An Efficient Framework for Configurable RO PUF

Zhuwei Chen*, Yici Cai*, Qiang Zhou*, Gang Qu†
Tsinghua National Laboratory for Information Science and Technology
*Department of Computer Science and Technology, Tsinghua University
†University of Maryland
czwcarelife@gmail.com, {caiyc,zhouqiang}@tsinghua.edu.cn, gangqu@umd.edu

***Abstract*—Physical Unclonable Function (PUF) is one of the most efficient technique to generate unique and random identification for chip authentication. Ring oscillator (RO) PUF takes advantage of delay variations of a pair of ROs, which is easy to implement on FPGAs. An important consideration for FPGA based RO PUF is how to eliminate systematic variation without reducing the number of output bits. To address this problem, we introduce a high performance RO organization and comparison framework. Moreover, an enhanced configurable RO, which has up to 512 different configurations but only occupies one FPGA slice, is proposed to improve the reliability and output bits number. Experimental results demonstrate that our PUF achieves best value on bit-aliasing rate (50.37%) compared with other existing configurable RO PUFs. The output bits number also increases by the factors of 2.1-9.2.**

I. Introduction

With the dramatically development of electronic devices in communication and computation areas, a unique identification (ID) string is necessary to authenticate a specific device. Traditional methods like saving a unique number into a persistent storage on chip are easily to be attacked or cloned. Physical Unclonable Function (PUF) is proposed to solve this problem. It generates unique and random identifications by using chip's fabrication variation.

Ring Oscillator (RO) PUF was first introduced in 2007 by Suh and Devadas [1], which is one of the most effective PUF. It generates response bits through the different delays between two identically designed ring oscillators. RO PUF has advantages of easy implementation on FPGA and high security against side-channel attack, but it's sensitive to environmental noise and systematic variation. Environmental noise such as temperature variation or voltage variation may make the PUF unreliable, while systematic variation is an unwanted correlated frequency variation due to spatial location on FPGA boards, which may lead to identical responses at particular bit position among different chips.

Several architectures and techniques have been put forward to improve the performance of PO PUF so far. For instance, the 1-out-of-8 scheme mentioned in [1] improved the reliability significantly. The group-based RO PUF [2], [3] achieved more response bits at the expense of high implementation difficulty on chips. [4] first introduced the systematic variation problem and used an indicator value called "bit-aliasing rate" to evaluate the performance of a PUF against systematic variation. [5] proposed a structure that using a placement constraint on the ROs to align them closely in a 2D array. Only physically adjacent ROs were chosen to extract output bits. This structure has been widely used in the later works due to its easy implementation. However, the bit extraction rate per ring of the structure is lower than 1.0, which means a great waste on hardware resources. [6] further improved the bit-aliasing rate by comparing 4 rings simultaneously. The improvement was achieved at the cost of even less output bits per ring. On the other hand, Maiti and Schaumont introduced the conception of configurable RO PUF in [5]. They used two inverters at each stage of an RO and a multiplexer to select one out of two inverters. In 2011, [7] presented an enhanced implementation with 256 possible configurations for each RO but still used one CLB. [8] replaced one inverter into a single wire to extract more reliable bits. Habib [9] first applied LUT internal delays in configurable RO PUF with only half hardware cost compared with Maiti's. However, their PUF only provides 8 different configurations for each RO, which may miss some important frequency choices.

In this work, we analyze the distribution regularity of systematic variation and propose a high performance RO comparison and organization framework to eliminate the influence of systematic variation without reducing output bits number. An improved configurable RO based on LUT internal delays is also applied to further increase output bits number and ensure the reliability of our PUF. The contributions of our work can be summarized as follows:

1) A new RO array framework including two techniques is introduced. The reusable organization technique provides an RO comparison constraint as well as a reuse method by grouping every 6 adjacent ROs into a "comparison unit". While the double comparison technique changes traditional comparison objects from ROs to "RO Pairs". This framework greatly eliminates the influence of systematic variation and provides 1.5X bits more than the method in [5] and [9].
2) An improved configurable ring oscillator based on [9] is proposed. The number of different configurations increases from 8 in [9] to 512, while the hardware cost remains unchanged. Coupled with a pre-filtering technique, our RO enhances both reliability and output bits.

The rest of this paper is organized as follows. Section II presents the implementation details of our PUF. Section III shows the experimental results and a conclusion is reached in section IV.

II. Architecture and Implementation Details

A. Overall Architecture

Figure 1 illustrates the architecture of our PUF. It contains a 10×10 RO array and a controller model. Different from other PUFs, we do not compare the frequencies between two ROs but between two RO pairs. An **RO pair**(also called **ROP**) is the combination of two ROs in a unit according to a certain pattern, while a **unit** is a group of six adjacent ROs. Detail introduction for the RO array can be found in section B.

The address generator provides different selections for RO pairs through two selection decoders, which are named

This work was supported by Natural Science Foundation of China (NSFC) No.61274031.

978-1-4799-5341-7/16/$31.00 ©2016 IEEE

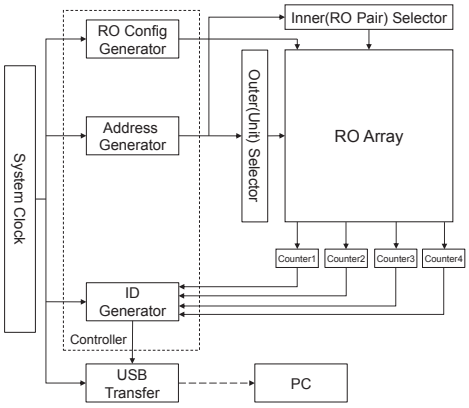

Fig. 1. Architecture of configurable RO PUF

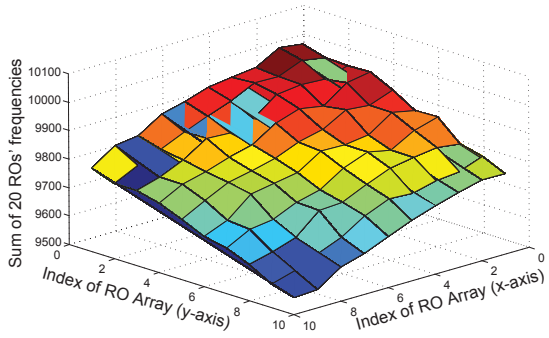

Fig. 2. Distribution of the summary of 20 boards' frequencies on 100 bit position

as "Outer Selector" and "Inner Selector". The outer selector decides which comparison unit to use, while the inner selector determines the indexes of two RO pairs in a certain unit and makes a comparison. The RO configuration generator responds to configure delays of ROs in one comparison stage through configuration lines. Finally, an ID generator is applied to compare the output frequencies and extract response bits. All of these modules are controlled by a finite state machine, driven by a 100MHz on-chip system clock. The state machine also serves to transfer the response bits to PC through USB transfer protocol.

B. Technique of RO Array Framework

[4] indicated that variation of supply voltage in different chip regions is the main factor of systematic variation. In fact, RO frequencies and the distance between ROs and BRAMs (which cost much energy) can be described as a monotonic decreasing function in a statistical sense, as is shown in figure 2. X-axis and y-axis are the indexes of ROs in the array. The larger the index is, the closer of the RO is to the BRAM. Z-axis represents the sum of 20 ROs' frequencies on each ID position. Detail experiment illustrates that the function is an elliptical equation.

Based on this special spatial-frequency distribution, we introduce an improved framework shown in figure 3 to eliminate influence of systematic variation. First of all, the RO array is located beside the BRAMs, hence the frequencies of ROs decrease from bottom left to up right. Then, every 6 adjacent ROs are grouped as a "comparison unit". Each RO can be reallocated to up to 6 units. It divides our 10×10 RO array into $9 \times 8 = 72$ units. For convenience, we number the six ROs

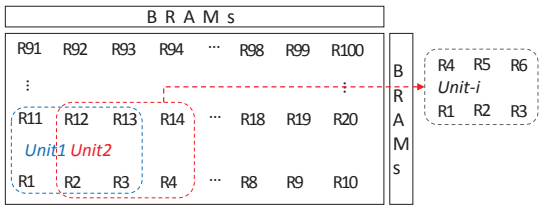

Fig. 3. Improved RO array organization structure

TABLE I. EXAMPLE FOR COMPARISON PAIR CHOOSING(MHZ)

RO No.	RO_1	RO_2	RO_3	RO_4	RO_5	RO_6
$freq$	495.5	495.8	496.5	498.2	497.5	503.2
RO No.	$P_1(f_1+f_6)$		$P_2(f_2+f_5)$		$P_3(f_3+f_4)$	
$freq$	998.6		993.3		994.7	
Comp Result	$D_1(P_1,P_2)$		$D_2(P_1,P_3)$		$D_3(P_2,P_3)$	
$\Delta freq$	5.34		3.93		-1.41	

TABLE II. COMPARISON OF EVERY 4, 6, 8 ROS IN ONE UNIT.

Number of ROs per unit	4	6	8
Number of output bits	99	144	189
Average number of influenced units	12	17	23
PUF uniqueness	50.29	50.37	51.21

in a unit from 1 to 6. While generating a bit, RO_1 and RO_6 are combined together as a **ring oscillator pair (ROP)**. The frequency of this ROP is the sum of f_{RO_1} and f_{RO_6}. Situations are similar for $\{RO_2,\ RO_5\}$ and $\{RO_3,\ RO_4\}$. Finally, the comparison is made between 2 ROPs, if the former ROP has larger frequency than the latter, it generates 1, otherwise 0.

$$\begin{cases} f_{ROP_1} = f_{RO_1} + f_{RO_6} \\ f_{ROP_2} = f_{RO_2} + f_{RO_5} \\ f_{ROP_3} = f_{RO_3} + f_{RO_4} \end{cases}$$

This combination and comparison technique helps us to eliminate the subtraction part of the frequencies due to systematic variation, while fabrication variation is still retained.

According to the principle of entropy increase mentioned in [1], there are only two independent results for three ROPs. However, in order to improve the reliability, we still conduct all comparisons among three ROPs and take two results with largest absolute difference. For example, table 1 lists the frequencies of six ROs in one unit where P_i is the frequency of ROP_i. The comparison results D_1, D_2 is chosen and D_3 is discarded for D_1, D_2 are larger than D_3.

Now we discuss why we choose 6 ROs in one unit instead of 4 or 8 or even more. An important issue is that ROs only follow monotonic decreasing distribution in statistical sense. Quite a few ROs are irregular on particular FPGA boards for the practical supply voltage situation is complicated, which means there may exists such ROs that are close to BRAMs but have larger frequencies. We call this kind of ROs as "abnormal points". If a unit contains abnormal points, the systematic variation is probably magnified instead of being eliminated. It's obvious that reducing the number of ROs contained in one unit will reduce the possibility of failure caused by abnormal points (each abnormal point influences up to 6 units when we group 6 ROs in one unit and influences 8 units when grouping 8 ROs). However this operation also reduces the number of independent responses in a unit (three responses are produced in an 8-ROs unit while only two in a 6-ROs unit). Table 2 lists the output bits number and uniqueness results among grouping 4, 6, 8 ROs in one unit. The 6-ROs unit gives respectively

better results compared with the other two. Therefore, we choose 6 ROs in one unit.

After applying all of the techniques, our framework generates $8 \times 9 \times 2 = 144$ bits on a 10×10 RO array, which is 1.44X of traditional structure.

C. Configurable RO & Reliability Optimization

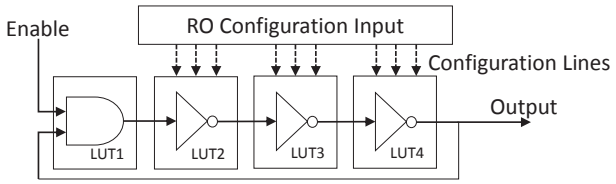

Fig. 4. Structure of our configurable RO

Figure 4 shows the structure of our configurable RO, every four 4-input LUTs constitute a ring oscillator. The first LUT is used as an AND gate, while the remaining three LUTs are inverters. Three configuration lines are connected to each inverter LUT with a selection input of 0 or 1 per line. In order to control the whole RO delay by these 9 lines, each configurable RO is implemented inside an FPGA slice to minimize the impact of wire delay. The configuration string is same for all of the candidate ROs in one comparison process for the independency of output bits.

There are 512 different RO frequencies through the configuration string in theory. However, not all values are meaningful. The first problem is that the value graphs of two ROPs don't always cross. If the frequency of one ROP is always higher than another in different configuration situations, only one meaningful bit can be generated by them. We use a method inspired from [9] to solve this problem. If two ROPs don't cross, we only record the first bit. Otherwise, 512 bits will be recorded. The result is pre-stored in the FPGA testing phase with such structure {Cell#, ROP#, isCross}.

Another problem is that some of the configurations are vulnerable to producing "bit-flips" since the frequencies are too close. Except for the method introduced in section II.B, we employ a threshold to avoid the problem at RO level. For each comparison, we only accept the output bit if the frequency difference between two ROPs is greater than the threshold. The value of threshold depends on the frequency fluctuation range in different environments. For instance, in our experiments, the maximum frequency difference range of two ROPs is around 0.5MHz and the threshold is set as 1MHz, which is twice of the environmental range.

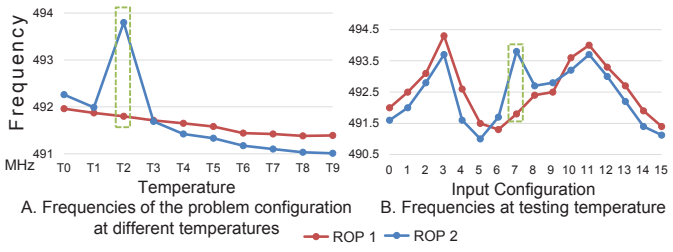

Fig. 5. Frequency jump case when testing whether a bit passes threshold condition

Furthermore, we detect a frequency jump phenomenon in different environment when testing our PUF. An example is showed in figure 5. Two poly lines represent the frequencies of ROP_1 and ROP_2. Figure 5a lists the frequencies of a problem bit at various temperatures in a particular configuration. A frequency jump occurs at temperature T2 of ROP_2. If we chanced to pre-test our PUF at this temperature (T2) as what figure 5b shows, the marked bit(covered by the green box) would pass the threshold condition. However, it would fail the condition at usage temperatures (T0, T1, T3, ..., T10), which leads to producing "bit-flips". This situation mainly occurs when the frequencies of two ROPs are close. Hence, we use a more strict filtering strategy at pre-testing stage. If there are more than three quarters of the bits of two ROPs fails the threshold condition in different configurations, we consider these two pairs are too similar to distinguish. All of the other bits are discarded. Note that this problem rarely happens, but we'll get a fully unsafe bit once it occurs.

III. Experimental Results

The experiments are conducted on 20 Xilinx Virtex-5 LX110T FPGA boards. 100 configurable ROs together with a control module are placed on each board to extract outputs. A script provided in [10] is run on PC to validate whether the generated bits are superior to others. There are altogether three tests are made:

1) Minimum number of output bits, which represents the efficiency of a PUF.
2) Intra-die Hamming distance (uniqueness, and bit-aliasing rate), which indicates whether the outputs are unique and random enough.
3) Inter-die Hamming distance in different environments, which indicates the reliability and stability of the outputs.

A. Number of Output Bits

The number of output bits per ring indicates whether a PUF is efficient on generating identification number. It also reveals hardware cost. Among all of the 20 chips in our experiments, the maximum length of the output bits generated by one chip is 617, while the minimum is 462. We use the minimum length as our final output chip ID length and ignore the excessive part. Table 3 shows the comparison with several existing RO PUFs. Due to our improved framework and large number of RO configurations, we have largest output bits number per ring, which is from 2.1X times to 9.2X times of other PUFs.

B. Uniqueness and Bit-aliasing rate

Uniqueness indicates whether a PUF can generate distinct outputs on different chips. The average percentage of intra-die Hamming Distance (HD) between every two PUF responses is an estimate of the uniqueness, with an ideal value of 50%. It is defined as follows

$$Uniqueness = \frac{2}{K(K-1)} \sum_{i=1}^{K-1} \sum_{j=i+1}^{K} \frac{HD(R_i, R_j)}{n} \times 100\%$$

where $HD(R_i, R_j)$ is the Hamming distance between two n-bit responses R_i, R_j from chip i and chip j. K is the total number of chips. The formula above should include all of the possible pair-wise Hamming Distances among these chips.

Bit-aliasing rate is responsible for checking the distribution of '0's and '1's at particular bit position in different response strings. As is indicated in section II.B, systematic variation leads to generating identical bits in same position on different chips. However, the intra-die Hamming Distance may neglect this problem. For instance, if the i-th bit in each n-bit response always output '1' across the chips, while the j-th bit always

TABLE III. COMPARISON OF THE NUMBER OF GENERATED BITS.

	RO No.	Strong responses	Bits per Ring
Traditional PUFs	128	64	0.5
1-out-of-8 PUFs	128	16	0.125
Maiti's[5]	128	127	1
Habib's[9]	130	283	2.17
Xin's[7]	128	255	1.99
Qu's[8]	128	64	0.5
Our	100	462	4.62

TABLE IV. DISTRIBUTION OF BIT-ALIASING PERCENTAGE FOR ALL 462 BITS

Percentage	10%-20%	20%-30%	30%-40%	40%-50%
Number of bits	1	17	83	130
Percentage	50%-60%	60%-70%	70%-80%	80%-90%
Number of bits	121	91	19	0

output '0', the uniqueness of the whole PUF is still 50%. However, the contribution of i-th bit and j-th bit is zero, which means the responses of the PUF are actually not distinct and random enough. Therefore, we use bit-aliasing rate to check whether the problem occurs. It is defined as

$$(Bit - aliasing)_j = \frac{1}{K}\sum_{i=1}^{K} R_{i,j} \times 100\%$$

where $R_{i,j}$ is the j-th binary bit in the i-th chip's n-bit string. Similar to uniqueness, we use an average bit-aliasing value of all the bits $(Bit - aliasing)_{average} = \frac{1}{N}\sum_{i=1}^{N}(Bit - aliasing_j)$. The closer of bit-aliasing is to 50%, the less likely of the problem will come out.

Table 4 lists the distribution of bit-aliasing percentages for all 462 bits. The average value is 50.37% while the maximum value is 76.9% and the minimum value is 17.4%. Furthermore, the percentages range in [30%, 70%] hold a strong majority compared with others, which means most of the bits are evenly distributed among '0' and '1'.

Table 5 gives the comparison results of uniqueness and bit-aliasing rate among several configurable RO PUFs. To make a fairer comparison, we implemented these PUFs on our boards. Our work performs better on bit-aliasing rate which only greater than the ideal value by 0.37% and smaller than others from 0.84% to 2.43%. Owing to this improvement, we also achieve a better value on the uniqueness.

C. Reliability against Environmental Variation

The delay of LUTs changes along with the outside environmental variations such as temperature and voltage, which results in the change of RO frequency. This difference is large enough to produce "bit-flips". Reliability is used to evaluate how reliable the PUF is against temperature and voltage variation. It is defined as

$$R = 100\% - \frac{1}{X}\sum_{x=1}^{X}\frac{HD(R_i, R'_{i,x})}{n} \times 100\%$$

where R_i is the response at room temperature and standard voltage, R'_i is the response when temperature or voltage changes. The ideal value of reliability is 100%.

We measure our PUF at varying temperatures and voltages. The range of temperatures is $\{25°C,\ 33°C,\ 38°C,\ 47°C,\ 55°C\}$, while the range of supply voltages is $\{0.98V,\ 1.08V,\ 1.20V,\ 1.32V,\ 1.44V\}$. At each environment condition, we test our PUF for 10 times. Figure 6 shows the average unreliable bit numbers of a single chip and single measurement. The reliability of our PUF reaches 100% in the normal environment ($25°C$,$1.20V$), while the worst value is 98.53% when the supply voltage is 1.44V. Detail comparison results with other PUFs can also be found in table 5.

TABLE V. COMPARISON WITH OTHER CONFIGURABLE RO PUFS(RELIA MEANS RELIABILITY)

	Uniqueness	Bit-aliasing	Best Relia	Worst Relia
Maiti's[5]	53.49	51.92	100	98.69
Habib's[9]	52.40	52.03	99.90	97.88
Xin's[7]	55.01	52.80	100	98.32
Qu's[8]	52.24	51.21	99.89	97.47
Our	51.54	50.37	100	98.53
ideal	50	50	100	100

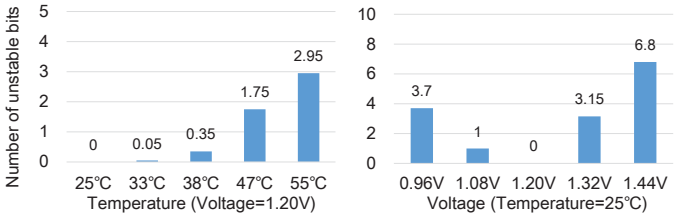

Fig. 6. Number of Unstable Bits

IV. CONCLUSIONS

In this paper, we propose a novel RO array structure including reusable organization technique and double comparison technique to solve systematic variation problem as well as increase the number of output bits. An improved configurable RO based on LUT internal delays is also introduced, which extends the number of configuration inputs from 8 to 512. Experimental results demonstrate that our PUF generates 4.6 bits per ring, which is much greater than others. Meanwhile, the bit-aliasing value and reliability are also improved. Further works will include finding a better way to optimize the aging problem of hardware.

REFERENCES

[1] S.Devadas G.E.Suh, "Physical unclonable functions for device authentication and secret key generation," *the 44th annual Design Automation Conference*, pp. 9–14, 2007.

[2] C.E.D. Yin and G. Qu, "Lisa: Maximizing ro pufs secret extraction," *Hardware-Oriented Security and Trust*, pp. 100–105, 2010.

[3] C.E.D. Yin and G. Qu, "Design and implementation of a group-based ro puf," *Design, Automation & Test in Europe Conference & Exhibition*, pp. 416–421, 2013.

[4] L. McHale P. Schaumont A. Maiti, J. Casarona, "A large scale characterization of ro-puf," *Hardware-Oriented Security and Trust*, pp. 94–99, 2010.

[5] Patrick Schaumont, Abhranil Maiti, "Improving the quality of a physical unclonable function using configurable ring oscillators," *FPLA*, pp. 703–707, 2009.

[6] P.H.W Qiang Xu Haile Yu, Leong, "An fpga chip identification generator using configurable ring oscillator," *Field-Programmable Technology*, pp. 312–315, 2010.

[7] K. Gaj X. Xin, J.-P. Kaps, "A configurable ring oscillator-based puf for xilinx fpgas," *Euromicro Conference on Digital System Design*, pp. 651–657, 2011.

[8] Gang Qu, Mingze Gao, Khai Lai, "A highly flexible ring oscillator puf," *Design Automation Conference*, pp. 1–6, 2014.

[9] Jens-Peter Kaps Bilal Habib, Kris Gaj, "Fpga puf based on programmable lut delays," *Euromicro Conference on Digital System Design*, pp. 697–704, 2013.

[10] http://rijndael.ece.vt.edu/puf/script_download.html.