A reliable physical unclonable function based on differential charging capacitors

Yuan, Hang; Guo, Wei; Chang, Chip-Hong; Cao, Yuan; Wei, Shaojun; Yin, Shouyi; Deng, Chenchen; Liu, Leibo; Ge, Wei; Zhang, Fan

2019

Yuan, H., Guo, W., Chang, C.-H., Cao, Y., Wei, S., Yin, S., ... Zhang, F. (2019). A reliable physical unclonable function based on differential charging capacitors. Proceedings of the 2019 IEEE International Symposium on Circuits and Systems (ISCAS).
doi:10.1109/ISCAS.2019.8702728

<https://hdl.handle.net/10356/145852>

<https://doi.org/10.1109/ISCAS.2019.8702728>

© 2019 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The published version is available at:
<https://doi.org/10.1109/ISCAS.2019.8702728>

Downloaded on 26 Apr 2023 19:47:35 SGT

A Reliable Physical Unclonable Function Based On Differential Charging Capacitors

Hang Yuan¹, Wei Guo¹, Chip-Hong Chang², Yuan Cao³, Shaojun Wei¹, Shouyi Yin¹, Chenchen Deng¹, Leibo Liu¹, Wei Ge⁴, and Fan Zhang⁴

¹Wuxi Research Institute of applied technologies, Tsinghua University

²School of Electrical and Electronic Engineering, Nanyang Technological University

³College of Internet of Things Engineering, Hohai University,

⁴Department of Electrical Engineering, Southeast University

⁵College of Information Science and Electronic Engineering, Zhejiang University

Abstract—Physical Unclonable Function (PUF) is an emerging security primitive for cryptography applications. However, achieving a very high reliability against the environmental variations remains a main challenge in PUF design and a key barrier for its commercialization. This paper presents a new PUF design based on the charging of a symmetric MOS capacitor pair by constant current with cross-coupled positive feedback inverters. The proposed weak PUF features high raw response reliability against variations in power supply and temperature without power-up reset noise and other issues due to the power-down and up of an array of cells. Extensive Monte-Carlo simulations have been performed using a standard 110nm CMOS process technology. The simulated results show an almost ideal uniqueness of 50.03% and superior reliability of 97.70% over a temperature range from 0°C to 80°C, and 96.20% with the supply voltage varies from 1.2 V to 1.8 V. The response bit can be generated at a rate of 27.78 Mbps with an average power consumption of 20.86 μ W at 1.5V, and the energy consumption is only 750 fJ/bit.

I. INTRODUCTION

Unsecured Internet of Things (IoT) devices are consistently being exploited to launch Internet attacks [1-5]. Physical Unclonable Functions (PUFs) have been widely investigated and contemplated for commercial use as a hardware security primitive in IoT devices to complement the vulnerability of hardware roots of trust that rely heavily on the secure local storage of shared cryptographic keys. PUF has shown advantage as a more reliable means to uniquely identify devices or chips than conventional supply chain tagging methods. In contrast to classical cryptography, whereby the secret key is stored in the local non-volatile memory (NVM), a PUF regenerates the random secret key through a challenge-response mapping mechanism based on random physical property deviation imprinted by the uncontrollable chip manufacturing process variation [1]. The response of the PUF to an arbitrary challenge is unknown and unpredictable at design time until the PUF circuit is fabricated, measured in a control environment during the enrollment phase, and recorded in the secure server database for verification.

A PUF circuit is typically constructed by an abutment or cascade of symmetrically structured basic cells. It is classified as a weak PUF if the number of challenges is small or grows only polynomially with the number of basic cells, as opposed

to the strong PUF which has an exponential number of challenges. Weak PUF is also known as physically obfuscated key (POK). Owing to the limited number of challenge-response pairs (CRPs), it is more suited to cryptographic key generation, hybrid random number generator and device identification. For cryptographic key generation, owing to the avalanche effect of bit error on encryption and decryption, more reliable challenge-response mapping that is robust to changes in operating conditions and repeated measurements is demanded to reduce the cost of error correction [6]. For device identification, the PUF responses produced by the same or different manufacturing lots should be unique and maximally discriminable. For hybrid random number generator, the response of the PUF should be random and unpredictable. The expectation on the reliability and uniqueness on the native responses of a weak PUF is generally higher than a strong PUF in view of their different applications.

One of the earliest weak PUFs was implemented by Lofstorm *et al.* [7]. A repeatable binary identification is produced from random threshold mismatch in an array of addressable MOSFETs, and an auto-zeroing comparator. The reported reliability is 95%, but the speed (30 kbps) and power consumption (250 μ W) are obviously inferior for today applications. Later in 2007, Y. Su, J. Holleman and B. Otis [8] presented a chip-ID circuit based on cross-coupled devices. Before the ID evaluation, the cross-coupled devices are brought to a meta-stable state. Then their outputs are allowed to transit spontaneously to a steady state determined by the device mismatch. This design achieved a competitive reliability of 96.96% but has a poor uniqueness of only 64.70%. Recently, J. Li and M. Seok [9] implemented a weak PUF based on a pair of ultra-compact analog circuits with the output proportional to absolute temperature (PTAT). The design was found to be vulnerable to temperature variations from 0°C to 80°C with a measured bit error rate (BER) of 3.5% in the worst case. The most popular intrinsic weak PUF implementation exploits random power-up reset behavior of static random-access memory (SRAM) cells. However, as stated in [10], SRAM PUF suffers from relatively low average intrinsic reliability of 85%. As the response bit generation is highly susceptible to change in threshold voltage V_{th} , post manufacturing noise and systematic variations not due to fabrication process and lithography tolerance are more likely to skew the response bit distribution or cause undesirable

Fig. 1: Block diagram of proposed PUF.

Fig. 2: Schematic of a PUF cell.

response bit flip with repeated measurements. Moreover, the data originally stored in the SRAM cells will be lost in PUF operation as the entire memory array has to be reset to generate the response bits.

In this paper, a weak PUF with high reliability is built around the cross-coupled inverters of an SRAM cell with additional components, most noticeably a pair of MOS capacitors for differential charging. The stronger entropy source provided by the oxide capacitance deviation of MOS transistor due to process variation [11] is harnessed for random response bit generation with higher immunity to spatial and temporal noises caused by environmental factors. The rest of the paper is organized as follows. Section II describes the proposed PUF structure, its basic cell circuit and operations. Section III presents the simulation results on uniqueness, reliability, randomness, throughput and power consumption of the proposed PUF and compared them against reported results of other weak PUFs. Section IV concludes the paper.

II. PROPOSED PHYSICAL UNCLONABLE FUNCTION BASED ON SRAM WITH CHARGING CAPACITORS

A. PUF Structure

The proposed PUF consists of four main parts, namely biasing circuit, row and column address decoders, array of PUF cells and multiplexer, as shown in Fig. 1. There are altogether 2^n PUF cells arranged into a square matrix of equal number of rows and columns. All the cells share the same biasing circuit. A challenge of bit length n is input into the circuit to select a PUF cell as well as control the multiplexer to produce a response bit. To conserve power, during response generation, only the selected PUF cell is powered up.

B. PUF Cell

Fig. 2 depicts the circuit schematic of the proposed PUF cell. The symmetric transistors between the branches, M_1 and M_2 , and the cross-coupled inverters are identically sized to avoid systematic skew. Two MOS capacitors, C_1 and C_2 , are each connected to an output of the cross-coupled inverter pair. The main idea of the proposed PUF cell is to charge the MOS capacitor pair with the same charging currents such that the complementary output voltages, V_1 and V_2 , of the cross-coupled inverter race to reach the trip points of their respective inverters. C_1 and C_2 are realized by MOS capacitors to take advantage of large capacitance per unit area. Before the charging process starts, both capacitor voltages are reset to ground by the pull-down switches (the two nMOS switches with gate input controlled by the signal PD). Once the charging process starts, the pull-down switches are turned off, and the capacitors start to be charged by the matched current sources M_1 and M_2 . Both M_1 and M_2 are biased by the same voltage V_b . A common biasing circuit is used to provide V_b to all cells but only the addressed cell is active.

The major entropy source of the PUF cell is the MOS capacitor pair (C_1 and C_2). The size of the MOS capacitors are kept small so as to amplify their capacitance mismatch induced by manufacturing process variation. Due to process variation, the oxide thickness of the two MOS capacitors are not the same and the oxide capacitance and threshold voltage deviation of the same MOS capacitor also differ from one cell to another. This process induced mismatches result in different rise time of the voltage on each capacitor of the pair for the same charging current. Once either capacitor has been charged to the inverter's trip point, the inverter output switches and discharges the output of the other capacitor down to ground, which in turns switches the other inverter's output high to charge the capacitor up fully. However, there will be a time delay in switching the output voltages by the cross coupled inverters. Once the voltage difference is sufficient to trigger the positive feedback, the output state will be locked. At this moment, the pMOS switch of the slower charging branch will be turned off so that the charging current is shut off. This ensures that logic state, once stabilized, cannot be easily switched by noise. The data is ready to be read out, and is not likely to be flipped at this time.

The operation of this PUF is divided into three stages. The first stage is initialization. During this stage, all the charges on the capacitors are removed by turning on the pull-down switch. Both the cell supply and the current mirror biasing of the PUF cells are not applied to save energy. The second stage is pre-evaluation. In this stage, the cell supply and bias are applied while the pull-down switch is still on. The advantage of introducing this intermediary step is to eliminate any glitches before charging up the capacitor pair. The last stage is the evaluation stage, where pull-down switches are turned off to direct the source currents to charge the capacitors. Upon completion of the charging process, the output data is stable.

The randomness and uniqueness of the PUF response is derived from the independent capacitance mismatch between the two identically designed MOS capacitors of each cell. The reliability of the response is due to low susceptibility of the MOS capacitance to voltage and temperature variations. It

turns out that the reliability of this PUF design also benefits from a large variation of the two capacitor values within the same cell. With a larger difference in their capacitances, the circuit will be even more immune to operating condition changes like temperature and supply voltage shift. For a good design, the layout of the structure is kept as symmetrical as possible so that any deviation of electrical properties are predominantly contributed by the manufacturing process variations and tolerance of lithography. All devices must be matched by design so that the nominal voltages of V_1 and V_2 of the two complementary outputs of cross-coupled inverter pair are identical. The offset between these two node voltages is minimized at design time to ensure that the manufacturing process variations of the two MOS capacitors play a dominant role in determining the response bit, and the response bits generated by different cells of the array or the same cell address of different cell arrays are independently and identically distributed.

III. SIMULATION RESULTS AND QUALITY ANALYSIS

The proposed PUF with differential charging capacitors was simulated by Cadence Virtuoso Spectre using the process design kit (PDK) of HHGrace 0.11 μm E-flash 1.5 V Ultra Low Leakage 4P7M process. To simulate the reliability and uniqueness, Monte-Carlo (MC) simulation was performed with 1000 iterations. The nominal operating condition was set to be 25 $^{\circ}\text{C}$ and 1.5 V power supply. The variation option of the MC simulation was set to all for both mismatch and process variation. Furthermore, in order to examine the reliability, the 1000 iterations with the same MC simulation seed were repeated in different operating conditions by altering the environment temperature from 0 $^{\circ}\text{C}$ to 80 $^{\circ}\text{C}$, and changing the supply voltage by $\pm 20\%$ from its nominal value of 1.5 V. In total, nine sets of temperature and supply variation combinations were simulated.

A. Uniqueness

Uniqueness is a measure of the randomness of the PUF response distribution and is calculated by the average Hamming Distance (HD) between different MC iterations. An ideal PUF has a uniqueness of 50%. Let R_u and R_v be the n -bit responses of two different iterations, u and v , to the same input challenge C , the uniqueness U of m chips (viz. MC iterations) can be expressed as

$$U = \frac{2}{m(m-1)} \sum_{u=1}^m \sum_{v=u+1}^m \frac{HD(R_u, R_v)}{n} \times 100\% \quad (1)$$

Based on our simulation result, the uniqueness is calculated to be 50.03%, which is very close to the ideal 50%.

B. Stability

Reliability is a measure that indicates how stable the CRPs of a PUF measured at various time or operating conditions are. In this design, the bit error rate (BER) is calculated by setting the response in the nominal condition as reference, and the responses generated in various conditions were compared with the reference. Let R_i be an n -bit response to an arbitrary challenge C produced by the MC iteration number i in the nominal condition. The same challenge is then applied k times

to the same PUF cell under various operating conditions to obtain the responses $R_{i,j}$ for $j = 1, 2, \dots, k$. The reliability S is calculated by

$$S = 1 - \text{BER} = 1 - \frac{1}{k} \sum_{j=1}^k \frac{HD(R_i, R_{i,j})}{n} \times 100\% \quad (2)$$

The reliability of the proposed PUF was measured based on the responses generated by the MC simulation of 1000 iterations for each condition. The nominal operating condition was set to be 25 $^{\circ}\text{C}$ and 1.5V supply. The nominal condition is changed by combining temperature variation from 0 $^{\circ}\text{C}$ to 80 $^{\circ}\text{C}$ and power supply variation of $\pm 20\%$. The measured worst-case reliability is 97.70% across the range of temperature tested, and 96.20% across the range of supply voltage. On average, the PUF reliability S is calculated to be 97.26%.

C. Randomness

Randomness refers to the unpredictability of a PUF response. The responses of the PUF should be independently and identically distributed with an equal probability of bits “0” and “1”, and the response bits to different challenges of the same device or same challenge across different devices should be uncorrelated. The cryptographic randomness of a binary bitstream is commonly evaluated by autocorrelation test and National Institute of Standards and Technology (NIST) cryptographic randomness test.

1) Auto-correlation Test

The autocorrelation of a random process is statistically evaluated by the Pearson correlation between the values of the process at different times, as a function of the two times or of the time lag. The autocorrelation function (ACF) was used for the calculation of bit sequence autocorrelation. There are two inputs involved in ACF. One is the input bit sequence generated from the proposed PUF, the other is bit lag. Fig. 3 shows the plot of the autocorrelation test at 95% confidence level for 1000 consecutive bits generated by the proposed PUF. It plots the ACF values with the bit lags from 1 to 256. As shown in Fig. 3, most of the points are within the passing limits. According to [12], tighter limits imply less susceptibility to correlation analysis attacks.

2) NIST Test

The tests were carried out using the NIST SP 800 statistical test suite. The NIST test results are listed in Table I. A uniform distribution shown in columns C1 to C10 corresponds to a uniform frequency distribution of various P-values. The P-values calculated by a chi-square test are listed in the column next to C10. In each NIST test, the P-value calculated is a statistical indicator to quantify the level of randomness. To reach a confidence level of 99% for concluding an arbitrary information source to be random, a P-value greater than 0.01 is required [13]. From the results presented in Table I, the proposed PUF exhibits P-values greater than 0.01. The 12th column shows the rate of passing for the test sequences. All the calculated results attest the high randomness of the bit sequence produced by the proposed PUF.

Fig. 3. Autocorrelation test results.

D. PUF Speed and Power

Based on the simulation results, it takes 36 ns to generate a response bit. So, the PUF has a throughput of 27.78 Mbps. The average power consumption at this rate and the nominal supply voltage of 1.5 V is 20.86 μ W, and the corresponding energy consumption per response bit is 0.75 pJ/bit.

E. Comparisons with Previous Works

The performance of this work is compared with several existing weak PUFs. Table II lists the figures of merit, which include uniqueness, reliability, power and speed of six existing PUFs together with this work. Unfortunately, the power consumptions and throughput of [10], [14] and [15], as well as the uniqueness of [7] are not reported in those papers.

From the data presented in Table II, it is evident that the uniqueness results are all close to the ideal value of 50.0% except [8]. The main advantages of this proposed PUF over other weak PUFs are its high reliability and uniqueness, while remaining competitive in other figures of merit.

The proposed PUF has an important advantage over the other weak PUFs, especially the SRAM PUF, in terms of the reproducibility of response bit at different time. Since the response bits of an SRAM PUF are generated by powering down and up an entire array, the ramp up rate of the two outputs is highly susceptible to both temporal and spatial noises during the race period. This results in poor repeatability of response. A typical SRAM array is only capable of producing less than 90% of stable PUF response bits even under the same operating condition. Furthermore, with the change in the ambient temperature and the supply voltage, the response instability becomes even worse. According to [18], the worst-case inconsistent response bits can reach up to 20.5%.

Our proposed design does not rely on power-up reset to generate the response bits. The main entropy source is harnessed from the mismatch of the charging capacitor pair

instead of the cross-coupled inverters. In other words, the outcomes of an applied challenge depend less on the threshold voltage difference of the two cross-coupled inverters but more on the capacitance difference of the two matched MOS transistors. Unlike power-up reset of SRAM PUF, the charging process of the two MOS capacitors only commences after the supply voltage and the bias voltage have been stabilized. Under the same operating condition, the difference in capacitance values is relatively constant during the response generation process, which results in identical measurement at different times. Although this design has a drawback of using more transistors per cell, it dissipates less power per response bit as only the cell addressed by the challenge is active in response bit generation. Moreover, since the capacitors are still able to hold their charges even after the power supply is off, before the response droops to zero, there is no need to temporarily transfer the bit to a buffer memory before the response generation and restore them back after the response generation. This has eliminated the large overhead of mirror buffer memory required by SRAM PUF for dual mode operation.

IV. CONCLUSION

A reliable PUF based on differential charging capacitors has been presented. The proposed PUF harvests the rich entropy of fabrication process induced MOS capacitance mismatch to generate random but yet more robust response bits that are less susceptible to voltage and temperature variations. The design avoids the pitfall of power-up reset in conventional memory PUF design to conserve power consumption. Using Cadence Spectre with HHGrace 110 nm models, Monte-Carlo simulations were performed with the temperature varied from 0°C to 80°C and supply voltage varied from 1.2 V to 1.8 V ($\pm 20\%$ of nominal 1.5 V). The uniqueness of the proposed PUF was calculated to be 50.03% and its worst-case reliability was 97.70% over the range of temperature and 96.20% over the range of supply voltage simulated. Other figures of merit were also competitive compared with six other existing weak PUFs. The power dissipation and throughput were measured to be 20.86 μ W and 27.78 Mbps, respectively.

ACKNOWLEDGEMENT

The authors would like to acknowledge the support of the the Singapore Ministry of Education Tier 1 Grant MOE2018-T1-001-131 (RG87/18), National Natural Science Foundation of China (61601168), Natural Science Foundation of Jiangsu Province (BK20170205), and the Major Scientific Research Project of Zhejiang Lab (Grant No. 2018FD0ZX01).

TABLE I. NIST TEST RESULTS

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-Value	PROP	TEST
1	1	1	1	1	2	2	0	1	0	0.911413	10/10	Frequency
1	1	1	1	1	2	2	0	1	0	0.911413	10/10	BlockFrequency
1	2	2	2	0	0	0	0	2	1	0.534146	10/10	CumulativeSums (forward)
1	1	0	2	1	1	1	1	2	0	0.911413	10/10	CumulativeSums (backward)
1	1	1	1	2	0	4	0	0	0	0.122325	10/10	Runs
0	1	2	3	0	1	1	0	0	2	0.350485	10/10	Serial (forward)
1	2	1	1	1	1	1	0	2	0	0.911413	10/10	Serial (backward)
1	1	1	0	2	0	1	1	2	1	0.911413	10/10	LinearComplexity

TABLE II. COMPARISON AMONG WEAK PUFs

PUF	Uniqueness	Reliability	Power (μ W)	Speed (Mbps)	Test Condition
[10]	49.97%	88%	NA	NA	-20°C to 80°C, nominal supply
[14]	49.20%	97.12%	NA	NA	25°C to 85°C
		86.60%			0.67 V to 0.87 V
[15]	49.97%	94.93%	NA	NA	10°C to 85°C, nominal supply
[7]	NA	95.00%	250	0.03	-25°C to 125°C, 1.5 V to 5 V
[8]	64.70%	96.96%	0.93	1	0.9 V to 1.2 V
[9]	50.01%	96.50%	54.8	10	0°C to 80°C, 0.6 V to 1.2 V
This Work	50.03%	97.70%	20.86	27.78	0°C to 80°C
		96.20%			1.2 V to 1.8 V

REFERENCES

- [1] C. H. Chang, Y. Zheng and L. Zhang, "A retrospective and a look forward: fifteen years of physical unclonable function advancement," *IEEE Circuits and Systems Magazine*, vol. 17, no. 3, pp. 32-62, 2017.
- [2] Z. Liu, H. Jin, Y. Hu and M. Bailey, "Practical Proactive DDoS-Attack Mitigation via Endpoint-Driven In-Network Traffic Control," in *IEEE/ACM Transactions on Networking*, vol. 26, no. 4, pp. 1948-1961, Aug. 2018.
- [3] Y. Cao, Y. Gao, R. Tan, Q. Han and Z. Liu, "Understanding Internet DDoS Mitigation from Academic and Industrial Perspectives," in *IEEE Access*, vol. 6, pp. 66641-66648, 2018.
- [4] Z. Liu, Y. Cao, M. Zhu and W. Ge, "Umbrella: Enabling ISPs to Offer Readily Deployable and Privacy-Preserving DDoS Prevention Services," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1098-1108, April 2019.
- [5] Zhuotao Liu, Hao Jin, Yih-Chun Hu, and Michael Bailey. 2016. MiddlePolice: Toward
- [6] Enforcing Destination-Defined Policies in the Middle of the Internet. In *Proceedings of the*
- [7] 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). ACM,
- [8] New York, NY, USA, 1268-1279.
- [9] Z. Liu, Y. Cao, M. Zhu and W. Ge, "Umbrella: Enabling ISPs to Offer Readily Deployable and Privacy-Preserving DDoS Prevention Services," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1098-1108, April 2019.
- [10] C. Herder, M.-D. Yu, F. Koushanfar and S. Devadas, "Physical unclonable functions and applications: a tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126-1141, Aug. 2014.
- [11] K. Lofstrom, W. Daasch and D. Taylor, "IC identification circuit using device mismatch," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, pp. 372-373, San Francisco, CA, USA, Feb. 2000.
- [12] Y. Su, J. Holleman and B. Otis, "A 1.6 pj/bit 96% stable chip-ID generating circuit using process variations," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, pp. 406-407, San Francisco, CA, USA, Feb. 2000.
- [13] J. Li and M. Seok, "Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 9, pp. 2192-2202, Sept. 2016.
- [14] J. Guajardo, S. S. Kumar, G.-J. Schrijen and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protections," in *Proc. Int. Workshop on Cryptographic Hardware and Embedded Sys. (CHES)*, pp. 63-80, Vienna, Austria, Sept. 2007.
- [15] W. F. Lyu, G. Y. Wang, M. Lin and L. L. Sun, "Statistical modeling of gate capacitance variations induced by random dopants in nanometer MOSFETs reserving correlations," *Chinese Physics. Lett.*, vol. 32, no. 10, 108502, 2015.
- [16] S. K. Mathew *et al.*, "2.4 Gbps, 7 mW all-digital PVT-variation tolerant true random number generator for 45 nm CMOS high-performance microprocessors," *IEEE Journal of Solid-State Circuits*, vol. 47, no. 11, pp. 2807-2821, Nov. 2012.
- [17] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *NIST Special Publication 800-22*, Apr. 2010.
- [18] Y. Zheng, M. S. Hashemian and S. Bhunia, "RESP: A robust physical unclonable function retrofitted into embedded SRAM array," in *Proc. ACM/EDAC/IEEE Design Automation Conf. (DAC)*, pp. 1-9, Austin, USA, Jun. 2013.
- [19] F. Zhang, S. Yang, J. Plusquellic and S. Bhunia, "Current based PUF exploiting random variations in SRAM cells," in *Proc. Design, Automation and Test in Europe Conf. Exhibition (DATE)*, pp. 277-280, Dresden, Germany, Mar. 2016.
- [20] G.-J. Schrijen and V. Leest, "Comparative analysis of SRAM memories used as PUF primitives," in *Proc. Design, Automation and Test in Europe Conf. Exhibition (DATE)*, pp. 1319-1324, Dresden, Germany, Mar. 2012.