ELectronics EXpress

LETTER

IEICE Electronics Express, Vol.15, No.5, 1–8

A low-overhead RO PUF design for Xilinx FPGAs

Songwei Pei[1,2a)], **Jingdong Zhang**[2], **and Ruonan Wang**[2]

[1] *School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[2] *College of Information and Technology, Beijing University of Chemical Technology, Beijing 100029, China*

a) *peisongwei@163.com*

Abstract: Ring Oscillator (RO) Physical Unclonable Function (PUF) can effectively generate unique chip responses to support a variety of security-related applications. However, RO PUF typically incurs high hardware overhead when implemented in FPGA. In this paper, we designed a low-overhead RO PUF for Xilinx FPGAs, by which, on average, one-bit reliable PUF response can be generated by using only a single CLB (Configurable Logic Block). In the designed RO PUF, two different ROs can be configured in a single CLB at the same time based on the RO construction unit designed in the LUT (Look-Up Table). The designed RO PUF is implemented and verified by Xilinx Spartan 6 FPGA. Experimental results show that the implemented RO PUF has low hardware overhead and satisfactory quality.

Keywords: physical unclonable function (PUF), ring oscillator (RO), field-programmable gate array (FPGA)

Classification: Integrated circuits

References

[1] C. Herder, *et al.*: "Physical unclonable functions and applications: A tutorial," Proc. IEEE **102** (2014) 1126 (DOI: 10.1109/JPROC.2014.2320516).

[2] C.-H. Chang, *et al.*: "A retrospective and a look forward: Fifteen years of physical unclonable function advancement," IEEE Circuits Syst. Mag. **17** (2017) 32 (DOI: 10.1109/MCAS.2017.2713305).

[3] A. Maiti and P. Schaumont: "Improved ring oscillator PUF: An FPGA-friendly secure primitive," J. Cryptol. **24** (2011) 375 (DOI: 10.1007/s00145-010-9088-4).

[4] Y. Yu, *et al.*: "Improving RO PUF design using frequency distribution characteristics," IEICE Electron. Express **12** (2015) 20141043 (DOI: 10.1587/elex.12.20141043).

[5] B. Gassend, *et al.*: "Silicon physical random functions," Proc. ACM CCS (2002) 148 (DOI: 10.1145/586131.586132).

[6] S. V. Sandeep Avvaru, *et al.*: "Estimating delay differences of arbiter PUFs using silicon data," Proc. ACM/IEEE DATE (2016) 543 (DOI: 10.3850/9783981537079_0926).

[7] N. Tumuganti, *et al.*: "Novel TCAM-based PUF with improved reliability for hardware-entangled security," IEICE Electron. Express **14** (2017) 20170716 (DOI: 10.1587/elex.14.20170716).

[8] X. Xu, *et al.*: "A highly reliable butterfly PUF in SRAM-based FPGAs," IEICE

DOI: 10.1587/elex.15.20180093
Received January 30, 2018
Accepted February 8, 2018
Publicized February 22, 2018
Copyedited March 10, 2018

Electron. Express **14** (2017) 20170551 (DOI: 10.1587/elex.14.20170551).
[9] X. Xin, *et al.*: "A configurable ring-oscillator based PUF for Xilinx FPGAs," Proc. IEEE DSD (2011) 703 (DOI: 10.1109/dsd.2011.88).
[10] G. E. Suh and S. Devadas: "Physical unclonable functions for device authentication and secret key generation," Proc. ACM/IEEE DAC (2007) 9 (DOI: 10.1109/dac.2007.375043).
[11] A. Maiti and P. Schaumont: "Improving the quality of a physical unclonable function using configurable ring oscillators," Proc. IEEE FPL (2009) 703 (DOI: 10.1109/fpl.2009.5272361).
[12] J. Zhang: "Research and design of FPGA-based low overhead RO PUF," Master Dissertation, Beijing University of Chemical Technology, Beijing (2017).
[13] M. Gao, *et al.*: "A highly flexible ring oscillator PUF," Proc. ACM/IEEE DAC (2014) 9 (DOI: 10.1145/2593069.2593072).
[14] J. Zhang, *et al.*: "Design and implementation of a delay-based PUF for FPGA IP Protection," Proc. IEEE CADGraphics (2013) 107 (DOI: 10.1109/CADGraphics.2013.22).
[15] J. Zhang, *et al.*: "A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing," IEEE Trans. Inf. Forensics Security **10** (2015) 1137 (DOI: 10.1109/TIFS.2015.2400413).

1 Introduction

Silicon Physical Unclonable Function (PUF) is an innovative technology to generate non-volatile chip-unique response by taking advantage of manufacturing process variations. The PUF can be applied in many security-related fields, such as secure key generation, trustworthy computing, and device authentication etc. [1, 2]. A variety of PUF types have already been designed, such as RO PUFs [3, 4], arbiter PUFs [5, 6], and memory-based PUFs [7, 8]. The RO PUF can generate chip-unique response by comparing frequency between a pair of ROs designed identically. Fig. 1 shows a simple one-bit RO PUF design with two identically laid-out ROs [2].

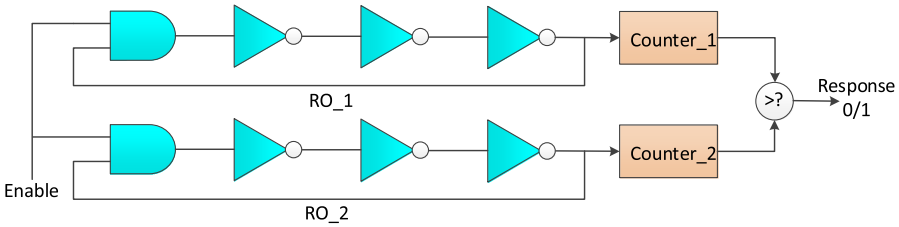

Fig. 1. The simple structure of RO PUF.

Due to process variations, the two ROs will have slightly different frequencies. By simultaneously starting and stopping the ROs, the values of the two counters will be different and can be compared to produce one-bit PUF response, for instance, a bit '0' is generated if counter_1 is larger than counter_2 and a bit '1' is generated otherwise. RO PUF typically contains multiple ROs, among which two ROs can be paired by user-specified challenges for frequency comparison and

DOI: 10.1587/elex.15.20180093
Received January 30, 2018
Accepted February 8, 2018
Publicized February 22, 2018
Copyedited March 10, 2018

generate one-bit response. The challenge-response pairs (CRPs) can be stored in a secure database to support security-related applications [3]. The important advantage of RO PUF is that it only requires to ensure all ROs are identical rather than the entire design is symmetric. Note that ROs can be easily implemented identically by using hard-macro techniques [3, 9]. Hence, RO PUF research has attracted great attentions for FPGA security-related applications.

In the traditional RO PUF [3, 10], given N ROs, $N(N-1)/2$ distinct RO pairs can be found to generate responses. By this way, however, many response bits would be correlated. Even though each RO is only used once to avoid correlation, these response bits are still not reliable due to the fluctuation of working environment. The 1-out-of-8 RO PUF scheme [10] can improve the reliability of PUF response significantly. In this work, the fastest and slowest ROs are selected from every 8 ROs to generate one more reliable response bit. Hence, $8N$ ROs are required to generate N response bits. This scheme sacrifices high hardware overhead to achieve better reliability. In [11], a configurable RO is designed with the same area as the basic RO in [10], which can be configured to 8 different ROs with slightly different frequencies. For a pair of configurable ROs, from the configuration possibilities, the two configurable ROs can be configured to ROs with maximum frequency difference. Hence, the configurable RO PUF can still achieve better reliability but bring significant hardware overhead reduction. In [9], the flip-flops in the slices are configured as transparent latches. By utilizing latches as additional delay units, the configurable RO in [11] is further extended to include more configuration possibilities. The extended configurable RO PUF can generate more output bits. Likewise, this RO PUF also has the ability to keep better reliability. Both in [9] and [11], one configurable RO is designed with a single CLB. Hence, by defining the configurable RO as a hard macro, different duplicates of configurable RO can easily remain identical. The frequency difference between a pair of ROs will relies solely on the manufacturing process variations.

As mentioned above, the configurable RO PUFs have many advantages, such as high quality, low overhead, and easy implementation. However, the hardware overhead for the configurable RO PUFs is still considerable and can be further reduced [12]. In this work, a more low-overhead RO PUF for Xilinx FPGAs is designed and implemented. Two ROs with different frequencies can be configured in a single CLB at the same time based on the RO construction unit designed in the LUT (Look-Up Table). In the designed RO PUF, two bit PUF responses can be generated by comparing two pair of ROs designed in two CLBs, which means that, on average, one-bit reliable PUF response only requires a single CLB. As a result, the designed RO PUF has a reduced hardware overhead. Likewise, the designed RO PUF is also based on configurable ROs. Hence, a satisfactory quality can also be achieved by the implemented RO PUF.

2 The proposed low-overhead RO PUF design

2.1 The design of OR construction unit in a LUT

Fig. 2(a) shows the basic 6-input LUT structure, which is very popular in Xilinx FPGAs. As shown in Fig. 2(a), the 6-input LUT structure, denoted with LUT6, is

DOI: 10.1587/elex.15.20180093
Received January 30, 2018
Accepted February 8, 2018
Publicized February 22, 2018
Copyedited March 10, 2018

composed of two LUT5s that have 5 inputs and 1 output respectively. The inputs of the two LUT5s are shared. The input A6 of the LUT6 plays the role of choosing one of the two outputs of LUT5s to the output 1 of LUT6.

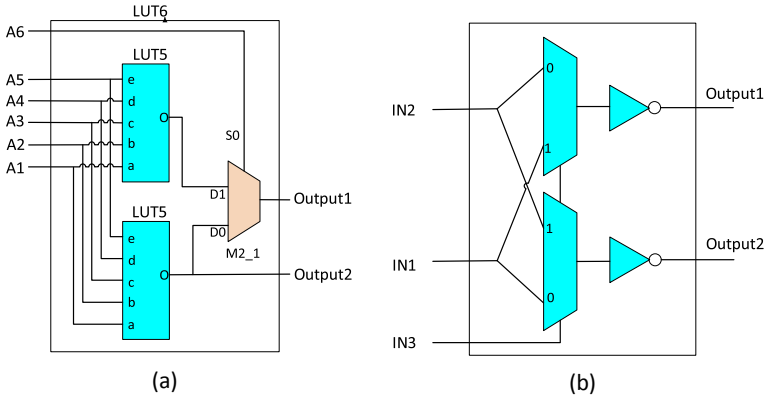

Fig. 2. The basic component of RO PUF, (a) LUT structure; (b) OR construction unit

Based on the important characteristic of the LUT6 structure, in this work, we designed an OR construction unit in LUT6 by fully utilizing the resources of the two LUT5 and the two outputs. The logic functionality of the OR construction unit is shown in Fig. 2(b), which includes two inverters and two MUXs. Considering the structure of LUT6, the configuration value of the LUT6 can be set to "0x0000_0053_0000_0035" to realize the functionality of the OR construction unit. The OR construction unit will be used to construct the RO PUF with high hardware utilization and will be presented in the next sub-sections in detail.

2.2 The configuration of ROs in a CLB

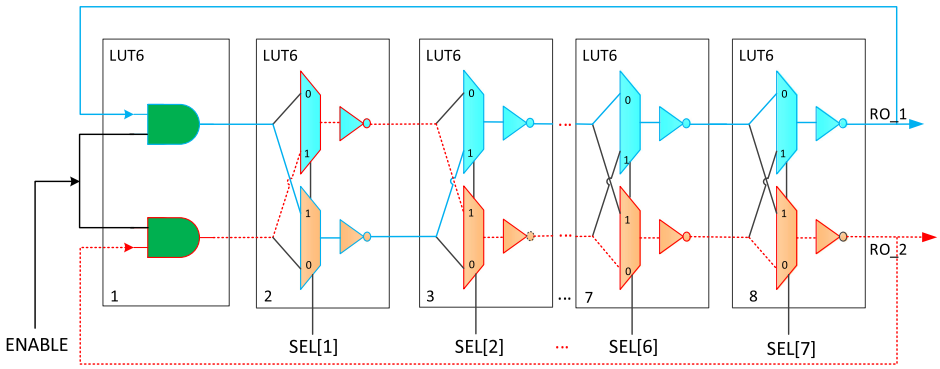

Fig. 3. The structure for configuring different ROs in a CLB

In many Xilinx FPGAs, such as Xilinx Spartan 6 serie, one CLB consists of 8 LUTs. To further enhance the hardware utilization and ensure the identical of ROs, as shown in Fig. 3, we designed a configurable RO structure that can be configured to two ROs with different frequencies at the same time in a single CLB based on the OR construction unit mentioned above. The SEL[i]s ($1 \leqslant i \leqslant 7$) are used to select specific inverters and MUXs to configure ROs with different frequencies. In the

DOI: 10.1587/elex.15.20180093
Received January 30, 2018
Accepted February 8, 2018
Publicized February 22, 2018
Copyedited March 10, 2018

configurable RO structure, the first LUT6 is configured to two AND gates to start the oscillations. The configurable RO provides the premise to construct a low-overhead RO PUF, which will be presented in the next sub-section in detail. It is worthy of note that the number of logic-1s for SEL[i]s should be even to ensure that the two configured ROs can oscillate correctly, which is similar to the requirement of the flexible RO PUF in [13].

To illustrate the functionality of the configurable RO, without loss of generality, we set "1100000" corresponding to the values of SEL [1] to SEL [7] as an example to realize two different ROs in a single CLB at the same time. As shown in Fig. 3, based on the values of SEL [1] to SEL [7], two different ROs, indicated by red and blue routes, are constructed symmetrically.

2.3 The design of low-overhead RO PUF

To facilitate graphic illustration, Fig. 4 shows the RO PUF designed only in 2 CLBs to generate 2 response bits. Clearly, the designed RO PUF can be easily extended for generating more response bits by adding more configurable ROs. And the counters can also be shared by feeding different ROs with MUXs [3].

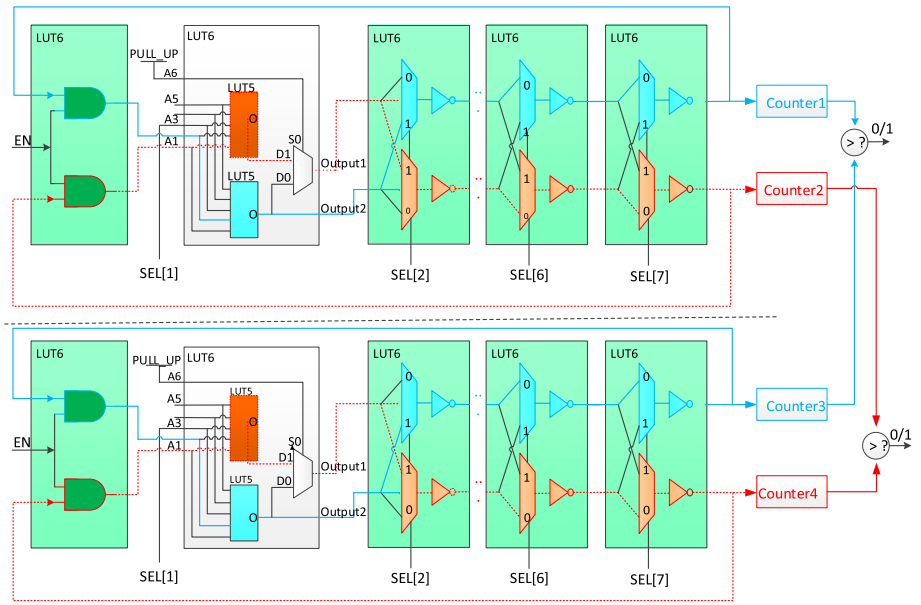

Fig. 4. The design of low-overhead RO PUF

It is worthy of note that the ROs located in the same site of different CLBs can be paired to generate response bits with satisfactory symmetric. Clearly, by configuring the pair of ROs with large frequency difference from the configuration possibilities, one reliable response bit can be generated by comparing the values of counter 1 and counter 3 after oscillation, and likewise for counter 2 and counter 4. Clearly, as presented above, on average, a pair of ROs can be configured in a single CLB to generate one reliable response bit. As a result, the designed RO PUF can bring significant hardware overhead reduction. Moreover, similar to the technique in [11], based on configurable ROs, the designed RO PUF can also have a satisfactory quality.

DOI: 10.1587/elex.15.20180093
Received January 30, 2018
Accepted February 8, 2018
Publicized February 22, 2018
Copyedited March 10, 2018

3 Experimental results and analysis

3.1 Experimental setup

To verify the effectiveness, we implemented the proposed RO PUF with 62-bit reliable response on a Xilinx Spartan 6 FPGA development board. Similar to the verification method in [14, 15], in this work, the FPGA is divided into 16 regions, in each of which a 62-bit proposed RO PUF is implemented. Fig. 5 shows the layout of the 16 62-bit PUFs, in which the PUF is specified into a designated region by the range constraint supported by Xilinx.

Fig. 5. The layout of 16 62-bit RO PUFs on FPGA

In the experiments, serial communication is implemented between FPGA development board and PC, by which the FPGA can receive the challenges from PC and send the responses generated by the 16 62-bit RO PUFs to PC for quality analysis. In the work, the popular quality factors including uniqueness and reliability are verified for the proposed RO PUF through analyzing the responses of the implemented 16 62-bit RO PUFs. In the following sub-section, we will firstly analyze the quality factor of the designed RO PUF, and then evaluate its hardware overhead.

3.2 Experimental results of the designed RO PUF

1) Uniqueness: Uniqueness is an important quality factor of PUF, which reflects how uniquely the response could be generated by a PUF. In general, the uniqueness of a PUF can be evaluated by the following formula [3, 14]:

$$u = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(P_i, P_j)}{n} \times 100\% \tag{1}$$

where P_i and P_j $(i! = j)$ represent a pair of n-bit PUF responses generated by two different PUFs with a challenge; $HD(P_i, P_j)$ represents the Hamming distance between *Pi and Pj*; k represents the number of n-bit PUF responses. In this experiment, the uniqueness of the proposed RO PUF is evaluated by the formula (1) with the parameters set to $k = 16$, $n = 62$.

Fig. 6 shows the frequency distribution of Hamming distance considering the 16 62-bit PUF responses with a challenge. Ideally, the uniqueness value, namely u, is expected to 50% if the Hamming distance between any two of the 16 62-bit response equals to the theoretical expectation value, 31 bits. As shown in Fig. 6,

DOI: 10.1587/elex.15.20180093
Received January 30, 2018
Accepted February 8, 2018
Publicized February 22, 2018
Copyedited March 10, 2018

the majority of experimental Hamming distances approach to the theoretical expectation value. The maximum and the minimum of Hamming distances are 47 and 18 bits respectively. The experimental uniqueness value u calculated by formula (1) is 50.013% considering all the experimental Hamming distances. The experimental results show that the proposed RO PUF has a satisfactory uniqueness.

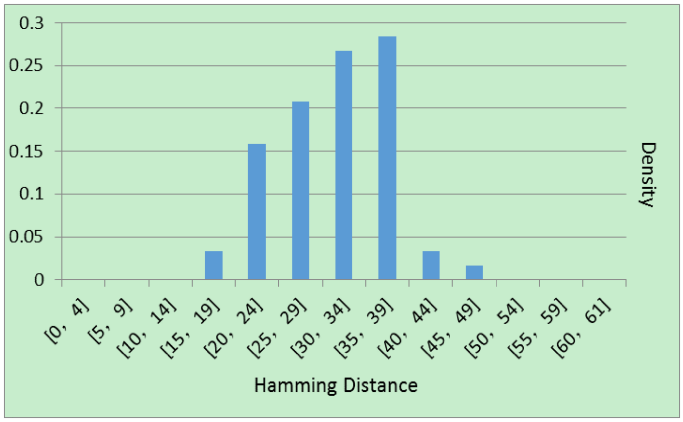

Fig. 6. Frequency distribution of Hamming distances considering the 16 62-bit PUF responses

2) Reliability: The response generated by a PUF with the same challenge in repeated operations are expected to be consistent. Reliability is the quality factor to reflect how consistently the response could be generated by a PUF under repeated operations with environment changes. The reliability of a PUF are usually evaluated by the following formula [3, 14]:

$$r = \frac{1}{x}\sum_{y=1}^{X}\frac{HD(R_i, R_{i,y})}{n} \times 100\% \tag{2}$$

where R_i represents a n-bit response; $R_{i,y}$ represents the y^{th} sampling of the response; x represents the number of sampling; $HD(R_i, R_{i,y})$ represents the Hamming distance between R_i *and* $R_{i,y}$. In the experiment, we recorded CRPs of 16 PUFs in the normal operational conditions firstly. Then we repeated the experiment after a few days with the environmental variations. Fig. 7. shows the frequency distribution of the Hamming distance of the 62-bit PUF responses between samplings. Ideally, the reliability value, namely r, is expected to 0 if the PUF responses keep stable with the same challenge in repeated experiments.

As shown in Fig. 7, the Hamming distances between PUF responses in multiple experiments are very small. The minimum and the maximum hamming distances are only 0 and 4 respectively. The experimental reliability value r calculated by formula (2) is only 1.125, which shows that the designed RO PUF kept a high PUF response reliability.

3) Hardware overhead: LUT is the basic building block of FPGA architecture. In this work, 16 implemented 62-bit RO PUFs consume only 4096 LUTs. The hardware overhead of the designed RO PUF is also compared with the RO PUFs in [3, 9, 10, 11] in terms of the number of LUTs per one-bit reliable PUF response. Consider a CLB consists of 8 LUTs. The comparisons are shown in Table I.

DOI: 10.1587/elex.15.20180093
Received January 30, 2018
Accepted February 8, 2018
Publicized February 22, 2018
Copyedited March 10, 2018

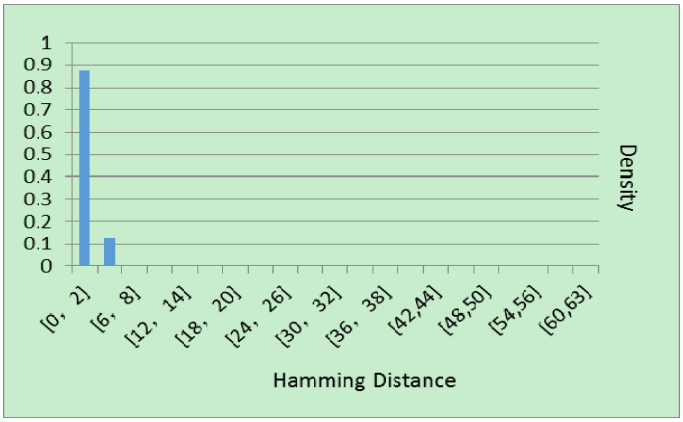

Fig. 7. Frequency distribution of Hamming distances between samplings

Table I. Comparisons of hardware overhead

Hardware Overhead	1-out-of-8 RO[10]	Traditional RO[3]	Xin's RO[9]	Maiti's RO[11]	Proposed RO
LUTs	64	16	16	16	8
Flip-flops	0	0	8	0	0

For the 1-out-of-8 RO PUF in [10], 8 ROs designed with 8 CLBs are required to generate one-bit reliable PUF response. For the RO PUF in [3, 9, 11], 2 ROs designed in 2 different CLBs are required to generate one-bit reliable PUF response. Moreover, 8 extra flip-flops are required in the RO structure in [9]. As discussed in Section 2, in the proposed RO PUF, 2-bit reliable PUF responses can be generated with 2 CLBs. Hence, in the work, the hardware overhead per one-bit reliable PUF response is only 8 LUTs. The major reason of the low hardware overhead of designed RO PUF is that two different ROs can be configured in a single CLB.

4 Conclusion

In this paper, we designed a low-overhead RO PUF for Xilinx FPGAs by taking advantage of the CLB resources. The RO construction unit is designed in a single LUT. On average, the hardware overhead per one-bit reliable PUF response is only 8 LUTs. As a result, the designed RO PUF has very low hardware overhead. Experimental results on Xilinx Spartan 6 FPGA also demonstrate that the designed RO PUF has satisfactory uniqueness and reliability.

Acknowledgments

This work was supported in part by National Natural Science Foundation of China (NSFC) under grant No. (61770261, 61402031).

DOI: 10.1587/elex.15.20180093
Received January 30, 2018
Accepted February 8, 2018
Publicized February 22, 2018
Copyedited March 10, 2018