ELectronics EXpress

LETTER

IEICE Electronics Express, Vol.12, No.3, 1–6

Improving RO PUF design using frequency distribution characteristics

Yifei Yu[1], **Chenghua Wang**[1], **Weiqiang Liu**[1a)], **Yijun Cui**[1], **and Máire O'Neill**[2]

[1] *The Key Laboratory of Radar Imaging and Microwave Photonics, Ministry of Education, Nanjing University of Aeronautics and Astronautics, Nanjing, 210016, China*

[2] *Centre for Secure Information Technologies (CSIT), ECIT, Queens University Belfast, Belfast, BT3 9DT, UK*

a) *liuweiqiang@nuaa.edu.cn*

Abstract: A Physical Unclonable Function (PUF) can be used to provide authentication of devices by producing die-unique responses. In PUFs based on ring oscillators (ROs) the responses are derived from the oscillation frequencies of the ROs. However, RO PUFs can be vulnerable to attack due to the frequency distribution characteristics of the RO arrays. In this letter, in order to improve the design of RO PUFs for FPGA devices, the frequencies of RO arrays implemented on a large number of FPGA chips are statistically analyzed. Three RO frequency distribution (ROFD) characteristics, which can be used to improve the design of RO PUFs are observed and discussed.

Keywords: physical unclonable function, RO PUF, comparison strategies, entropy density

Classification: Electron devices, circuits, and systems

References

[1] R. Pappu, B. Recht, J. Taylor and N. Gershenfeld: Science **297** (2002) 2026. DOI:10.1126/science.1074376

[2] G. E. Suh and S. Devadas: DAC (2005) 9.

[3] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola and V. Khandelwal: IEEE RFID (2008) 58. DOI:10.1109/RFID.2008.4519377

[4] S. Morozov, A. Maiti and P. Schaumont: in *Reconfigurable Computing: Architectures, Tools and Applications*, ed. A. Koch, R. Krishnamurthy, J. McAllister, R. Woods and T. El-Ghazawi (Springer Press, Berlin, 2010) 382.

[5] A. Maiti, J. Casarona, L. McHale and P. Schaumont: HOST (2010) 94.

[6] A. Maiti and P. Schaumont: FPL (2009) 703. DOI:10.1109/FPL.2009.5272361

[7] R. Maes: Ph.D thesis University of KU Leuven (2012).

[8] C. E. Yin and G. Qu: DAC (2013) 184.

[9] A. Maiti and P. Schaumont: Research on physical unclonble functions (PUFs) at SES Lab, Virginia Tech (2011) http://rijndael.ece.vt.edu/puf/main.html.

DOI: 10.1587/elex.12.20141043
Received November 5, 2014
Accepted January 13, 2015
Publicized January 28, 2015
Copyedited February 10, 2015

1 Introduction

A PUF as proposed by Pappu *et al.* in 2001 [1] has the ability to generate unique responses and as such can be utilized as a security primitive to provide authentication. In a PUF solution, a set of challenges are issued to a device, which returns a set of unique responses for that device. The relationship between the challenges and responses is determined by random variations in the physical material of the device. Silicon PUFs exploit the manufacturing variations inside integrated circuits (ICs), which cannot be manipulated by the manufacturer. As such, silicon PUFs can generate chip-unique challenge/response pairs which have promising applications in security for device authentication, secret key generation [2], RFID anti-counterfeiting [3] and so on.

The RO PUF is a delay-based silicon PUF, and was proposed by Suh and Devadas in 2007 [2]. A RO PUF exploits the propagation delay deviation of signals caused by manufacturing process variations. Most previous research into RO PUF focuses on the improvement of the RO construction [6] and evaluating its performance using PUF metrics such as uniqueness and reliability [5]. However, the security of RO PUF designs has not been fully considered.

A regular RO PUF is comprised of four different parts that include a RO array, two n-to-1 MUXes, two counters and a comparator, as shown in Fig. 1. A RO array is constructed by a number of identically laid-out ROs, where every RO is a form of closed-loop chain of n inverters, and n must be odd (usually 3 or 5). A challenge signal selects two ROs via two MUXes to feed the two counters, which are used to count the number of oscillations of the ROs and start/stop simultaneously. Due to manufacturing variations, the frequencies of the ROs are different, and therefore, the counter output values will be different. Unlike other PUF constructions, RO PUFs are very suitable for implementation on FPGA devices as they do not require strictly symmetrical routing [4].

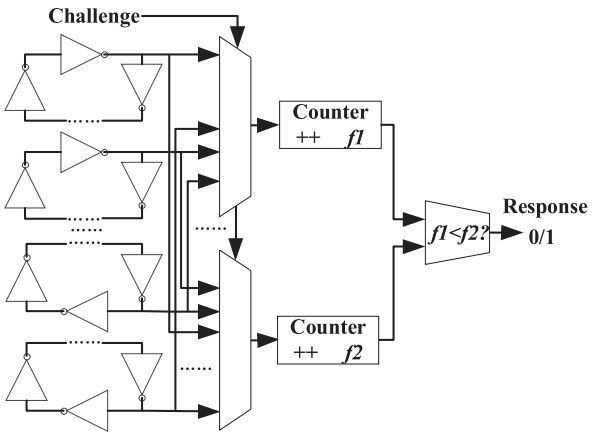

Fig. 1. A RO PUF circuit [7]

In previous research, Maiti *et al.* [5, 9] implemented and evaluated RO PUF arrays comprising 512 ROs in each array on 193 Spartan3E S500 FPGA devices. The ROs are placed in a 32×16 array in the middle of a FPGA chip and their placement was controlled. Each RO is constructed using five logic gates, namely

DOI: 10.1587/elex.12.20141043
Received November 5, 2014
Accepted January 13, 2015
Publicized January 28, 2015
Copyedited February 10, 2015

four inverters and a 2-input NAND gate with one of the inputs used as an enable signal for the RO oscillation. A complete RO loop is implemented in a configurable logic block (CLB) and in order to keep all ROs identically configured, they are created as hard macros.

In this letter the design of RO PUFs is evaluated by statistically analysing the RO frequency distribution (ROFD) characteristics in RO arrays. The frequency data provided by Maiti *et al.* is used to perform the statistical analysis [9]. This evaluation leads to the discovery of three significant ROFD characteristics, which are closely associated with the security of RO PUFs.

2 ROFD characteristics

In order to obtain the relationship between the location of ROs and their frequencies, an intuitive way is to present both in a two dimensional figure, as shown in Fig. 2. There are 32×16 cells that represent 512 hard macro ROs implemented on a Spartan3E FPGA. The layout of the 512 hard macros in this figure is the same as their layout in the implementation on the Spartan 3E FPGA by Maiti *et al*. [9]. The darker colours are used to represent ROs with lower frequencies.

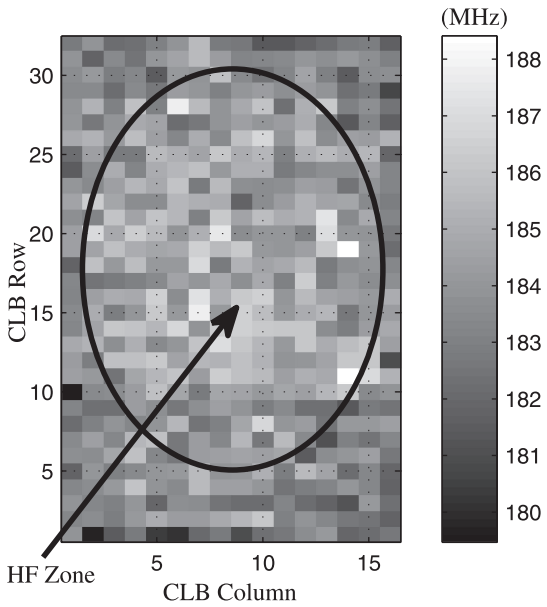

Fig. 2. Real frequencies of ROs from a FPGA chip (*HF*: *high frequency*)

In Fig. 2, it is clear that the frequencies of ROs located in the centre are generally higher than those placed along the border. This is also observed by Maiti [6]. However, this ROFD is for just one RO array of a FPGA chip. A more extensive analysis is required in order to evaluate this effect on the design of RO PUFs in general.

By calculating the average frequencies of ROs in the RO arrays that were implemented in the 193 FPGA chips by Maiti *et al.* [9], it reveals that RO frequencies and their locations are closely related. The average frequency of ROs is a defined as follows:

DOI: 10.1587/elex.12.20141043
Received November 5, 2014
Accepted January 13, 2015
Publicized January 28, 2015
Copyedited February 10, 2015

$$F_{avg}(x, y) = \sum_{l=1}^{L} f_l(x, y)/L, \quad (x \le X, y \le Y) \tag{1}$$

where, $f_l(x, y)$ is the frequency of a RO that is located at the x^{th} CLB row and y^{th} CLB column in the RO array of the l^{th} FPGA; L is the number of FPGA chips, and L is 193; X is the number of CLB rows and Y is the number of columns in the RO array. Therefore, $F_{avg}(x, y)$ is the average frequency of RO (x, y). A CLB row/column will be written as row/column in the rest of the letter.

The results of the ROFD evaluation are shown in Fig. 3. Equi-frequency curves are used to distinguish regions of ROs with similar frequencies as indicated in Fig. 3(b). Lighter coloured curves represent ROs with higher frequencies. Based on Fig. 3, three ROFD characteristics can be observed as follows:

1. The RO arrays can be divided into four different zones, namely, $P1$, $P2$, $P3$ and $P4$, which are shown using a dotted line in Fig. 3. ROs located in the centre of each zone oscillate faster than those located along the border. In Fig. 3(b), equi-frequency curves are nearly elliptical, which implies that RO frequencies are elliptically distributed in each zone.

2. Adjacent grid cells tend to have similar colours as shown in Fig. 3(a). That is to say, adjacently placed ROs have close frequencies.

3. In Fig. 3(a), ROs that are symmetrically placed to the 17^{th} row have similar frequencies. The 17^{th} row is located along the border of zone $P2$ and zone $P3$.

In order to further explore these distribution characteristics, the average RO frequency in each row, $F_{row}(x)$, is calculated as follows and depicted in Fig. 4:

$$F_{row}(x) = \sum_{y=1}^{Y} F_{avg}(x, y)/Y, \quad (x \le X) \tag{2}$$

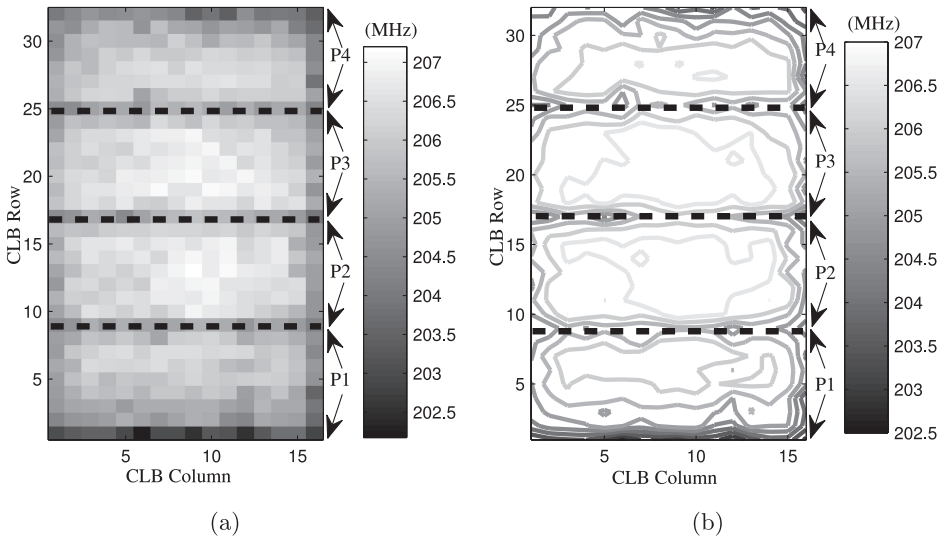

Fig. 3. Average frequencies of ROs from 193 FPGA chips: (a) Average frequencies of ROs denoted by cells; (b) Average frequencies of ROs denoted by equi-frequency curves

DOI: 10.1587/elex.12.20141043
Received November 5, 2014
Accepted January 13, 2015
Publicized January 28, 2015
Copyedited February 10, 2015

Obviously, the four zones ($P1$–$P4$) into which the RO layout has been divided in Fig. 3 are clearly evident in Fig. 4. $P1$ is from the 1^{st} row to the 9^{th} row. $P2$ is from the 9^{th} to 17^{th} row. $P3$ is from the 17^{th} to 25^{th} row and $P4$ is from the 25^{th} to 32^{nd} row. The middle rows have relatively higher average RO frequencies in each zone, as highlighted by ellipses $E1$, $E2$, $E3$ and $E4$.

Generally, rows which are adjacently located have close average RO frequencies. For example, the average frequency of the 2^{nd} row ($row - 2$) is closer with that of the 3^{rd} row ($row - 3$) than that of the 4^{th} row ($row - 4$) as shown in Fig. 4. This illustrates that adjacent ROs have similar frequencies.

In Fig. 4, $E1$, $E2$, $E3$ and $E4$ are used to represent the rows with close frequencies. It can be found that $E1$ and $E4$ ($E2$ and $E3$) are symmetrically placed to the 17^{th} row, and the frequencies in $E2$ ($E1$) are similar to the frequencies in $E3$ ($E4$). This demonstrates that the ROFD of RO arrays is symmetrical.

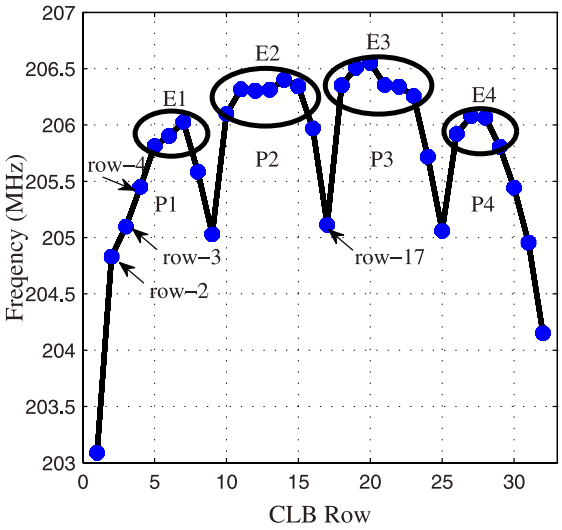

Fig. 4. Average frequency of ROs of each row

In [9], five FPGA chips were evaluated for varying core supply voltages (0.98v, 1.08v, 1.20v, 1.32v and 1.44v) and temperatures (35°C, 45°C, 55°C and 65°C). The resulting data was analysed in relation to ROFD and it was found that the characteristics identified above also hold for environmental variations.

3 Results analysis

The ROFD characteristics discussed above could be used to attack RO PUF or improve RO PUF design. On the one hand, an adversary could use these characteristics to perform attacks on RO PUFs by analysing the relationship of RO locations and their frequencies. For example, if there are two ROs ($RO1$ and $RO2$) that are separately chosen by two MUXes to feed two counters as illustrated in Fig. 1, assuming the condition that $RO1$ is located at the end of the 1st row and $RO2$ is located in the middle of the 20^{th} row of a RO array, then according to the ROFD characteristics, $RO2$ has a very high probability of oscillating faster than $RO1$. As a result, the response bit that is generated by comparing the counter output values of $RO1$ and $RO2$ has a high probability of being successfully predicted by an

DOI: 10.1587/elex.12.20141043
Received November 5, 2014
Accepted January 13, 2015
Publicized January 28, 2015
Copyedited February 10, 2015

adversary. On the other hand, for PUF designers, the characteristics can be used to guide the design of RO PUF. For example, from the second ROFD characteristic it can be seen that if the two selected ROs are adjacently located, it is hard to tell which RO will oscillate faster and as such, the response bit will be difficult to predict.

Therefore, it is clear that these ROFD characteristics are very important for improving the design of RO PUFs, especially with respect to RO PUF coding methods as studied in [8].

4 Conclusion

In this letter, three ROFD characteristics of RO arrays are observed by statistically analyzing the RO frequency distributions of RO arrays implemented on FPGAs. These characteristics are closely related to the security of RO PUF and can be used to improve the design of RO PUFs. Future work will focus on applying the observed ROFD characteristics into RO PUF designs.

Acknowledgments

This work is supported by a grant from National Natural Science Foundation of China (No. 61401197).

DOI: 10.1587/elex.12.20141043
Received November 5, 2014
Accepted January 13, 2015
Publicized January 28, 2015
Copyedited February 10, 2015