Design and security evaluation of PCM-based rPUF using cyclic refreshing strategy

Qi Zhang[1,2,3], **Houpeng Chen**[1,2a)], **Yaoyao Lu**[1,2,3], **Xiaoyun Li**[1,2,3], **and Zhitang Song**[1,2]

[1] *State Key Laboratory of Functional Materials for Informatics, Shanghai 200050, China*

[2] *Shanghai Institute of Micro-system and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*

[3] *University of Chinese Academy of Sciences, Beijing 100049, China*

a) *chp6468@mail.sim.ac.cn*

Abstract: Memory-based physical unclonable functions (PUFs), top priorities in the hardware security applications, are in the face of limited challenge-response pairs (CRPs). Concerned with this, we propose a differential reconfigurable PUF (rPUF) scheme with phase change memory (PCM) in this paper. By making use of the spontaneous resistant randomness between cycles, a simple but practical method for reconfiguration is realized. 30 PCM chips in 40-nm process are measured for their electrical properties and the PUF system is simulated. Diffuseness, uniqueness and stability of our PUF system are very close to the industry standards according to the experimental results. Meanwhile, system crisis from exhausted CRPs is remarkably decreased by effective entropy of cycling programming when the quantifiable level is increased.

Keywords: reconfigurable physically unclonable function, phase change memory, cycling randomness, hardware security

Classification: Integrated circuits

References

[1] R. Pappu, *et al.*: "Physical one-way functions," Science **297** (2002) 2026 (DOI: 10.1126/science.1074376).

[2] C. Q. Liu, *et al.*: "ACRO-PUF: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function," IEEE Trans. Circuits Syst. I, Reg. Papers **64** (2017) 3138 (DOI: 10.1109/TCSI.2017.2729941).

[3] G. E. Suh and S. Devadas: "Physical unclonable functions for device authentication and secret key generation," Proc. 44th Annu. Design Autom. Conf. **E98-C** (2007) 9866900.

[4] D. Lim, *et al.*: "Extracting secret keys from integrated circuits," IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **13** (2005) 1200 (DOI: 10.1109/TVLSI.2005.859470).

DOI: 10.1587/elex.15.20180239
Received March 6, 2018
Accepted April 4, 2018
Publicized April 20, 2018
Copyedited May 25, 2018

[5] D. E. Holcomb, *et al.*: "Initial SRAM state as a fingerprint and source of true random numbers for RFID tags," Proc. Conf. RFID Secur. (2007) 1.2.
[6] A. Chen: "Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions," IEEE Electron. Device Lett. **36** (2015) 138 (DOI: 10.1109/LED.2014.2385870).
[7] T. Marukame, *et al.*: "Extracting physically unclonable function from spin transfer switching characteristics in magnetic tunnel junctions," IEEE Trans. Magn. **50** (2014) 1 (DOI: 10.1109/TMAG.2014.2325646).
[8] K. Kursawe, *et al.*: "Reconfigurable physical unclonable functions enabling technology for tamper-resistant storage," IEEE International Workshop on Hardware-Oriented Security and Trust (2009) 22 (DOI: 10.1109/HST.2009.5225058).
[9] Y. Gao, *et al.*: "Emerging physical unclonable functions with nanotechnology," IEEE Access **4** (2016) 61 (DOI: 10.1109/ACCESS.2015.2503432).
[10] S. Raoux, *et al.*: "Phase-change random access memory: A scalable technology," IBM J. Res. Develop. **52** (2008) 465 (DOI: 10.1147/rd.524.0465).
[11] L. Zhang, *et al.*: "PCKGen: A phase change memory based cryptographic key generator," IEEE ISCAS (2013) 1444 (DOI: 10.1109/ISCAS.2013.6572128).
[12] D. Ielmini, *et al.*: "Physical interpretation, modeling and impact on phase change memory (PCM) reliability of resistance drift due to chalcogenide structural relaxation," 2007 IEEE Inter. Elec. Dev. Meet. (2007) 939 (DOI: 10.1109/IEDM.2007.4419107).
[13] A. Redaelli, *et al.*: "Numerical implementation of low field resistance drift for phase change memory simulations," 2008 NVSMW (2008) 39 (DOI: 10.1109/NVSMW.2008.17).
[14] M. Le Gallo, *et al.*: "Inherent stochasticity in phase-change memory devices," 2016 46th ESSDERC (2016) 373 (DOI: 10.1109/ESSDERC.2016.7599664).
[15] Y. Gao, *et al.*: "Memristive crypto primitive for building highly secure physical unclonable functions," Sci. Rep. **5** (2015) 12785 (DOI: 10.1038/srep12785).

1 Introduction

In recent decades, booming development of Internet of Things (IoTs) brings about an inventible challenge in authentication and cryptography. Compared with traditional security system using software encoding method, physical unclonable functions (PUFs) [1] becomes a priority for the reason of both easier on-chips building and duplicating impossibility, as well as the capability of defending mobile electronic devices against both non-invasive and semi-invasive attacks [2]. Many different topologies of PUFs have been proposed in the last few years [3, 4, 5, 6, 7, 8]. With the scaling down of CMOS process, however, PUFs with nanotechnology are showing out more severe levels of inherent randomness due to fabrication process variations [9]. The so-called reconfigurable PUFs (rPUFs) based on memory devices can simplify the PUF circuits by storing encryption keys spontaneously and solve the break-down crisis by refreshing keys unexpectedly at the same time. In consequence, these nanoscale rPUFs possess better performance over conventional CMOS PUFs.

Phase-change memory (PCM) is one of the possible alternative memory structures proposed for its high density, fast read accessing and remarkable scalability [10]. Such memory cell is a two-terminal device and use resistance to

DOI: 10.1587/elex.15.20180239
Received March 6, 2018
Accepted April 4, 2018
Publicized April 20, 2018
Copyedited May 25, 2018

represent information. Switching from high resistance (RESET state) to low resistance (SET state) is called 'set', whereas the reverse process is called 'reset'. Transition between the two states can be triggered by an electrical stimulus. K. Kursawe proposed the concept of PCM PUF for the very first time [8], while L. Zhang further studied the resistant variation related to programming currents and proposed a PCM key generator by using logarithmic amplifier [11]. Besides, several other characteristics of PCM affecting the reliability of the security system should also be concerned. For example, device resistance increasing as time goes on, called as resistance drift [12], degrades the uniformity of PUF system. Other phenomenon like cycling randomness, in contrast, provides new potentiality for increasing the number of Challenge-Response pairs (CRPs) and might enhance the system diffuseness and security. From these perspectives, we propose a PUF topology with differential method based on PCM and investigate the reconfigurable PUF system allied to cycling randomness for the first time.

This paper is organized as follow. The first section is the introduction. In Section II, we will state about several features of PCM and then propose a novel PUF system based on PCM in Section III. After that, we will elaborately analyze the security performance of our system. The last part will be the conclusion.

2 Characteristics for phase change memory

2.1 Resistance drifting of phase change material

It is well known that phase change memory realizes state changing by switching phase change material between amorphous and crystalline states with the application of electrical-pulse generated heat. Nonetheless, after a PCM cell is programmed, its resistance value can increase over time in result of structural relaxation physical phenomena [12]. More importantly, the drift coefficient increases monotonically with normalized resistance following an almost logarithmic law [13]. So, the drift effect is more noticeable in RESET state than SET state. As for PUF applications, the responses corresponding to the same challenge at different time nodes for one PUF should be the same. This requires a stable resistance value for the PUF device. Therefore, we choose to use PCM devices in SET state and further degrade this effect by using the differential scheme with two nearby PCM cells for variation generator.

2.2 Process variation and cycling randomness

Basically, the process variations of PCM device, such as the randomness in geometric structure and heater material, lead to a substantially difference in resistance from cell to cell after programming as shown in Fig. 1(a). Since the randomness derived from these inherent fabricated uncertainties are completely unpredictable, true random cryptophytic signatures can be realized via delicate circuits. In addition, the measurement results in Fig. 1(b) also show that the device resistance after each cycle with the same pulse can even be stochastic. Actually, it is inevitable because in each transition from SET to RESET, the high atomic mobility in the molten state results in substantially different distributions of quenched-in crystalline nuclei. This causes a unstableness in both effective amorphous thickness

DOI: 10.1587/elex.15.20180239
Received March 6, 2018
Accepted April 4, 2018
Publicized April 20, 2018
Copyedited May 25, 2018

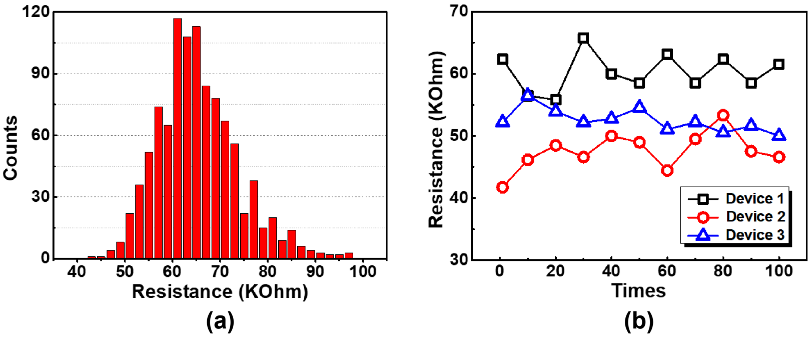

Fig. 1. (a) Resistance distribution for 1 K-bit PCM cells in SET state which are firstly programmed to fully RESET state (b) Resistance of 3 PCM devices in 100 cycles (SET pulse: 0.4 mA, 500 ns; RESET pulse: 0.6 mA, 100 ns)

and activation energy for conduction and arises a random memory switching from RESET to SET in further extent [14]. In order to address the issues like exhaustive CRP access attacks to PUFs that possess a limited number of CRPs [15], the method of reconfiguration by using cycling randomness is proposed. Although this approach has been mentioned for many times to date, its reliability has rarely been investigated in the past to the best of our knowledge. For the sake of it, we will make the first step in evaluating the system security from the aspect of response regeneration in cycles.

3 Differential topology of PCM PUF circuit

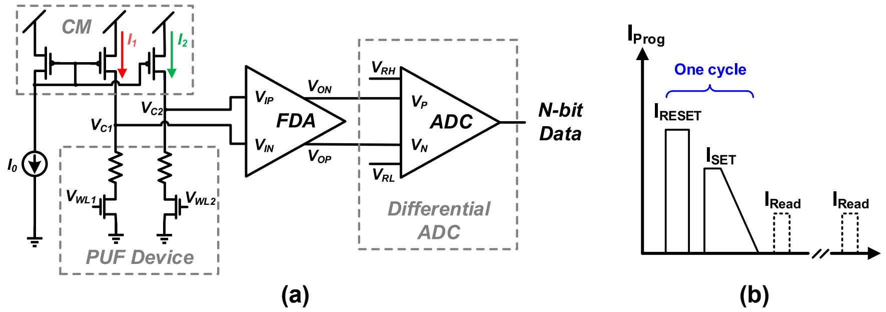

Fig. 2. (a) Differential PCM PUF scheme (b) Pulse sequence for device programming

As shown in Fig. 2(a), a fully differential topology of PCM PUF system is proposed for its high dynamic range and immunity to noise. I_0 is a reference current which can be adjusted from outside. I_1 equals to I_2 via current mirror (CM) structure. The resistant values of two PCM cells controlled by the inputted challenge are sampled via voltages V_{C1} and V_{C2}, and the differential voltage is amplified by a fully differential amplifier in negative feedback connection. After that, the amplified signal will be converted into N-bit digital data as a response. Other parts, like decoders and programming scheme for PCM cells are not presented here, however, the most important sequence for write operation is shown in Fig. 2(b). All the cells in PCM-PUF array should be programmed by a high-

DOI: 10.1587/elex.15.20180239
Received March 6, 2018
Accepted April 4, 2018
Publicized April 20, 2018
Copyedited May 25, 2018

narrow current pulse into a fully-RESET state and then programmed by a low-wide current pulse into SET state. Only after these procedures, which we defined as one cycle, the read operation can be carried out.

4 Experiments and results

In this paper, the resistant values for PCM cells were measured at room temperature from 30 chips of 1 K-bit PCM-PUF array with periphery circuits including programming circuits using SMIC 40 nm process. The PCM cells are made in sandwich structure with C-GST material and blade-type heaters of 6 nm × 63 nm. All the cells are firstly ‘reset’ by a 0.6 mA, 100 ns current pulse and then ‘set’ by a current pulse with max magnitude of 0.4 mA in 500 ns. Then, we applied these results in our differential PCM-PUF circuits and simulate out the response streams by Cadence.

4.1 Three evaluation terms for PCM-PUF system

Essential security evaluations of PUF system are diffuseness, uniqueness and stability. They are usually estimated by three commonly employed performance metrics, named the bias, the inter-chip Hamming Distance (inter HD) and the intra-chip Hamming Distance (intra HD).

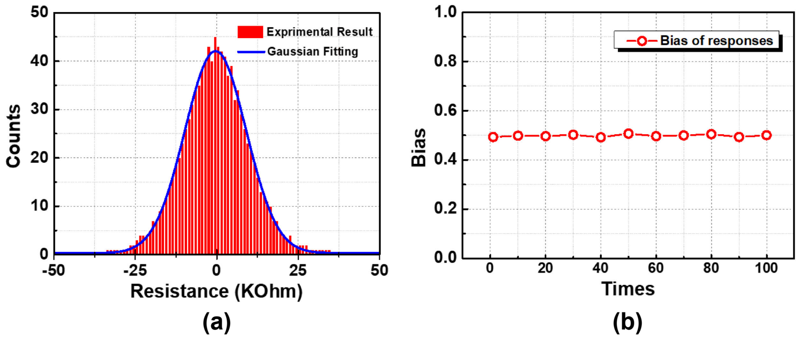

Fig. 3. (a) Resistance distribution of 1 K-bit PCM-PUF array (b) The biases of responses in 100-time read operation

Diffuseness The degree of diffuseness exhibited by a PUF is quantified in terms of the bias. It means that the difference among responses corresponding to different challenges for one PUF instance. The average tendency of the responses towards either a logical ‘0’ or a logical ‘1’ is showed via this term, which, ideally, no tendency can be observed when it equals to 0.5 in fraction.

In our research, we first build up our system with a 1-bit ADC, in another word, comparator. Because, as Fig. 3(a) shows, the typical differential resistant distribution of 1 K-bit PCM-PUF array is nearly fitting to Gaussian Distribution centered by 0. Therefore, the response of PUF challenge is defined as ‘1’ when the differential resistance is large than 0; otherwise is ‘0’. The biases calculated from the 1 K-bit response stream are all around 0.5 for 100-time measurements in a period of 10000 s, shown as Fig. 3(b). We can evidently conclude that the differential PUF resistances are random enough to become a foundation for PUF system and the differential PUF topology has a great immunity to resistance drifting effect.

© IEICE 2018
DOI: 10.1587/elex.15.20180239
Received March 6, 2018
Accepted April 4, 2018
Publicized April 20, 2018
Copyedited May 25, 2018

Uniqueness Uniqueness reflects the difference between responses from two PUFs when the challenge is the same. Due to intrinsic variations of PUF devices, the average inter HD is expected be close to 0.5 in fraction. And We use 30 PUF instances to estimate the uniqueness of our PUF system and the result is shown in Fig. 4 with red bars. The mean of the fractional HD (FHD) is 0.4704 and the standard deviation (Std) is 0.0526.

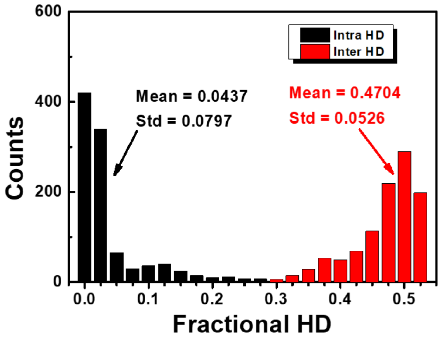

Fig. 4. Frequency counts for inter HD and intra HD of the results with 1-bit ADC PCM-PUF scheme

Stability The intra HD estimates the stability or reliability of a PUF by comparing a series of responses corresponding to the same challenge. The ideal value for an error-free PUF should be 0. In order to measure the consistency of our PUF system, the responses in 100-time read operations are collected and statistical data of intra HD for one PUF instance is shown in Fig. 4. Efficient defense against outside interference is obtained by most of the PUF devices while some devices exhibit a relatively big change attributed from noise or other environmental disturbs. In consequence, the mean and Std of intra HD are respectively 0.0437 and 0.0797.

In summary, the quantified results of the 1-bit PCM-PUF system demonstrates a competent performance in single cycle operation.

4.2 Security performance for reconfiguration in different cycles

The memory-based PUFs, which are usually configured using nano-crossbar, benefit from high density of array architecture for CRP increasing, but still belongs to weak PUFs. In order to overcome the drawbacks of limited CRPs, several potential features have been paid attention to. As for PCM, multi-level program shows a practical solution to refresh the distribution of device states for its sensitivity to program current. Alternatively, the stochastic results from cycle to cycle (C2C) even with equivalent program pulse seems to set up a more direct and easier way for reconfiguration. Therefore, we evaluated our system with the results from 100 cycles and detailed performance analysis are stated as below.

The statistic for biases calculated from 100-cycle data is firstly shown in Fig. 5(a). As we can see, the mean of biases is close to 0.5, showing a sufficient firmness in diffuseness.

In order to quantify the unpredictability for PUFs in different cycles, we develop a new metric named as inter-cycle Hamming Distance (inter HD_C2C).

© IEICE 2018
DOI: 10.1587/elex.15.20180239
Received March 6, 2018
Accepted April 4, 2018
Publicized April 20, 2018
Copyedited May 25, 2018

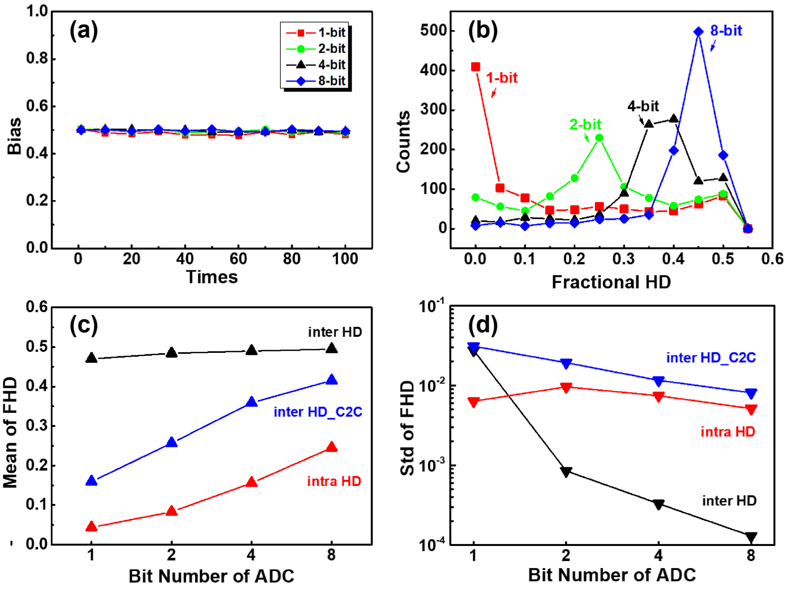

Fig. 5. (a) Biases for responses in 100 cycles; (b) Frequency counts for inter HD_C2C in different quantization levels; (c) Mean of three metrics in different quantization levels; (d) Std of three metrics in different quantization levels

If a PUF in two cycles produces R_i and R_j (n-bit response vectors) corresponding to the same challenge, then the inter HD_C2C can be defined as:

$$inter\ HD\_C2C = \frac{2}{m \times (m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \frac{HD(R_i, R_j)}{n} \tag{1}$$

Where m represents for the amount of cycles in the test. Similar with inter HD, the perfect reference value for a PUF instance ought to be 0.5 in average if the variation of resistance is large enough from cycle to cycle. However, when we use 1-bit ADC in our system, the mean of inter HD_C2C for the 1 K-bit PCM PUF responses is only 0.159, indicating that resistance varied in cycles cannot be distinguished on most occasions. Assume this deficient result is accused of the insufficient precision of quantifiable level, we reformed the PUF system with 2-bit, 4-bit and 8-bit ADC, respectively. Their max equivalent resistant magnitudes are all the same, i.e., ±20 kΩ, and the inter HD_C2C for different circuits are calculated. Shown as Fig. 5(b), the mean of inter HD_C2C is obviously moving towards 0.5. which we can also see from Fig. 5(c). Nevertheless, the highest value calculated from the 8-bit responses is 0.416, lower than 0.5. From this aspect, it can be inferred that, compared with the resistant variation contributed by the process fluctuation, a relatively weak variation from cyclic programming can only achieve the regeneration of responses when quantifiable interval is small enough.

Other estimated parameters are illustrated in Fig. 5(c) and (d). As we can see, the mean values of inter HD are all around 0.5, but still get a slight increase along with the bit number goes up. At the meantime, the impressive decline of Std for inter HD indicated an tighter distribution for inter HD. Thus, the differential PCM PUF topology is strengthened with a better uniqueness by a preciser scheme. Yet, better accuracy means higher sensitivity. The response changing for read operation due to surrounding turbulence, such as temperature fluctuation, is reflected from the

© IEICE 2018
DOI: 10.1587/elex.15.20180239
Received March 6, 2018
Accepted April 4, 2018
Publicized April 20, 2018
Copyedited May 25, 2018

accumulation of intra HD when the ADC possesses more bits. Hence, the condition for read operation should be constricted, or ECC circuit can be adopted.

4.3 Influence from cyclic endurance on PCM PUF system

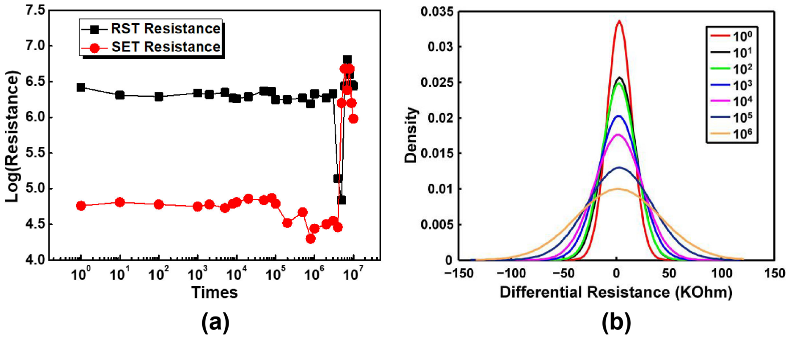

Fig. 6. (a) Endurance test result with 0.6 mA, 100 ns RESET pulse and 0.4 mA, 500 ns SET pulse; (b) Gaussian fitting curves for the resistance distribution of PCM-PUF array after a serious of cycles.

As a matter of fact, another characteristic of PCM, named as cyclic endurance, highly related to the uniqueness of PUF system, should also be concerned. We can basically see from Fig. 6(a) that the typical "stuck to RESET failure" is observed after about 10^6 times of cycling. We measured the differential resistance of PCM PUF array before this failure happened and the fitting curves illustrated in Fig. 6(b) display a wider and wider distribution of the PUF resistance when the cycle number accumulates. The results of average inter HD_C2C calculated in different magnitudes of cycling time change from 0.416 to 0.37, shown in Fig. 7, proving a descending tend after 100 cycles. Therefore, in order to maintain a stable performance using the method of cycling reconfiguration, the cycling time should be limited in certain range.

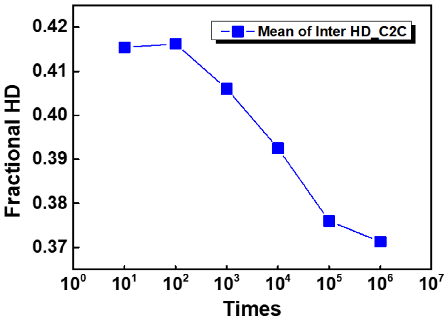

Fig. 7. Mean of inter HD_C2C as a function of cycling time with 8-bit ADC

5 Conclusion

The security performance for reconfigurable PCM PUF approaching with cyclic refreshing is evaluated in this paper. We firstly stated the resistance drifting effect of PCM and presented a differential topology of PCM PUF system accordingly. Then,

© IEICE 2018
DOI: 10.1587/elex.15.20180239
Received March 6, 2018
Accepted April 4, 2018
Publicized April 20, 2018
Copyedited May 25, 2018

we estimated the system efficiency from the perspectives of diffuseness, stability and uniqueness with the resistant experimental results from 30 40-nm PCM chips and further proposed the fourth metric, i.e. inter HD_C2C, to estimate the cycling randomness of PUF system. The simulation results show that, when we use 1-bit ADC in our system, the ideal values for the former three standards can be almost realized. However, the update for CRPs by cyclic reprogramming might fail for the reason of insufficient quantizaion level of the circuit, indicated by a low value of average inter HD_C2C. In view of this, we strengthened the accuracy of the system and better performance was evidently obtained for CRPs' regeneration. Combined with the simulation results based on endurance experiments, we can finally conclude that the unpredictable and unclonable PCM PUF is possibly accomplished with adequate quantizaion level within decent cycles.

Acknowledgments

Supported by the National Key Research and Development Program of China (2017YFA0206101, 2017YFB0701703), "Strategic Priority Research Program" of the Chinese Academy of Sciences (XDA09020402), National Integrate Circuit Research Program of China (2009ZX02023-003), National Natural Science Foundation of China (61376006, 61401444, 61504157, 61622408), Science and Technology Council of Shanghai (17DZ2291300).

DOI: 10.1587/elex.15.20180239
Received March 6, 2018
Accepted April 4, 2018
Publicized April 20, 2018
Copyedited May 25, 2018