this paper, we investigate the long-term effects of silicon aging on PUFs derived from the start-up behavior of Static Random Access Memories (SRAM). Previous research on SRAM aging is based on transistor-level simulation or accelerated aging test at high temperature and voltage to observe aging effects within a short period of time. In contrast, we have run a long-term continuous power-up test on 16 Arduino Leonardo boards under nominal conditions for two years. In total, we collected around 175 million measurements for reliability, uniqueness and randomness evaluations. Analysis shows that the number of bits that flip with respect to the reference increased by 19.3% while min-entropy of SRAM PUF noise improves by 19.3% on average after two years of aging. The impact of aging on reliability is smaller under nominal conditions than was previously assessed by the accelerated aging test. The test we conduct in this work more closely resembles the conditions of a device in the field, and therefore we more accurately evaluate how silicon aging affects SRAM PUFs.**

***Keywords*—SRAM PUF, long-term, aging, evaluation, reliability, uniqueness, randomness, entropy**

I. Introduction

The number of Internet-connected devices worldwide is expected to run in the tens of billions by 2030 [1]. One of the key components in the security of an Internet-connected device is a device-unique cryptographic identity that can be verified by the cloud infrastructure. Existing methods for securely storing such an identity in a large number of devices often rely on keys stored in one-time programmable memory. This method does not scale to billions of devices in the Internet of Things (IoT). An alternative solution for secure initiation of a cryptographic identity is based on Physical Unclonable Functions (PUFs), which utilizes deep submicron manufacturing process variation during the fabrication of the device. PUFs technology based on Static Random Access Memory (SRAM) has been commercially deployed in products by Microsemi [2] and NXP [3]. SRAM PUF is applicable to either generate reliable secure keys (reliability and uniqueness requirement) or provide random entropy to the device (randomness requirement) [4].

In commercial products, the lifetime of the device is a significant concern. Deep into the physical level of a silicon IC, some circuit's parameters slowly and gradually change over time, leading to the change of properties on the IC. This change is defined as *silicon aging*. It has been presented that silicon aging degrades the reliability of SRAM PUF [5] while it improves noise entropy over time [6].

One of the methods to analyze silicon aging on SRAM PUF is circuit simulation at transistor level. Another option is to measure a silicon device at high temperature and operating voltage which accelerates the aging effect. In this paper, for the first time we propose to run the silicon device in nominal condition for a sufficient amount of time to observe real-time, non-simulated and non-accelerated aging effects.

A. Related Work

The concept of SRAM PUF was firstly proposed by Guajardo et al. [7]. Kumar et al. studied the degradation of SRAM cells for 70nm and 100nm CMOS technology by performing transistor level simulation [8]. Aging of other technologies including Partially Depleted Silicon On Insulator (PDSOI) [9] and FinFET [10] are also investigated based on simulation. On the other hand, Maes et al. used accelerated aging on the silicon to demonstrate SRAM PUF reliability degrades for 65nm CMOS technology [5], [11].

B. Our Contribution

This paper presents the first experimental aging test of SRAM PUF under nominal condition continuously running for two years. The nominal aging test reflects the practical aging effect on a device in the field more accurately, since we do not expect constant stress conditions during the device's lifetime. Long-term continuous aging assessment of the SRAM PUF with respect to reliability, uniqueness and randomness has been conducted. For the assessment we used SRAMs of low cost generic use Commercial Off-The-Shelf (COTS) devices.

The evaluation indicates that even after years of continuous use, SRAM PUF remains of sufficient quality for reliable and secure key generation scheme and random number generation. The reliability property is worsened to some extent. The impact, however, is less pessimistic than the equivalent aging effect derived from accelerated aging.

C. Paper Outline

Section II provides the background of SRAM PUF technology, in particular the silicon aging effect on SRAM PUF cells. Section III describes the measurement setup of our long-term aging experiment. Section IV presents the evaluation result and discussion on the aging data from the measurement, and the paper is finally concluded in Section V.

978-3-9819263-4-7/DATE20/©2020 EDAA

II. Background

A. SRAM PUF technology and applications

The basic 6T-SRAM cell structure consisting of two cross-coupled inverters and access transistors (not shown) is shown in Fig. 1. The initial state Q after a new power-up is determined by uncontrollable variations during manufacturing. The preferred power-up state is persistent and stable after manufacturing. On the other hand, a small quantity of SRAM cells are unstable and show a random preference at every power-up. Taking both stable and unstable SRAM cells into consideration, previous research has shown that the power-up pattern of SRAM memory is perfectly reproducible (with the proper application of error-correction codes), unique [11] and also capable of providing randomness [12]. Therefore, SRAM PUF can be applied in the following scenarios.

1) Secure Key generation: The most common application of PUFs is secure key generation and storage. The cryptographic key is derived based on SRAM PUF and stored via helper data scheme. In this application, reliability and security are important properties for SRAM PUFs.

Reliability means the response of SRAM PUFs is reproduciable with limited amount of bit error rate in predefined environmental and system conditions. Error correction codes can be designed to correct up to 25% of bit error rate without reproduction failure [13].

On the other hand, security means two properties. First, SRAM PUF should have sufficient entropy to prevent significant information leakage on the generated key. It implies that bias present on SRAM PUFs should be within the boundary. Current debiasing schemes can deal with 25% / 75% bias [14]. Second, the response of an SRAM PUF is unpredictable even given all the responses of other SRAM PUFs. It implies that SRAM PUF should have good uniqueness.

2) True Random Number Generation: True Random Number Generator (TRNG) provides an unpredicted seed to cryptographic systems. Electrical noise influences the initial state of unstable SRAM cells. By utilizing these noises in the circuits, SRAM PUFs can also serve as TRNG. In this application, a sufficient amount of bits should flip over multiple power-ups in order that SRAM PUFs can provide sufficient randomness at next power-up test.

B. Aging Effect on SRAM Cells

During nominal operations, a digital CMOS circuit in a silicon chip degrades over time. The dominant aging effect is Negative Bias Temperature Instability (NBTI) resulting in a temporal increase in the threshold voltage, particularly for a switched-on PMOS transistor [5]. For simplicity, all the following parameters related to PMOS are treated as positive values. In Fig. 1, when an SRAM cell stores state zero ($Q = 0$), P1 is switched off and P2 is switched on. As a result of NBTI, $V_{\mathrm{th,P2}}$ will increase while $V_{\mathrm{th,P1}}$ is not affected. Also, the fact that P2 is switched on indicates that initially $V_{\mathrm{th,P2}} < V_{\mathrm{th,P1}}$. Therefore, the temporal tendency of this SRAM cell is that $|V_{\mathrm{th,P2}} - V_{\mathrm{th,P1}}|$ grows smaller. This

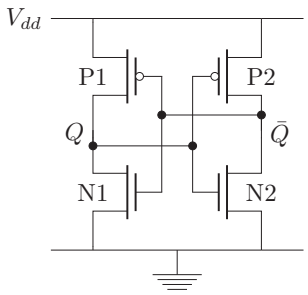


Fig. 1: Two cross-coupled inverters at the core of each SRAM cell (Other two access transistors not shown).

tendency also holds when $(Q = 1)$. Smaller $|V_{\mathrm{th,P2}} - V_{\mathrm{th,P1}}|$ means the SRAM cell is more balanced and more likely to have PUF response bits flip. From the reliability perspective, this effect deteriorates SRAM PUF as key generation scheme since more SRAM cells tend to lose stability and randomly flip, i.e. the reliability of SRAM PUF worsens over time. From the randomness perspective, more SRAM cells become balanced and unpredictable over measurements, i.e. more randomness can be harvested based on SRAM PUFs.

Additionally, with the introduction of high-permittivity gate dielectrics, Positive Bias Temperature Instability (PBTI) for a switched-on NMOS transistor is also becoming more significant [9]. Due to this effect, then NMOS transistor operating with a positive gate-to-source voltage experiences time-dependent threshold voltage increase.

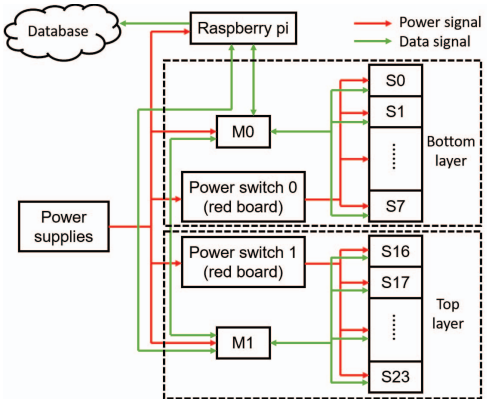
Other silicon aging mechanisms including hot electron injection, gate dielectric breakdown and electromigration are discussed in [15].

III. Measurement Setup

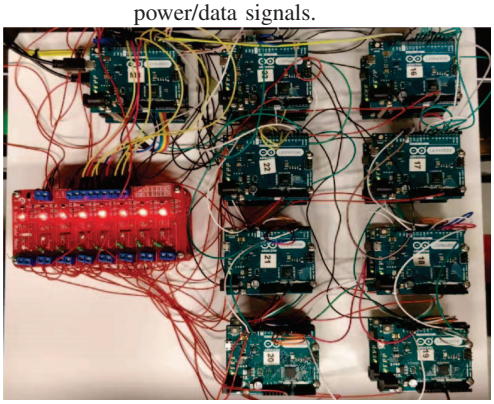
The measurement platform was set up for the continuous SRAM PUF observation read-out at room temperature. SRAM chips were getting successive power cycles from Feb. 8, 2017 to Feb. 8, 2019. Each SRAM chip has been powered up and read out approximately 11 million times within this period, i.e. around 10 measurements per minute. For the more exhaustive evaluation, 16 devices were tested in the measurement setup, leading to around 175 million measurements in total.

The type of the SRAM chips used in the setup is the SRAM on an ATmega32u4 microcontroller on an Arduino Leonardo board. The operating voltage of ATmega32u4 is 5V, and the size of the SRAM is 2.5 KByte.

As shown in Fig. 2, the whole measurement setup consists of the following components: 1) An external power supply that provides power to the setup system; 2) 2 Arduino boards as master boards. The two master boards are denoted as M0 and M1 respectively in Fig. 2a. Each master board controls its slave boards via I2C protocol and communicates with other components in the system; 3) 16 Arduino as slave boards. The slave board reads out its SRAM power-up data and sends them back to its master board; 4) A power switch board that provides power to all the slave boards according to the command of each master board. Separate connections between



(a) Schematic of SRAM PUF on Arduino boards measurement setup and flow of power/data signals.



(b) Practical measurement setup including 18 Arduino boards stacked up in two layers and power switch circuits.

Fig. 2: Measurement setup for the long-term test.

the power switch and each slave board avoid interference between boards in the same stack; 5) Raspberry Pi receives SRAM data from master boards, and sends them to a database and stores them in a JSON format.

In Fig. 2a, all the 18 Arduino boards were stacked up in two layers. The top layer consisting of M1 and from S16 to S23 is visible in Fig. 2b. Two layers communicate with each other via connection between M0 and M1 so that data from different layers are synchronized, i.e. each slave board always produces the same quantity of SRAM PUF data within a fixed period of time. The layer at bottom is denoted as layer 0, and the layer at the top is denoted as layer 1. The detailed test flow of layer 0 as an example is described in Algorithm 1.

We used Tektronix TDS 3034B oscilloscope to observe the power cycle curve of four slave boards, namely S3, S4 from layer 0, and S19, S20 from layer 1. S3 and S19, S4 and S20 are in the same stack, respectively. As shown in Fig. 3, the period of one power cycle is 5.4s. The power-on time of each board is 3.8s and the power-off time is 1.6s. Boards on the same layer (e.g. S19 and S20) are powered on and off at the same time. The power curves between two layers are unsynchronized to avoid interference, and to increase the

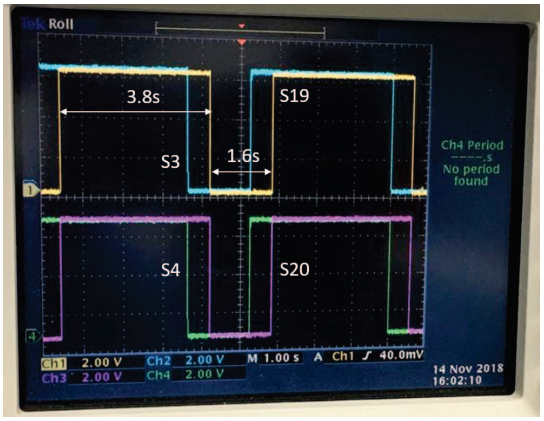


Fig. 3: Waveforms of power curves of board S3, S4, S19, S20 observed from the oscilloscope.

Algorithm 1 Test flow on layer 0

1) M0 waits the end signal from M1, meaning layer 0 starts its test flow after layer 1 finalizes its last test cycle.
2) M0 enables the power of its slave boards S0 to S7, via power switch
3) When all the slaves on layer 0 are switched on, M0 gives the signal to M1, enabling layer 1 to starts its new test flow
4) Each slave board reads the first 1 KByte of its SRAM power-up pattern, and sends the data back to M0 via I2C protocol
5) M0 receives data from slave boards and sends the data to Raspberry pi
6) M0 disables the power of slave boards S0 to S7
7) M0 waits the start signal from M1, meaning layer 0 finalizes its cycle when autonomous read-out starts in layer 1.
8) M0 gives the signal to M1, indicating that layer 0 finalizes its test cycle.

throughput of measurements.

IV. Evaluation

A. Initial SRAM PUF quality evaluation

To visualize the distribution of the initial SRAM PUF, the first SRAM power-up pattern of board S0 is plotted in Fig. 4. For evaluating the initial SRAM PUF quality, we select the first 1,000 read-out data of each board measured on Feb. 8, 2017 (starting date of the test). Three important metrics are adopted for the evaluation, as described in the following paragraphs.

1) Within-Class Hamming Distance: As described in Section II-A, the difference between a reference pattern and another measured pattern of the same SRAM chip is supposed to be limited. To evaluate the reliability of SRAM PUF, the first read-out pattern is used as the reference. The other measurements of the same chip are compared to this

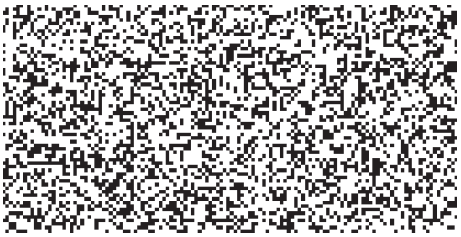


Fig. 4: Visualized startup pattern of 1KB memory on Arduino board with ID = 0.

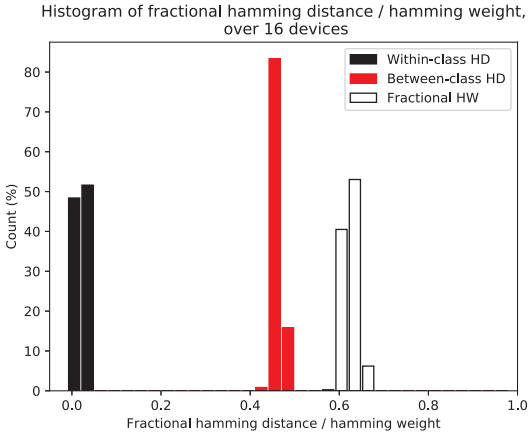


Fig. 5: Fractional Hamming distance / Hamming weight distributions at the beginning of the test (all the 16 Arduino boards included).

reference using fractional Hamming Distance (FHD)[1]. The FHD assessment within the same SRAM chip is defined as Within-Class Hamming Distance (WCHD). It is observed in Fig. 5 that WCHD remains below 3%. This value is well within the boundary, as specified in Section II-A for error correction. So WCHD results show good reliability.

2) Between-Class Hamming Distance: The SRAM PUF response of a chip should be unpredictable, even given the responses of other chips. The FHD between reference of every two different chips is defined as Between-Class Hamming Distance (BCHD). The BCHD is supposed to be significantly larger than WCHD and ideally close to 50% so that the PUF of a certain chip is distinguishable from others. As shown in Fig. 5, the BCHD is distributed between 40% and 50%. The BCHD significantly deviates from the WCHD, showing good uniqueness among devices.

3) Fractional Hamming Weight: Hamming Weight (HW) is the number of non-zero bits in the PUF response. In case of Fractional Hamming Weight (FHW), the HW is divided by the length of the string. As shown in Fig. 5, the FHW of different SRAM chips lies between 60% and 70%. This indicates that the SRAM PUF is not perfectly unbiased, but still capable of generating a key of sufficient security strength [14].

[1]Hamming Distance (HD) is defined as the number of bits that different between two bit strings. In case of fractional Hamming Distance (FHD), the HD is divided by the length of the string.

B. Reliability and Uniqueness Evaluation

We select the first 1,000 consecutive measurements after midnight on the 8th of each month for each SRAM chip. These SRAM PUF data are used for evaluating the effect of aging on reliability and uniqueness. The method for the evaluation is presented below.

1) WCHD: We select the first read-out pattern of each board on the starting date as the reference. Measurements derived in the following months are compared to this reference.

2) BCHD: For each month, the first SRAM read-out data of the 1,000 consecutive measurements mentioned above is used to calculate BCHD.

3) FHW: For each month, we use the 1,000 consecutive measurements to calculate FHW.

4) PUF entropy: In addition to the metrics mentioned above, PUF entropy is introduced to assess the uniqueness of SRAM PUFs using min-entropy [16]. If a binary source has probability p_0 and p_1 to produce '0' and '1' respectively, then the definition for min-entropy of this binary source is:

$$H_{min,PUF} = -\log_2 (\max (p_0, p_1)).$$

Assuming all bits from the SRAM PUF are independent [17], each bit location can be regarded as an individual binary source. Thus the average min-entropy of SRAM PUFs over n bits is:

$$(H_{min,PUF})_{average} = \frac{1}{n} \sum_{i=1}^{n} -\log_2 (\max (p_{i\_0}, p_{i\_1})) .$$

For the calculation, the SRAM PUF data for BCHD computation is used to derive PUF entropy, i.e. p_0 and p_1 are computed as probabilities over all measured SRAMs.

C. Randomness Evaluation

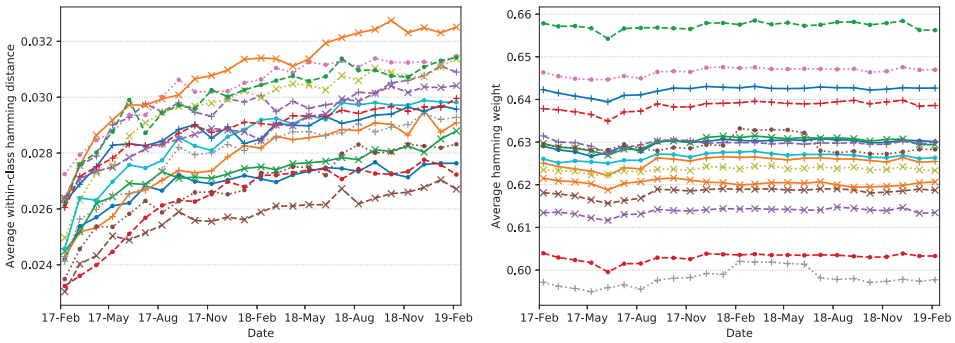
Apart from what are important if SRAM PUFs are applied for key generation, randomness is evaluated to assess the feasibility of using SRAM PUFs as a random source [12]. Two randomness-related properties are presented below.

1) Stable cells: Both process variation and electrical noise impact the skewness of SRAM cells [4]. An SRAM cell which is always powered up to state 0 or 1 over a large number of power-ups is considered as a *stable cell*. More quantitatively, one-probability is introduced to assess the stability of SRAM cells. One-probability (p_i) of a cell i at a certain SRAM is the probability that the response value of this cell (R_i) is '1' over multiple power-ups [18], defined as:

$$p_i := \mathbf{Pr}(R_i = 1)$$

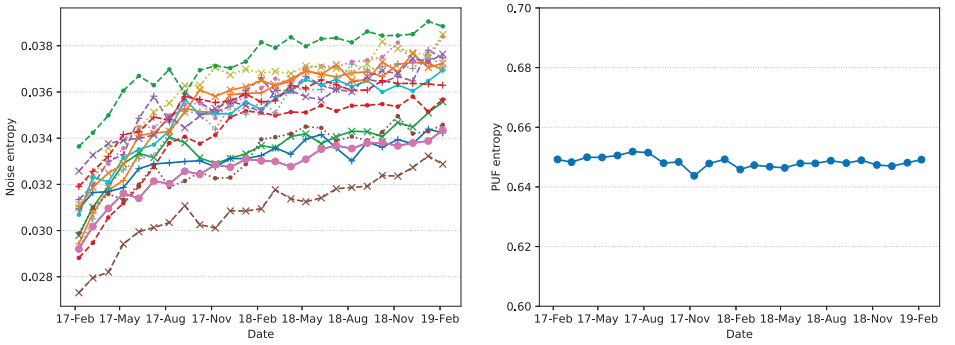
In practice, the cell with one-probability of zero or one over 1,000 consecutive measurements in a certain month is counted as a stable cell in that particular month.

2) Noise entropy: Noise entropy measures the unpredictability of next SRAM power-up response given the information of prior responses. A balanced cell is sensitive to noise and thus contributes to noise entropy of SRAM PUF based TRNG. Similar to PUF entropy, min-entropy is applied



(a) Development of WCHD with respect to the first SRAM observation at the start of the test

(b) Development of Hamming weight



(c) Development of noise entropy

(d) Development of PUF entropy

Fig. 6: Development of reliability and uniqueness qualities of SRAM PUFs and randomness of SRAM PUF based TRNG on all the 16 Arduino boards during the long-term aging test. The aging period started from Feb. 2017 and ended in Feb. 2019. The test condition is at room temperature. Different lines in (a), (b) and (c) mean qualities of different SRAMs.

to estimate entropy of noise on SRAM PUF over multiple power-ups [12]. Using 1,000 consecutive measurement data, the average min-entropy of noise on SRAM PUF over n bits based on the one-probability of each bit is

$$(H_{min,noise})_{average} = \frac{1}{n}\sum_{i=1}^{n} -\log_2\left(\max\left(p_i, 1-p_i\right)\right).$$

Note that $H_{min,noise}$ is noise entropy calculated based on multiple measurements of single SRAM, evaluating the randomness of TRNG based on SRAM PUFs. $H_{min,PUF}$ is PUF entropy calculated based single measurement of multiple SRAMs, evaluating the uniqueness of SRAM PUFs.

D. Result discussion

The experimental aging results after 2-year of continuous test is summarized in Table I. Both the average value (AVG.) and worst-case value (WC.) among 16 devices are presented in the table. The development of core properties over time is plotted in Fig. 6. The evaluation result of aging effect on SRAM PUF is discussed in two aspects.

1) SRAM PUF as key generation scheme: Within the time frame of 2-year aging, the FHD with respect to the initial reference at the start of the test is averagely increased from 2.49% to 2.97%, or in other words, the average number of bit errors with respect to the initial measurement increases by about 0.74% each month over a 2-year period, indicated in Fig. 6a. The increase of WCHD is in line with NBTI aging effect on SRAM. Therefore, the reliability of SRAM PUF worsens within a limited boundary due to aging effect. In contrast to accelerated aging showing WCHD increases from 5.3% to 7.2%, which is about 1.28% monthly change over the first 2 years [5], the reliability suffers less reduction. This means the previous research based on accelerated aging overestimated the degradation of SRAM PUF reliability.

Over the aging period, the HW of each SRAM remains almost constant, leading to a negligible change in BCHD and PUF entropy. Thus, the uniqueness of SRAM PUF is not impacted by aging effects. The results are indicated in Fig. 6b and Fig. 6d.

2) SRAM PUF as true random number generation: The ratio of stable cells decreases from 85.9% to 83.7% on average among devices, with a 0.11% decrease monthly. This result is also consistent with the hypothesis of NBTI aging effect in Section II-B.

As a consequence of fewer stable SRAM cells, the noise entropy is increased from 3.05% to 3.64%, with a 0.74%

TABLE I: EVALUATION RESULT OF SRAM PUF QUALITIES AT THE START AND THE END OF THE TEST

Evaluation		Start	End	Relative Change	Monthly Change
WCHD	AVG.	2.49%	2.97%	+19.3%	+0.74%
	WC.	2.72%	3.25%	+19.5%	+0.74%
HW	AVG.	62.70%	62.70%	negligible[a]	negligible
	WC.	65.78%	65.62%	-0.24%	-0.01%
Ratio of Stable Cells	AVG.	85.9%	83.7%	-2.49%	-0.11%
	WC.	87.2%	85.4%	-2.22%	-0.87%
Noise entropy	AVG.	3.05%	3.64%	+19.3%	+0.74%
	WC.	2.73%	3.29%	+20.5%	+0.78%
BCHD	AVG.	46.79%	46.80%	negligible	negligible
	WC.	44.31%	44.67%	+0.81%	0.03%
PUF entropy		64.92%	64.91%	negligible	negligible

[a]Negligible means change is less than 0.01%.

increase rate per month. Therefore, the randomness of SRAM PUF based TRNG is improved after aging. The result is indicated in Fig. 6c.

Another notable result is that the monthly change rate in WCHD and noise entropy is larger at the start of the test than after 1 year. This can be explained as follows: We define stable cells as fully-skewed cells, and unstable cells with preference on power-up pattern as partially-skewed cells. For instance, in Fig. 1, assume that initially the SRAM cell is fully skewed at state zero, i.e. $V_{\mathrm{th,P2}} < V_{\mathrm{th,P1}}$ (all the values are treated as positive). At the start, the power-up state is always zero, leading to smaller $|V_{\mathrm{th,P2}} - V_{\mathrm{th,P1}}|$, which gradually converts this cell to a partially-skewed cell. This indicates that after a certain period of aging, the stable cell becomes unstable, and sometimes the new power-up state $Q = 1$, leading to larger $|V_{\mathrm{th,P2}} - V_{\mathrm{th,P1}}|$. As a result, the tendency of $|V_{\mathrm{th,P2}} - V_{\mathrm{th,P1}}|$ is not monotonic over the aging.

V. CONCLUSION

This paper has presented the result of silicon aging on SRAM as PUF and as source of TRNG based on long-term test in nominal conditions. Based on the experimental result derived from 2-year measurement, the evaluation confirms the anticipated NBTI effect on SRAM cells. The uniqueness keeps almost constant during the aging period. The reliability of SRAM PUF gradually degrades, the extent of which, is less pessimistic than the emulated result from accelerated aging test. WCHD increases by 0.74% each month in nominal conditions, while WCHD increases by 1.28% each month in accelerated aging. Meanwhile, the aging effect slightly improves the randomness of SRAM PUF based TRNG. Noise entropy improved by 0.74% each month.

ACKNOWLEDGMENT

The author would like to thank Peter Simons and Tobias Adryan for their help in establishing and maintaining the measurement setup. This work has been supported by H2020 Project "INSTET[2]: Securing the Internet of Things with a unique microchip fingerprinting technology" with grant agreement No 811509.

REFERENCES

[1] IEEE Spectrum - Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated, https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated; 2019.

[2] Microsemi - Product Overview PolarFire FPGA, https://www.microsemi.com/document-portal/doc_download/136518-po0137-polarfire-fpga-product-overview-datasheet; 2019.

[3] NXP - LPC55S6x 32-bit ARM Cortex-M33+ MCU Data Sheet, https://www.nxp.com/docs/en/data-sheet/LPC55S6x.pdf; 2019.

[4] D. E. Holcomb, W. P. Burleson and K. Fu, "Power-Up SRAM state as an identifying fingerprint and source of true random numbers," in IEEE Transactions on Computers, vol. 58, no. 9, pp. 1198-1210, Sept. 2009.

[5] R. Maes and V. van der Leest, "Countering the effects of silicon aging on SRAM PUFs," 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Arlington, VA, 2014, pp. 148-153.

[6] S. Kiamehr, M. S. Golanbari and M. B. Tahoori, "Leveraging aging effect to improve SRAM-based true random number generators," Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017, Lausanne, 2017, pp. 882-885.

[7] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in Cryptographic Hardware and Embedded Systems (CHES), ser. LNCS, vol. 4727. Springer, 2007, pp. 63–80.

[8] S. V. Kumar, K. H. Kim and S. S. Sapatnekar, "Impact of NBTI on SRAM read stability and design for reliability," 7th International Symposium on Quality Electronic Design (ISQED'06), San Jose, CA, 2006, pp. 6 pp.-218.

[9] A. Bansal, R. Rao, J.-J. Kim, S. Zafar, J. H. Stathis, and C.-T. Chuang, "Impacts of NBTI and PBTI on SRAM static/dynamic noise margins and cell failure probability," Microelectron. Rel., vol. 49, pp. 642–649, 2009.

[10] S. Khan, I. Agbo, S. Hamdioui, H. Kukner, B. Kaczer, P. Raghavan, and F. Catthoor, "Bias temperature instability analysis of FinFET based SRAM cells," 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, 2014, pp. 1-6.

[11] R. Maes, V. Rozic, I. Verbauwhede, P. Koeberl, E. van der Sluis and V. van der Leest, "Experimental evaluation of Physically Unclonable Functions in 65 nm CMOS," 2012 Proceedings of the ESSCIRC (ESSCIRC), Bordeaux, 2012, pp. 486-489.

[12] V. van der Leest, E. van der Sluis, G.-J. Schrijen, P. Tuyls, and H. Handschuh, "Efficient implementation of true random number generator based on sram pufs," in Cryptography and Security: From Theory to Applications, ser. Lecture Notes in Computer Science, D. Naccache, Ed. Springer Berlin Heidelberg, 2012, vol. 6805, pp. 300–318.

[13] B. Chen, T. Ignatenko, F. M. J. Willems, R. Maes, E. van der Sluis and G. Selimis, "A Robust SRAM-PUF key generation scheme based on polar codes," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6.

[14] R. Maes, V. van der Leest, E. van der Sluis, F. Willems, "Secure key generation from biased PUFs." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2015.

[15] C. Böhm, M. Hofer, Physical unclonable functions in theory and practice. Springer Science & Business Media; 2012 Oct 16.

[16] P. Simons, E. van der Sluis and V. van der Leest, "Buskeeper PUFs, a promising alternative to D Flip-Flop PUFs," 2012 IEEE International Symposium on Hardware-Oriented Security and Trust, San Francisco, CA, 2012, pp. 7-12.

[17] M. Cortez, S. Hamdioui, A. Kaichouhi, V. van der Leest, R. Maes and G. Schrijen, "Intelligent voltage ramp-up time adaptation for temperature noise reduction on memory-Based PUF systems," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 7, pp. 1162-1175, July 2015.

[18] R. Maes, "An accurate probabilistic reliability model for silicon PUFs." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2013.

[2]https://cordis.europa.eu/project/rcn/216842/factsheet/en