Statistical Analysis of process variations on the delay-based PUF

Songde Hu, Huansheng Ning, Yang Xu, Lingfeng Mao
School of Computer & Communication Engineering
University of Science and Technology Beijing
Beijing, China

Youzhong Li,Lijun Zhang
School of Urban Rail Transportation
Soochow University
Suzhou, China

***Abstract*—Silicon physical unclonable function (PUF) is a special circuit that can reflect the uncontrollable intrinsic variation of integrated circuits (ICs) manufacturing process. These PUFs can be used as hardware security in security fields, such as authentication of devices and key generation in security applications. In order to know how the PUF circuits express the physical characteristics due to manufacturing process variations and provide a reference for researchers in the field of security, we briefly introduce the arbiter-based PUF and analyze the arbiter-based PUF in depth as it is a typical one of the silicon PUFs. Instead of paying attention to the whole PUF circuit which most studies do,we just focus on the stages so we can determine a demand of the arbiter. Monte Carlo simulation has been used to simulate the manufacturing process variations and the simulation is based on 40nm and 65nm technology libraries. Finally, a Monte Carlo-based statistical analysis has demonstrated that advanced technologies can enlarge intrinsic variation.**

Keywords—Physical unclonable function(PUF), intrinsic variation, Monte Carlo simulation, statistical analysis

I. INTRODUCTION

At present, among a lot of information security technologies, encryption techniques and identity authentication techniques are the two kinds of common means of protection[1]. However, these two methods have a few limitations to some extent. For example, classic cryptography protocols need secret key, but digitally stored secret keys can be easily attacked and cloned. In addition, the development of embedded system also brings new challenges to the current security mechanism and protocols. Embedded systems are not only in need of light-weight security protocols because of the strict power, cost and size constrains, but also easily facing physical attacks as they are often mobile [2].

Physical unclonable function (PUF) is a promising innovative primitive that are used for authentication and secret key storage by leveraging intrinsic manufacturing variability of deep submicron technology to create low power and area efficient security mechanisms[3]. Originally, a PUF is a mathematical function which is extracted from the behavior of a physical object or device[4]. But now, with the deepening of the study, it is gradually defined as a class of circuits, which are designed to map a set of challenges to responses replying upon the intrinsic manufacturing process variations in logical gates[5]. When referring to the integrated circuit, it is well known that it is unable to manufacture two identical circuits due to variations in the process. PUF circuits just take the advantage of this principle to achieve unclonable. From the point of view of integrated circuit, the principle of circuit design is the use of integrated circuit process parameters deviation existing in the manufacturing process. Process deviation in the same structure of the circuits result in parameter mismatch, such as delay and threshold voltage, and the mismatch impact the circuit performance [6]. The type of mismatch can be divided into two kinds: global mismatch M_{global} and local mismatch M_{local}, expressed as (1)

$$M_{total} = M_{local} + M_{global} \quad (1)$$

Global mismatch is caused by the fabrication technology in integrated circuits. Local mismatch is caused by inherent process variability. It is derived from the difference on atomic-scale and there is no way to control atomic-scale processes so far. The PUF circuit performance is the outcome of combined action of these mismatches. With the rapidly development of fabrication technology, the influence of the global mismatch will decrease gradually. But on the contrary, the influence on the circuit parameters caused by each atom will be intensified.

Physical unclonable function circuits can be used in many fields because of its advantages, such as true random number generator [7], privacy protection [8], IP protection [9] [10], public-key cryptography [11], key storage [12] [13], low cost authentication [14] in RFID tag [15] [16] or key cards [17]. Usually, PUFs can be formed as a single-chip secure processor [18], and linked inseparably to other device with the purpose of making it more security without compromising on cost or power [19] [20] [21].

At present, the literatures of PUF research are mainly focused on the PUF-based applications and the security of such circuits. Only few papers pay attention to the analysis on the basic structural unit of the PUF circuit. In view of this kind of situation, we make detail analysis on the PUF circuit and provide reliable simulation data for researchers who are not professional in electronic field to do future research. For simplicity, we choose Arbiter-PUF circuit as it is a typical one. In this paper, we design the circuit in 40-nm and 65-nm complementary metal-oxide-semiconductor (CMOS) technologies and use Monte Carlo simulation process library to

conduct simulation. The software tools we used are Hpice-2012, Cadence IC-5141 and CosmosScope-2011. The rest of this paper is organized as follows. The detailed about Arbiter-PUF is presented in Section II. Section III shows the Monte Carlo-based simulation methodology of arbiter-based PUFs. Section IV shows the simulation results. Section V draws conclusions and discusses future work.

II. ARBITER-BASED PUF

Arbiter-PUF was first described in the paper by Gassend et al. in 2004 using manufacturing variability in gate delay as the source of unclonable randomness [22]. The basic structure of it is shown in Fig.1. It has two parallel transmission lines and 128 delay stages. Each delay stage includes two symmetric multiplexers. Initial signals are applied to the two transmission lines simultaneously. And the challenges X[i] applied to every delay stage determine wheare the signals are transmited in cross or parallel as shown in Fig.2.All the input ports use step input signals. Every delay stage is designed in symmetric sizes to make sure the different of the delay is caused only by the manufacturing variations. Different challenges generate different response and we call this mapping relation CRP (challenge response pair).

There are many implementations of the delay stage. In [24],the author achieves the structure of the delay stage as the Fig.2 shown and we do the simulation analysis basing on this foundation architecture. In the delay stage built by NAND gates, shown in Fig.3, q and p (or r and s) are always chosen together, and meanwhile, they accord with the requirement of symmetry. So, we believe they can eliminate the delay bias caused by non-process-variation. The principle of Arbiter-PUF is that all the delay stages generate different time-delay on each path. The final response is determined by the different path selected by the 128 delay stages. In addition to delay stage, the other important part of the Arbiter-PUF is the ARBITER. The arbiter judges whether the top line or the bottom line is faster, and then outputs the response.

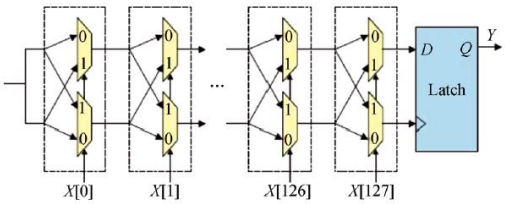


Fig. 1. Structure of arbiter PUF[23]

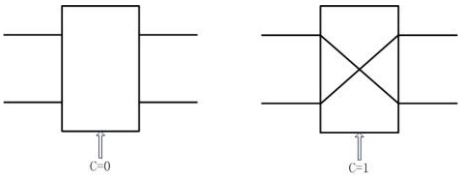


Fig. 2. Challenge determine the signal transmission mode

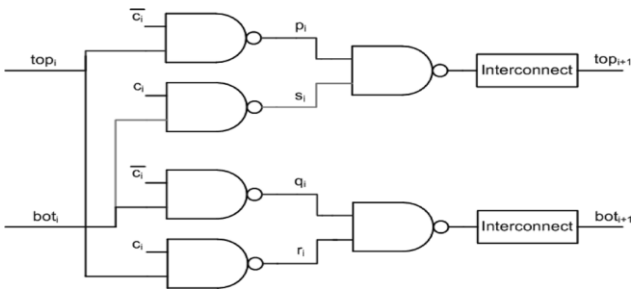


Fig. 3. Symmetric routing for single PUF stage circuit [24]

In Arbiter-PUF，the “Arbiter” takes on the important role of generating a response. But in the truth, the implementation of the role of the arbiter depends on the performance of the delay stage. The traditional arbiter is a D flip-flop or a set-reset (SR) latch. No matter which one is used in the circuit, there are limitations if the difference between the top and bottom delay path are too close. So, before designing the arbiter, we must make full research on the delay stage.

Incidentally, the arbiter PUF requires the routing of the two multiplexer chains to be completely symmetric or else the asymmetry of chains would dominate the effect of manufacturing variations. Hence, the arbiter PUF is difficult to be designed and implemented on FPGAs[25].

In this paper, we design the delay stage by NAND gates as Fig.5 shown. The schematic circuit diagram is shown in Fig.4. And the NOT gate used in the simulation is shown as Fig.6. The platform to do the simulation is Hspice-12.0.

Fig. 4. schematic circuit diagram

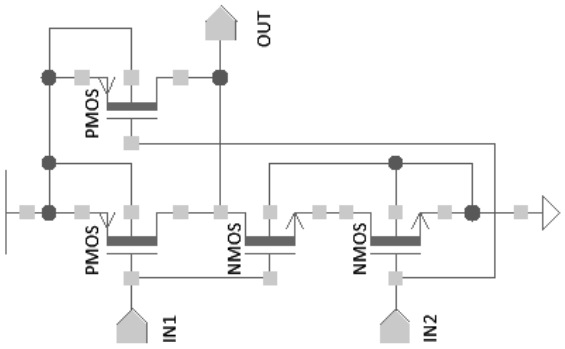
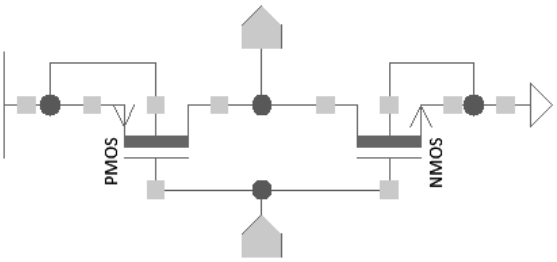


Fig. 5. NAND gate



Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

Fig. 6. NOT gate

III. MONTE CARLO SIMULATION

A. Simulation Model Selection

PUF circuit design principle is the use of integrated circuit process parameters deviation existing in the manufacturing process. The deviation of the process parameters will lead to the different operating characteristics of the different circuits with the same structure.

In the field of integrated circuit design, there are 3 main kinds of analysis methods to analyze the influence of process variables. One is called the PVT-corner(process, voltage, temperature)[26]. The aim of the PVT-corner is to get the suitable corner, namely F/S corner (Fast corner and Slow corner). The designers use the PVT-corner to design the circuit. And the advantage of this method is that the simulation speed is fast. But the shortcoming is obvious. The precision is not very high. The other method to analyze the circuit is called Monte Carlo statistic analysis[27]. Monte Carlo can show the distribution of variables in the statistical model and consider the correlation between the parameters of the model. But it need a lot of time to simulate. Sometimes, it may need a few days if the circuit is very complex. The last method is called High-Sigma statistic analysis [28]. High-Sigma statistic analysis is mainly used for designing the products which have strict requirements for finished product ratio.

In the study of PUF circuits, we need to observe the performance of the circuit in details. Moreover, the features of the PUF are produced by the physical properties of the transistors, so different physical parameters in the simulation model must be considered. Based on the above information, we finally choose the Monte Carlo statistic analysis to simulate and analyze the performance of the circuit. The PUF circuit is exactly not complicated. So, this experiment just avoided the shortcomings of MC statistic analysis.

B. The Cause of The Delay

The propagation delay of CMOS gates can be modeled [29] by（2）：

$$t_p = \left(\frac{V_{TH}+\alpha}{\frac{V_{DD}}{1+\alpha}} - \frac{1}{2}\right) t_T + \frac{C_L V_{DD}}{2\frac{W}{L_{eff}} P_C (V_{DD}-V_{TH})^{\alpha}} \quad (2)$$

Among many parameters in this equation, $V_{(DD)}$signifies a supply voltage and P_c and P_v are parameters, C_L is output capacitance, W is channel width, L_{eff} is effective channel length, V_{TH} is threshold voltage and α is velocity saturation index. Obviously, delay is depending on W and L. So, we determined that the simulation variables are width and length. In the actual simulation process, the width and length of the CMOS conform to the Gauss distribution.

C. Comparison Voltage Selection

The output of the PUF circuit is the result of the competition of two delay paths. So, it is important to set up the "finish point voltage". The following Fig.7 shows the trend of the voltage waveforms. The peak value of the output voltage of the circuit is 1.1V. During the process of the voltage value reaching 1.1V, the voltage values of two delay paths are very close in a long time. There exit two serious problems if 1.1V is selected as the "finish point". First, the arbiter can't distinguish which path is faster, because the voltage values are too close. Second, as the voltages are too close, the response of the PUF would be changed easily because of the noises, such as temperature. So, we need to choose a suitable voltage value. By analyzing the waveform, shown in Fig.8,we can know that when the "finish point" is 0.9V, the voltage difference between the two signals is very obvious, and the time interval of the two signals is more appropriate. The following tables show the output of the stage with temperature changes when 1.1V and 0.9V are chosen as "finish point".

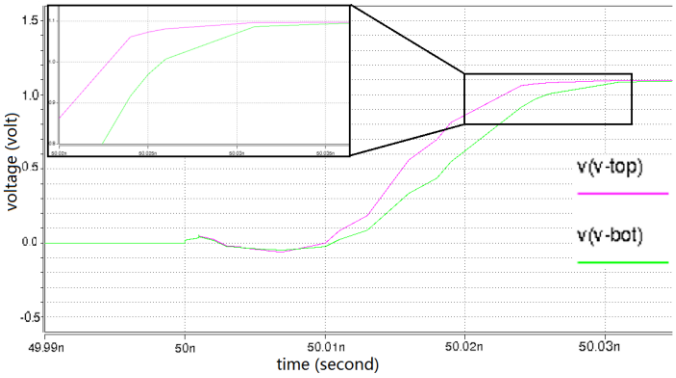


Fig. 7. Transmission Voltage Waveforms of the delay lines in a stage with given challenge. When closing to 1.1V， the two voltages become very close，but they don't peak for a long time. But when one voltage reached 1.1V, it will take a long time for another voltage to peak.

When 1.1V is selected, the response string will overturn as the temperature changed. Especially, as the temperature rises from 27 degrees to 30 degrees, the response changes continuously. But in table2, the response has been very stable. Choosing 0.9V as "finish point" has reduced the influence of environmental temperature effectively.

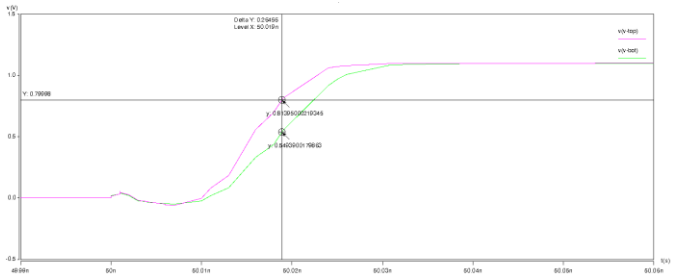


Fig. 8. There are problems if the voltage with the biggest delta is selected as the "Finish point voltage". So we turn to select a condition with a great voltage difference.

	Temp（℃）	Delay	Response
	0	-4.8997810 * 10^{-8}	0

Voltage =1.1V	20	$7.5190539 * 10^{-11}$	1
	21	$1.3863024 * 10^{-10}$	1
	22	$1.1554189\ 8\ 10^{-10}$	1
	23	$8.5024216 * 10^{-11}$	1
	24	$5.6499570 * 10^{-10}$	1
	25	$9.7986011 * 10^{-10}$	1
	26	$7.9465746 * 10^{-10}$	1
	27	$1.6088734 * 10^{-11}$	1
	28	$-4.4821579 * 10^{-11}$	0
	29	$4.9371822 * 10^{-08}$	1
	30	$-1.8498082 * 10^{-10}$	0
	50	$8.0476430 * 10^{-10}$	1

Table. 1. The tempertature dependences of the delay with 1.1 "finish point" voltage.

	Temp（℃）	Delay	Response
Voltage =0.9V	0	$3.4019211 * 10^{-12}$	1
	20	$3.0661677 * 10^{-12}$	1
	21	$3.0588894 * 10^{-12}$	1
	22	$3.0516230 * 10^{-12}$	1
	23	$3.0445434 * 10^{-12}$	1
	24	$3.0376576 * 10^{-12}$	1
	25	$3.0309435 * 10^{-12}$	1
	26	$3.0244152 * 10^{-12}$	1
	27	$3.0180686 * 10^{-12}$	1
	28	$3.0118973 * 10^{-12}$	1
	29	$3.0058995 * 10^{-12}$	1
	30	$3.0000701 * 10^{-12}$	1
	50	$3.3786021 * 10^{-12}$	1

Table. 2. The tempertature dependences of the delay with 0.9"finish point".

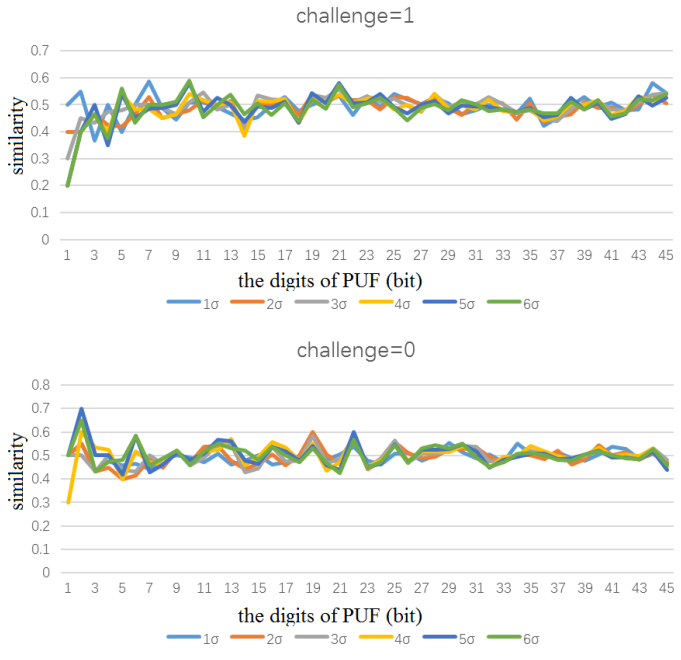


Fig. 9. The trend of similarity with a growing digits of PUF. The similarity is defined as the ration between Hamming distance and the digits of PUF.

D. Determine the times of simulation

In order to improve the efficiency of simulation, and also to be more scientific, we need to determine the appropriate times of simulation. Firstly, simulate the single stage 10 times with Monte Carlo Model Technology Library. And then, the 10 responses are divided into two groups, the first 5 outputs are combined into one group, and the later 5 outputs are combined into the other group. Finally, we calculate the inter-hamming distance between the two groups. In fact, by this way, we can regard these two groups as two PUFs with one challenge bit and five response bits. With the same method, we simulate 20 times and also divide the output into two groups. And then, calculate the inter-hamming distance. Ten times simulation increases every time, then calculate the Hamming distance. The simulation has been increased to 1000 times, finally draw the following Fig.9. In this figure, the abscissa represents a single PUF's response bits, namely half of the simulation times; The ordinate represents the similarity of two PUFs. As can be seen from the chart, when the number of simulation is less, the line is more unstable. With the increase of the times of simulation, the trend of the line gradually converges to a certain extent. When the simulation times are more than 600 times, the volatility of the discount is in the range of 0.43-0.53 generally.

IV. RESULT OF SIMULATING

In this paper, we mainly study the influence of the manufacturing process on the PUF circuit characteristics in simulation environment. After the previous discussion, we have determined the selection of the simulation method, the voltage "finish point" during the simulating and the times of simulation . We simulate the stage and generate responses with different challenges and different sigma. The stage is designed based on 40-nm and 65-nm.

By comparing the simulation results of different simulation models, the effects of the process on the PUF circuit characteristics are shown. On the other hand, by comparing the simulation results of different sigma based on the same simulation models, the influences of manufacturing capability on the PUF circuit are shown. In addition, we also analyze the two important properties, reliability and uniqueness, of the complete PUF from the simulation results. By simulating, we get the result as following.

Fig.10 summarizes the randomness results for stage simulation with different sigma across two simulation models. Whether challenge is 1 or 0, the results are very similar in the same technology node. The probability of 0 or 1 of the output is approximately close to 50%. Overall, whether choosing 40-nm simulation model or 60-nm simulation model, the probability of 0, namely the bottom delay path is faster than the top one, is slightly higher than the probability of 1. The maximum difference between the two probabilities is 6%, occurring in the simulating with the challenge is 1 in 40-nm simulation model. The change in Sigma can slightly change the randomness of the responses. As showing in each histogram, with the increase of sigma, the randomness of responses has improved slightly. This shows that with the increase of yield, the physical characteristics of each stage can be expressed

better. Since we find that the randomness in all cases is close to 50%, the PUF circuit consists of such stages should met security requirements. Although improving on process technology can't enhance the response's randomness obviously, we still need better process technology to produce circuits. This paper[24] refers to that technology scaling-down can improve temperature reliability and reduce the sensitivity of the circuit to temperature.

So far, only few papers pay enough attention to how small the bias is between the two delay paths. The bias's order of magnitude of the delay time has great influence on whether the PUF circuits can be used in practice. If the delay time is too short, the arbiter at the end of the circuit would be unable to make fair arbitration. And the response of the PUF circuit will fail. The delay of the circuit can be expressed as (3).

$$\text{Delay}=A*10^{-B} \qquad (3)$$

We simulate the stage 900 times and make the following figures. In Fig.11, magnitude B increased gradually along the X axis and the Y axis indicates the number of times that the B appears. The top two figures shows that the order of magnitude is mainly concentrated in 12. And, with the increase of the simulation precision, namely the increase of sigma, the number of B = 15 and 16 also begin to decrease. When selecting 65-nm simulation model, the results are interesting. The two figures below show that the change of simulation precision has great impact on B. The order of magnitude is mainly concentrated in 12 while choosing sigma=1.With the improvement of the simulation precision, the number of times of B=12 reduced rapidly. And finally, the order of magnitude is mainly concentrated in 13. As shown in Fig.11, we know that, when the yield is high, the magnitude of delay bias will increase. In the meanwhile, development of manufacture technology would bring down the order of magnitude of delay time. The main reasons for this result are as follows:

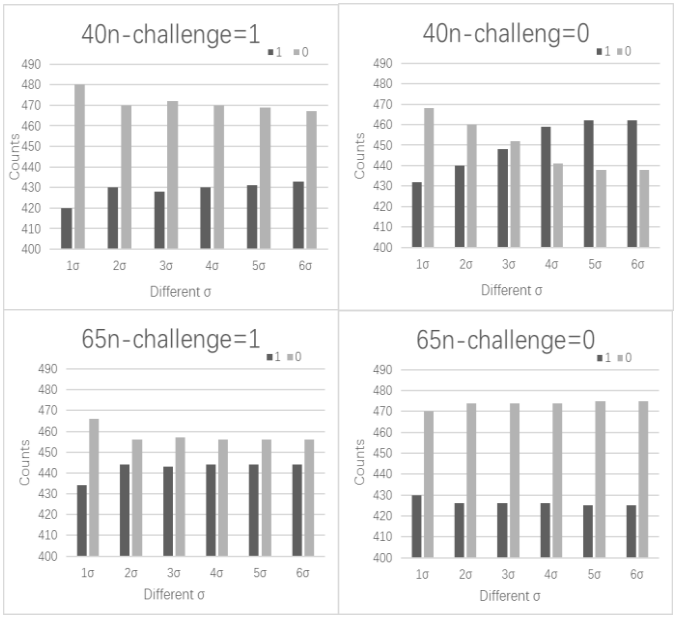
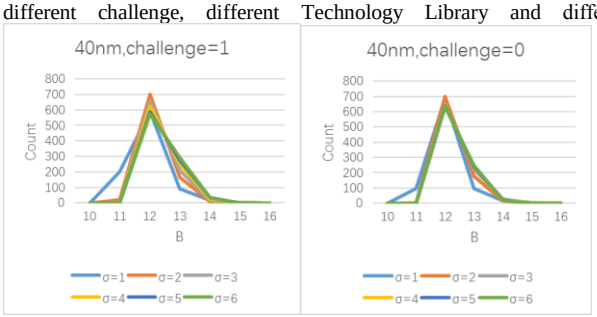


Fig. 10. The number of response 0 and 1 in 900 simulation results under different challenge, different Technology Library and different σ.



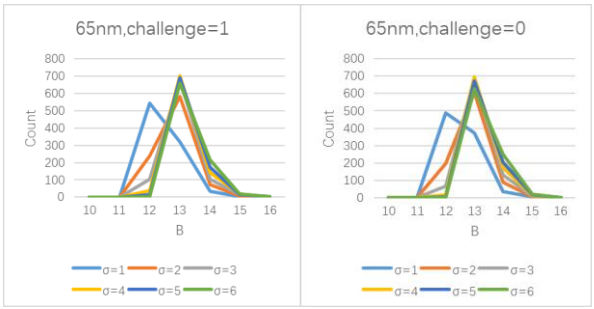


Fig. 11. The distribution of B in 900 simulation results under different challenge, different technology library， different σ

- Improving the yield can reduce the global mismatch M_{global}, but the local mismatch M_{local} is not changed while the simulation model remain the same. Therefore, the total mismatch M_{total} has changed. Eventually, leading to changes in the characteristics of the PUF circuit.
- The change of the simulation model leads to the change of local mismatch M_{local}. Because the order of magnitude in 40-nm simulation model is smaller than that in 65-nm simulation model, this shows that the effect of M_{local} is even greater.

V. CONCLUSION

After several years of development, the technology of PUF have made some progress, but it still has some shortcomings. In this paper, we have designed reasonable simulation experiments and obtained reliable simulation data, which will help security researchers make better judgment when they try to make use of PUF. From the experimental results, we can make conclude that the physical implementation of silicon PUFs still has some problems, which must be fully understood in PUF design and application in security field. The delay between the symmetric circuits is too short, which will seriously restrict the development of the application based on PUF. But there is no need to hold a pessimistic attitude towards PUF circuit. The simulation results show that CMOS technology scaling-down can effectively enhance the local mismatch influence. If appropriate adjustments and improvements are made to the stage and the arbiter, delay will be more obvious and this is our future work.

VI. ACKNOWLEDGMENT

This work was funded by National Natural Science Foundation of China (61471035), and Fundamental Research Funds for the Central Universities (06105031， 06500010). In particular, it was supported by Cybermatics and Cyberspace International Science and Technology Cooperation Base.

REFERENCES

[1] Majzoobi M, Koushanfar F. Time-Bounded Authentication of FPGAs[J]. IEEE Transactions on Information Forensics and Security, 2011, 6(3): 1123-1135.

[2] Majzoobi M, Koushanfar F, Potkonjak M, et al. Lightweight secure PUFs[C]. International Conference on Computer Aided Design, 2008.

[3] U. Ruhrmair, S. Devadas, and F. Koushanfar,"Security based on physical unclonabilityand disorder,'' Introduction to HardwareSecurity and Trust, M. Tehranipoor andC. Wang, Eds. New York, NY, USA:Springer-Verlag, 2012, pp. 65–102.

[4] Rührmair U, Sölter J, Sehnke F. On the Foundations of Physical Unclonable Functions[J]. Iacr Cryptology Eprint Archive, 2009.

[5] Chuang B, Xuecheng Z, Kui D, et al. A new physical unclonable function architecture[J]. Journal of Semiconductors, 2015, 36(3).

[6] Bernstein K, Frank D J, Gattiker A E, et al. High-performance CMOS variability in the 65-nm regime and beyond[J]. IBM journal of research and development, 2006, 50(4.5): 433-449

[7] Maiti A, Nagesh R, Reddy A, et al. Physical unclonable function and true random number generator: a compact and scalable implementation[C]// ACM Great Lakes Symposium on Vlsi 2009, Boston Area, Ma, Usa, May. 2009:425-428.

[8] Kardaş S, Çelik S, Yıldız M, et al. PUF-enhanced offline RFID security and privacy[J]. Journal of Network & Computer Applications, 2012, 35(6):2059-2067.

[9] Guajardo J, Kumar S S, Schrijen G J, et al. FPGA Intrinsic PUFs and Their Use for IP Protection[C]// Cryptographic Hardware and Embedded Systems - CHES 2007, International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings. 2007:63-80.

[10] Zheng J X, Potkonjak M. A digital PUF-based IP protection architecture for network embedded systems[C]// 2014:255-256.

[11] Batina L, Guajardo J, Kerins T, et al. Public-Key Cryptography for RFID-Tags.[J]. International Workshop on Pervasive Computing & Communication Security – Persec, 2007, 1(7):217-222.

[12] Yu M D, M'Raihi D, Sowell R, et al. Lightweight and Secure PUF Key Storage Using Limits of Machine Learning[M]// Cryptographic Hardware and Embedded Systems – CHES 2011. Springer Berlin Heidelberg, 2011:358-373.

[13] Cortez M, Roelofs G, Hamdioui S, et al. Testing PUF-based secure key storage circuits[C]// Conference on Design, Automation & Test in Europe. European Design and Automation Association, 2014:1-6.

[14] Zt E, Hammouri G, Sunar B. Towards Robust Low Cost Authentication for Pervasive Devices[C]// IEEE International Conference on Pervasive Computing & Communications. IEEE, 2008:170-178.

[15] Kardaş S, Çelik S, Yıldız M, et al. PUF-enhanced offline RFID security and privacy[J]. Journal of Network & Computer Applications, 2012, 35(6):2059-2067.

[16] Tuyls P, Batina L. RFID-Tags for Anti-counterfeiting[C]// The Cryptographers' Track at the Rsa Conference on Topics in Cryptology. Springer-Verlag, 2006:115-131.

[17] Gassend B, Clarke D, Van Dijk M, et al. Delay-based circuit authentication and applications[C]// ACM Symposium on Applied Computing. ACM, 2003:294-301.

[18] Suh G E, O'Donnell C W, Devadas S. AEGIS: A single-chip secure processor[J]. Information Security Technical Report, 2007, 10(2):570-580.

[19] Majzoobi M, Rostami M, Koushanfar F, et al. Slender PUF Protocol: A Lightweight, Robust, and Secure Authentication by Substring Matching[C]// IEEE Symposium on Security and Privacy Workshops. IEEE Computer Society, 2012:33-44.

[20] Lin L, Holcomb D, Krishnappa D K, et al. Low-power sub-threshold design of secure physical unclonable functions[C]// International Symposium on Low Power Electronics and Design, 2010, Austin, Texas, Usa, August. 2010:43-48.

[21] Yu M D, M'Raihi D, Sowell R, et al. Lightweight and Secure PUF Key Storage Using Limits of Machine Learning[M]// Cryptographic Hardware and Embedded Systems – CHES 2011. Springer Berlin Heidelberg, 2011:358-373.

[22] Lee J W, Lim D, Gassend B, et al. A technique to build a secret key in integrated circuits for identification and authentication applications[C]// VLSI Circuits, 2004. Digest of Technical Papers. 2004 Symposium on. 2004:176 - 179.

[23] Suh G E, Devadas S. Physical Unclonable Functions for Device Authentication and Secret Key Generation[J]. 2007:9-14.

[24] Lin L, Srivathsa S, Krishnappa D K, et al. Design and Validation of Arbiter-Based PUFs for Sub-45-nm Low-Power Security Applications[J]. IEEE Transactions on Information Forensics & Security, 2012, 7(4):1394-1403.

[25] 张吉良, 屈钢, 吕勇强, et al. A Survey on Silicon PUFs and Recent Advances in Ring Oscillator PUFs[J]. Journal of Computer Science & Technology, 2014, 29(4):664-678.

[26] P. G. Drennan, C. C. McAndrew,"Understanding MOSFET Mismatch for AnalogDesign,IEEE J. Solid State Circuits,March 2003.

[27] T.C. Hesterberg, Advances in importance sampling. Ph.D. Dissertation, StatisticsDept., Stanford University, 1988

[28] M. Qazi, M. Tikekar, L. Dolecek,D. Shah, and A. Chandrakasan, "Loop Flattening&Spherical Sampling: Highly Efficient Model Reduction Techniques for SRAMYield Analysis,,,Proc. Design Automation and Test in Europe, March 2010

[29] Sakurai T, Newton / R. Alpha-power law MOSFET model and its applications to CMOS inverter delay and other formulas[J]. IEEE Journal of Solid-State Circuits, 1990, 25(2):584-594.