Journal of Southeast University (English Edition) Vol. 34, No. 1, pp. 15 - 20 Mar. 2018 ISSN 1003—7985

A method to improve PUF reliability in FPGAs

Liang Huaguo Li Weidi Xu Xiumin Wang Haoyu

(School of Electronic Science and Applied Physics, Hefei University of Technology, Hefei 230000, China)

Abstract: Due to the impact of voltage, temperature and device aging, the traditional ring oscillator-based physical unclonable functions (RO-PUF) suffers from an unreliability issue, i.e., PUF output is subject to a constant change. To improve the reliability of the PUF, a stability test scheme related to the PUF mapping unit is proposed. The scheme uses ring oscillators with multiple complexity and various frequencies as sources of interference, which are placed near the PUF prototype circuit to interfere with it. By identifying and discarding unstable slices which lead to the instability of PUF, PUF reliability can be effectively improved. Experimental results show that surrounding logic circuits with multiple complexity and multiple frequencies can identify different unstable slices, and the higher the complexity, the more unstable slices are detected. Moreover, compared with newly published PUF literature, the PUF circuit possesses better statistical characteristic of randomness and lower resource consumption. With temperatures varying from 0 to 120 ℃ and voltage fluctuating between 0.85 and 1.2 V, its uniqueness and stability can achieve 49.78% and 98.00%, respectively, which makes it better for use in the field of security.

Key words: field programmable gate array (FPGA); physical unclonable function (PUF); security; ring oscillator (RO); reliability

DOI: 10.3969/j.issn.1003-7985.2018.01.003

With the rapid development of information technology, hardware security and credibility, which act as an important part in information security, have attracted significant attention. The physical unclonable function (PUF)[1-2], an emerging cryptographic primitive[3] using intrinsic integrate circuits (IC) to manufacture variables, presents a promising solution for low-cost device authentication and secure key generation. Different from traditional cryptography methods, PUFs extract signatures from complex inherent properties of physical materials rather than storing them in a non-volatile memory. Consequently, the keys generated by the PUF offer the advantages of low cost, volatility, unpredictability and a simple structure. Thus, it serves as an excellent solution for security related applications, such as chip encryption, key storage[4], authentication, FPGA intellectual property (IP) protection and ID generation[1-2,5-6].

Once the PUF is implemented with a nominally symmetric layout, the random mismatches induced by the manufacturing process determine the PUF outputs. However, when the fluctuation caused by the operating conditions is greater than or close to the mismatches, the outputs are likely to change constantly, i.e., poor reliability[7]. The conventional method used to improve PUF reliability is based on the use of error correction codes (ECC), while the approach significantly increases the complexity and cost of the design. Furthermore, the correcting code could reveal some important information. Another widely used method is mismatch selection, for instance, adjusting ring oscillator (RO) configuration to select the maximum frequency difference between two ROs with the same layout. Another common approach is to detect the bit-flipping situation of PUF responses by changing the operating conditions (voltage, temperature, aging, etc). However, this approach faces two main issues: 1) It needs to increase additional resources which consist of special voltage regulator circuits and temperature box equipment, etc. 2) It will be time-consuming due to the need for tuning operating conditions. To deal with these problems, we propose an effective test approach in FPGAs, utilizing the effect of different complexity of surrounding logic on PUF outputs to discard slices with bit-flipping (unreliable slices) and thus improve PUF reliability. This is achieved by mapping PUFs to cells which are highly reliable.

1 Related Works

Since Gassend et al.[1] proposed silicon PUF for the first time, researchers began to consider the factors affecting PUF reliability. They demonstrated that PUF is susceptible to environmental variations such as temperature, silicon aging[8], voltage[9], and the surrounding logic[10], which make it difficult to produce correct PUF responses.

To increase PUF robustness against environmental variations, one method is to choose the pairs only with large differences in initial frequencies[2]. However, the approach mainly faces an issue of high hardware resource overheads. In Ref. [11], data evaluation results show a reliability of 98.3% over the temperature range of 0 to

Received 2017-10-19, **Revised** 2018-01-05.

Biography: Liang Huaguo (1959—), male, doctor, professor, huagulg@hfut.edu.cn.

Foundation item: The National Natural Science Foundation of China (No. 61674048, 61371025, 61574052, 61604001).

Citation: Liang Huaguo, Li Weidi, Xu Xiumin, et al. A method to improve PUF reliability in FPGAs[J]. Journal of Southeast University (English Edition), 2018, 34(1): 15 - 20. DOI: 10.3969/j.issn.1003-7985.2018.01.003.

120 ℃ and 10% fluctuations in the supply voltage. As noted in Ref. [12], to improve PUF reliability, a configurable RO design was proposed, but the configurable oscillator design needs to add other gate units and multiplexers. In Ref. [13], a hybrid RO PUF with improved response stability was presented. Ref. [9] proposed an aging-resistant design which has 3.8% bits of PUF flip over a ten-year operational period due to the aging effect, compared with the conventional RO-PUF.

2 Design and Implementation of PUF

2.1 Ring oscillator PUFs

The proposed RO-PUF structure is shown in Fig. 1. The frequency of ring oscillators, composed of an odd number of inverters and some delay components, depends on manufacturing variations. Assuming that the two ROs generate periodical signals with the frequency of f_i and f_j ($i \neq j$), a final relative comparison of the counter values generates a logical 0 or 1 for this RO pair:

$$r_{i,j} = \begin{cases} 0 & \text{if } f_i < f_j \\ 1 & \text{otherwise} \end{cases}$$

where f_i and f_j are the frequencies of the i-th RO (RO_i) and the j-th RO (RO_j), respectively.

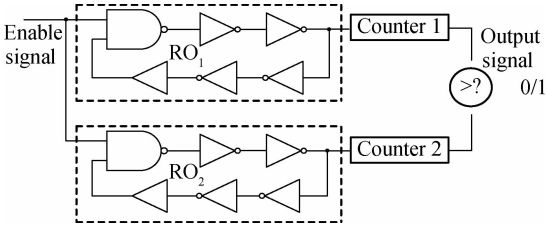

Fig. 1 RO-PUF structure

2.2 Hard macro design

In our design, the RO-PUFs are implemented on Xilinx Virtex-6 FPGA boards. Each RO consists of four inverters, an NAND gate and a buffer as shown in Fig. 2. Four inverters are implemented in a single slice. An NAND gate and a buffer are implemented in a single slice. Fig. 2 shows two nearly identical RO_1 and RO_2, implemented in four slices (slice_X_iY_j, slice_$X_{i+2}Y_j$, slice_X_iY_{j+1} and slice_$X_{i+2}Y_{j+1}$), the basic division of a Xilinx FPGA. Each slice contains four logic-function generators (or look-up tables). Fig. 2 also exhibits the result of estimated delay information between interconnections and gates provided by the Xilinx FPGA Editor.

The configurable logic blocks (CLBs) are the main logic resources for implementing sequential and combinational circuits. Fig. 3 shows that a hard macro with local routing for four inverters implemented in slice are completely identical with respect to placement and routing. A CLB element contains one pair of slices. To ensure identical routing for all RO instances, the locations of LUTs

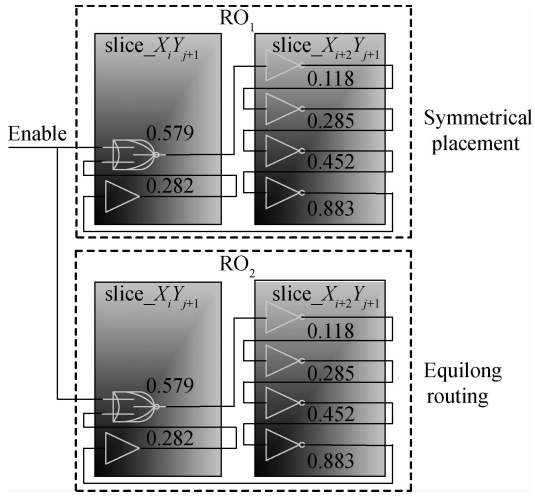

Fig. 2 Estimated delays between gates and interconnections (unit: ns)

and the measurement flip-flops are manually specified using relative location constraint, so that the identical placement of all PUFs can be achieved, which helps increase the uniqueness and randomness of the PUF outputs.

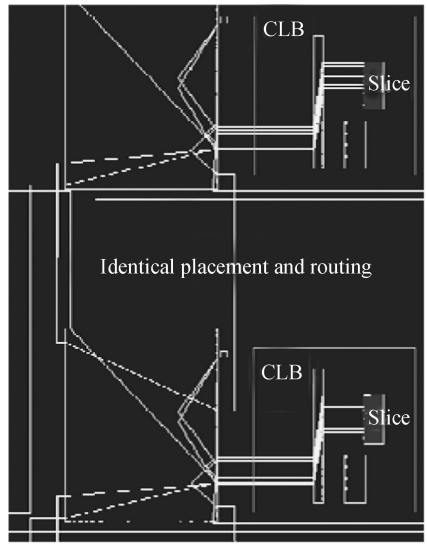

Fig. 3 Hard macro with local routing for four inverters (partial structure of RO) in a symmetrical slice

2.3 Surrounding logic design

In this paper, we present an effective reliability test methodology, by taking full advantage of surrounding logic circuits, to discard unsuitable slices, i. e., units which make PUF unstable after mapping into cells. First, we instantiate an array of original 128 PUFs with the hard macro implemented on the FPGA hardware resource. Meanwhile, the surrounding slices of original PUFs are manually disabled by using relative location constraints to obtain the original PUFs without interference. Then, the original 128-bit PUFs reliability tests are performed under a wide range of operating conditions.

As shown in the black border in Fig. 4, we can first implement 16-bit PUFs on the FPGA. Surrounding logic circuits with various complexity are applied to interfere with the 16-bit PUF circuits, and then the bits which make PUF circuits unstable (the bit-flipping bits) are discarded. There are two cases where surrounding logic circuit can act as a disturbance source, which are analyzed and discussed as follows.

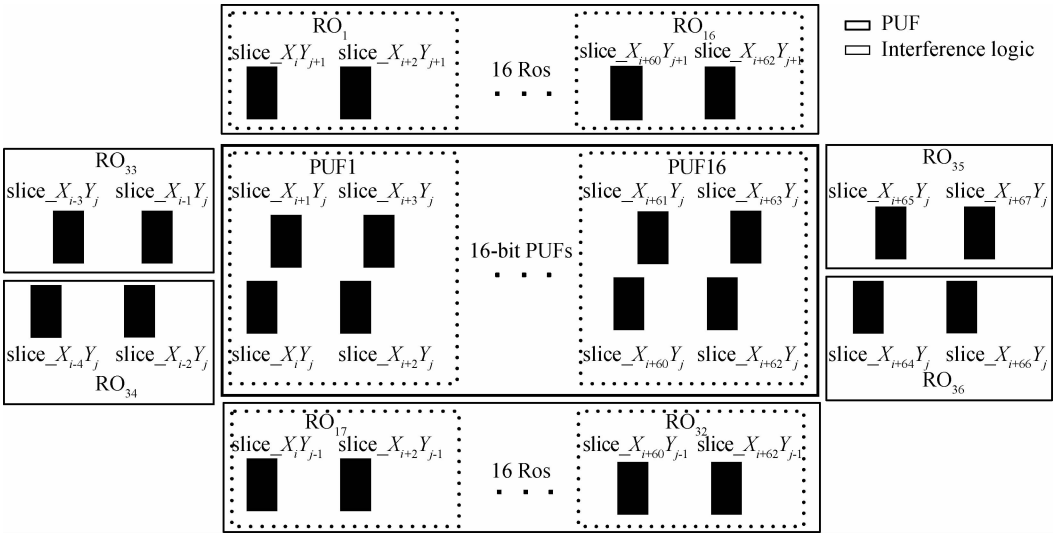

Fig. 4 Position distribution of the surrounding circuits

In the first case, we design a simple surrounding logic circuit, which is composed of 360 ring oscillators. In other words, 36 ring oscillators which are distributed close to the 16 PUFs are used as interference circuits. Their position distribution is shown in Fig. 4. Each ring oscillator consists of four inverters and an NAND gate, and the oscillation frequency of the ring oscillator is about 156 MHz. After discarding some of the unreliable slices by adding a surrounding logic circuit, we randomly extract 128-bit PUFs from the remaining relatively reliable PUFs and test their reliability. In the second case, we change the oscillation frequency of the ring oscillator and increase the complexity of the surrounding logic circuit. Here, the complex logic interference is from the 16-bit PUFs added with an extra 32 oscillators, and then the oscillation frequency of the ring oscillator is changed into about 215 MHz. More slices were discarded due to unreliability among the original PUFs. Finally, we randomly extract 128-bit PUFs from the remaining relatively reliable PUFs and test their reliability again.

3 Experimental Results and Analysis

To demonstrate the positive effects of the presented strategies on the quality of RO-PUFs, we first implemented 160 PUFs on the FPGA hardware resource, and then added surrounding logic near the 160 PUF instances and discarded these unreliable PUFs with bit-flipping.

As shown in Tab. 1, it reflects clear results after interference by simple and complex surrounding logic. We can find that after being interfered with by performing simple logic circuit, eight PUFs among them are discarded due to unreliability, and then we continue to add more complex surrounding circuits close to the remaining 152 PUF circuits. The data shows that other six unreliable PUFs have been found.

Tab. 1 RO-PUF quality results after interference by simple and complex surrounding logic

Interference type	Original PUF size	Unreliable PUFs	Remaining PUFs	Extracted PUF size
Simple interference	160	8	152	128
Complex interference	152	6	146	128

3.1 Uniqueness

We used our in-house data to validate the uniqueness and reliability of our approach. The PUFs are changed from 0 to 120 ℃ and the core voltage from 0.85 to 1.2 V, so that we can determine the percentage of flip in PUF response bit-streams under environmental variations. Fig. 5 shows the histograms of the inter-chip HD for our 8RO-PUF outputs under a normal temperature of 20 ℃. The

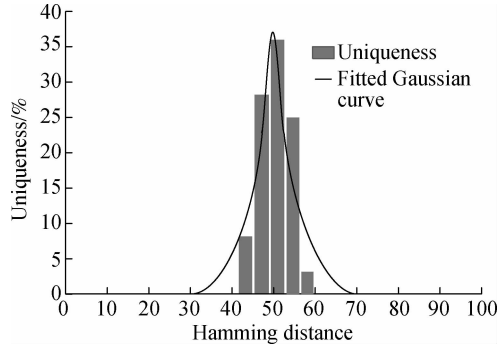

Fig. 5 Hard uniqueness profile under different FPGA configuration logic blocks and chips

mean Hamming distance of each histogram is 49.78%. Experimental results show that our PUF has near-ideal uniqueness.

3.2 Reliability

3.2.1 Reliability of original PUFs

To evaluate the reliability of PUFs without any surrounding logic circuits, the intra-chip HD is defined as the Hamming distance between the response sequences when realizing all sample data on the same chip under different operating conditions (Temperature varies from 0 to 120 ℃ and voltage changes from 0.85 to 1.2 V). Here, the core supply voltage is 1 V. As can be seen in Fig. 6, the mean value of the intra-chip variation in the implemented original RO-PUFs with 128-bit IDs is equal to 5.77% (PUF reliability is 94.23%), meaning that the average intra-chip Hamming distance (D_{intra}) is less than 7.4 bits from the 128-bit IDs. It also indicates that the original PUFs without any surrounding logic circuits have relatively low reliability.

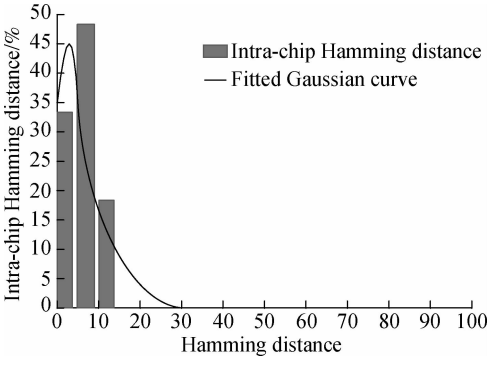

Fig. 6 Reliability under voltage and temperature variations for RO-PUF

3.2.2 Reliability test after processing

After adding simple surrounding logic circuits, 8-bit PUFs are discarded due to unreliability. Fig. 7(a) shows the reliability testing results of 128 PUFs which are extracted randomly from the remaining relatively reliable 152-bit PUFs. The mean value of the intra-chip variation in generated 128-bit IDs is equal to 3.69%, meaning that there is only 3.69% unreliable bits occupying the total instantiated PUFs (PUF reliability is 96.31%).

After adding complex surrounding logic, more 6-bit PUFs are discarded due to unreliability from the 152-bit PUFs. Fig. 7(b) shows the reliability testing result of 128 PUFs which are extracted randomly from the remaining relatively reliable 146-bit PUFs. We find that the mean value of the intra-chip variation in generated 128-bit IDs is equal to 2.00%, meaning that the average intra-chip Hamming distance is less than 2.6 bits in generated 128-bit IDs (reliability probability is 98.00%). It also indicates that our proposed methodology can effectively improve PUF reliability when taking surrounding logic into account.

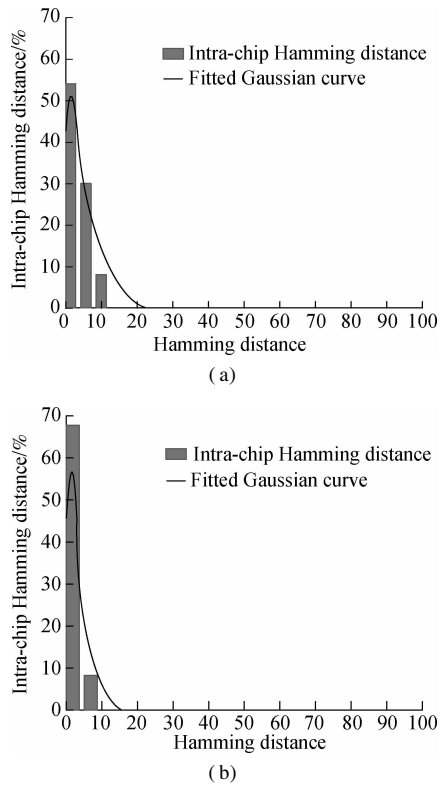

Fig. 7 Reliability result. (a) Simple interference; (b) Complex interference

3.3 Randomness

The NIST statistical test suite established for evaluating random number generators is used to prove PUF randomness. Tab. 2 gives the detailed test results, from which we conclude that our proposed PUF passes the randomness test and acquires good randomness. In addition, this resource overhead used in the PUF implementation in this paper is analyzed. The counters used to implement 128 PUFs take up 4 096 LUTs, accounting for 2.7% of the total resources and the flip flops used 3 840, accounting for 2.5% of the total resources. The logic gates for 128 pairs of ROs occupy 1 536 LUTs, accounting for 1% of

Tab. 2 Measured NIST test suite results of ten chips under normal conditions (20 ℃, 1 V)

Parameters	P value
Frequency	0.574 000
FFT	0.561 658
Linear complexity	0.320 837
Runs	0.574 000
Block frequency	0.574 000
Cumulativ sum(1)	0.334 146
Cumulativ sum(2)	0.574 000
Longest runs	0.106 882
Approximate entropy	0.999 878
Non overlapping template	Pass
Universal	Pass
Random excursions	Pass
Random excursions variant	Pass

the total resources. In short, the hardware resources used in this paper are relatively small compared to other methods.

3.4 Quality improvement analysis

To validate the positive effect of surrounding logic on the circuit delay, a certification experiment was carried out. As the impact of temperature on PUF is very small relative to voltage[14], we focus on the voltage change on PUF in this paper, and then try to find the environmental changes. For example, the voltage increasing from 0.85 to 1.2 V causes a higher level of noise in FPGA's PUF response. Fig. 8 shows the total unstable bits of 128 RO-PUF responses under different supply voltages. The golden PUF line represents the unreliable bits of the original 128 RO-PUF responses without added surrounding logic. Case 1 and Case 2 in Fig. 8 represent the unreliable bits of the 128 RO-PUF responses which are added to by a simple and complex surrounding logic, respectively. Apparently, the number of unreliable PUFs is significantly reduced. This indicates that the PUF reliability has been greatly improved, so it has a higher robustness against a change in the external environment. This can be explained as follows: The temperature or voltage variation produced by the surrounding circuit activity results in changes in the electrical parameters, and also affects the speed of digital signals. As a consequence, the entire power supply voltage of PUFs is affected by the surrounding logic activity.

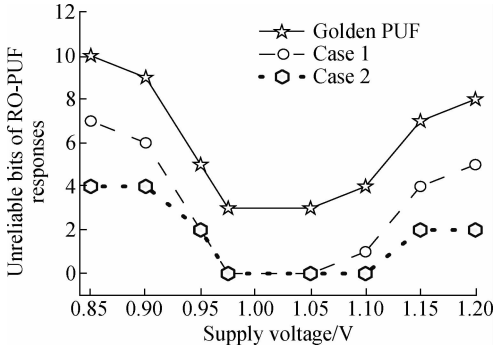

Fig. 8 Effect of voltage on RO-PUF

The characterization metrics comparison for related works of PUFs is shown in Tab. 3. In our work, in order to test the PUF randomness, 128-bit PUF-bit-streams are implemented in ten Xilinx Virtex-6 FPGAs. The temperature and voltage variations caused by the surrounding circuit activity result in changes in the power supply voltage of PUFs. By taking full advantage of surrounding logic circuit, the uniqueness and reliability reached 49.78% and 98.00%, respectively, under different temperatures (0 to 120 ℃) and voltages (0.85 to 1.2 V). Although the reliability of PUF in Ref. [9] is 0.45% higher than our results (see Tab. 3), our earlier research shows that the influence of voltage on circuit delay is much greater that of temperature[14]. Therefore, based on the voltage changes of ±2% from 1.2 V nominal supply reported in Ref. [9], we increased its voltage changes by more than 13%, which improved the reproduction ability of the PUF against environmental variations.

Tab. 3 Comparison of the characterization metrics of PUFs

PUF	Ref. [6]	Ref. [9]	Ref. [13]	This work
Uniqueness/%	64.70	47.78	50.42	49.78
Reliability/%	96.96	98.45	97.22	98.00
Randomness	NA	NA	NA	Pass
PUF ID size/bits	128	128	50	128
Conditions	0.9 to 1.2 V	0 to 85 ℃	±2% V_{dd} −40 to 120 ℃	±15% V_{dd} 0 to 120 ℃

Since surrounding logic activity has a significant effect on the delay of the circuit, in order to improve PUF reliability, the bit flipping rate of the PUF response is reduced. This is achieved by identifying and discarding the unsuitable slices which makes PUF output unstable. Experimental results show that PUF reliability is increased from 94% to 98%, leading to robustness improvement against environmental variations.

4 Conclusion

PUF reliability is seriously unstable as the fluctuations of environmental factors can make it difficult to reproduce identical output. In order to improve PUF reliability, we propose an effective stability test scheme, through which reliable slices and unreliable slices are distinguished. After that, by mapping PUF cells to reliable slices, PUF reliability can be effectively improved. The ring oscillator with multiple complexity and multiple frequencies can identify different unstable slices. The higher the complexity, the more unstable slices are detected. The proposed design has a lower hardware complexity than previous designs. Experimental results show that the proposed PUF has better PUF properties in terms of uniqueness and robustness. Moreover, it is shown that the proposed design is also robust with respect to process, voltage, and temperature variations.

References

[1] Gassend B, Clarke D, van Dijk M, et al. Silicon physical random functions[C]// *Proceedings of the 9th ACM Conference on Computer and Communications Security*. Washington, DC, USA, 2002: 148-160. DOI: 10.1145/586131.586132.

[2] Suh G E, Devadas S. Physical unclonable functions for device authentication and secret key generation[C]//2007 44*th ACM/IEEE Design Automation Conference*. San Diego, CA, USA, 2007: 9−14. DOI: 10.1109/dac.2007.375043.

[3] Herder C, Yu M D, Koushanfar F, et al. Physical unclonable functions and applications: A tutorial[J]. *Proceedings of the IEEE*, 2014, **102**(8): 1126−1141. DOI:

10.1109/jproc.2014.2320516.
[4] Delvaux J, Gu D, Schellekens D, et al. Helper data algorithms for PUF-based key generation: Overview and analysis[J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2015, **34**(6): 889 - 902.
[5] Zhang J L, Lin Y P, Lyu Y Q, et al. A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing[J]. *IEEE Transactions on Information Forensics and Security*, 2017, **10**(6): 1137 - 1150.
[6] Su Y, Holleman J, Otis B. A 1.6 pJ/bit 96% stable chip-ID generating circuit using process variations [C]// *IEEE International Solid-State Circuits Conference*. San Francisco, CA, USA, 2007: 406 - 407. DOI: 10.1109/isscc.2007.373466.
[7] Khan S, Hamdioui S, Kukner H, et al. Incorporating parameter variations in BTI impact on nano-scale logical gates analysis [C]//*IEEE International Symposium on Defect and Fault Tolerance VLSI and Nanotechnology Systems*. Austin, Texas, USA, 2012: 158 - 163. DOI: 10.1109/dft.2012.6378217.
[8] Kastensmidt F L, Tonfat J, Both T, et al. Voltage scaling and aging effects on soft error rate in SRAM-based FPGAs[J]. *Microelectronics Reliability*, 2014, **54**(9): 2344 - 2348. DOI: 10.1016/j.microrel.2014.07.100.
[9] Freijedo J F, Semião J, Rodriguez-Andina J J, et al. Modeling the effect of process, power-supply voltage and temperature variations on the timing response of nanometer digital circuits[J]. *Journal of Electronic Testing*, 2012, **28**(4): 421 - 434. DOI: 10.1007/s10836-012-5297-0.
[10] Stanciu A, Cirstea M N, Moldoveanu F D. Analysis and evaluation of PUF-based SoC designs for security applications[J]. *IEEE Transactions on Industrial Electronics*, 2016, **63**(9): 5699 - 5708. DOI: 10.1109/tie.2016.2570720.
[11] Tao S, Dubrova E. Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm CMOS[J]. *Electronics Letters*, 2016, **52**(10): 805 - 806. DOI: 10.1049/el.2016.0292.
[12] Maiti A, Schaumont P. Improving the quality of a physical unclonable function using configurable ring oscillators [C]//*International Conference on Field Programmable Logic and Applications*. Prague, Czech Republic, 2009: 703 - 707. DOI: 10.1109/fpl.2009.5272361.
[13] Cao Y, Zhang L, Chang C-H, et al. A low-power hybrid RO PUF with improved thermal stability for lightweight applications [J]. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2015, **34**(7): 1143 - 1147.
[14] Liang H G, Xu X M, Huang Z F, et al. A methodology for characterization of SET propagation in SRAM-based FPGAs[J]. *IEEE Transactions on Nuclear Science*, 2016, **63**(6): 2985 - 2992. DOI: 10.1109/tns.2016.2620165.

基于 FPGA 的提高 PUF 可靠性方法

梁华国　李伟迪　徐秀敏　王浩宇

(合肥工业大学电子科学与应用物理学院, 合肥 230000)

摘要:传统的基于环形振荡器的物理不可克隆函数(RO-PUF)因电压、温度、器件老化等影响,存在输出不可靠问题,即 PUF 输出随时变化,为了提高 PUF 的可靠性,提出一种针对 PUF 映射单元的稳定性测试方案. 该方案选择多复杂度和多种频率的环形振荡器作为干扰源,放置在 PUF 原型电路附近对其进行干扰. 通过识别和筛选掉不稳定的片,即识别和筛选掉使 PUF 结果不稳定的单元,来有效提高 PUF 的可靠性. 实验结果表明,不同复杂度和不同频率的周围逻辑电路可以识别出不同数量的不稳定片,复杂度越高,识别出的不稳定片也越多. 与最新发表的 PUF 文献相比,该 PUF 电路具有很好的统计随机性,资源消耗低. 在温度变化为 0 ~ 120 ℃和电压波动为 0.85 ~ 1.2 V 时,唯一性和可靠性分别达到 49.78% 和 98.00%,从而使其能够更好地被应用于安全领域.

关键词:现场可编程门阵列;物理不可克隆函数;安全;环形振荡器;可靠性

中图分类号:TN918.91