DOI 10.29042/2018-4334-4339

Helix Vol. 8(6): 4334- 4339

Investigation of ROPUF with Improved Temperature Performance on FPGA

[*1]Aman Pandey, [2]Sandeepkumar Pandey

[1,2]Department of Electronics Engineering, Shri Ramdeobaba College of Engineering and Management, Nagpur, India

*Email: [*1]amanpandey2109@gmail.com, [2]pandeys@rknec.edu*

Received: 20th September 2018, Accepted: 11th October 2018, Published: 31st October 2018

Abstract

Physically Unclonable Function (PUF) is one of the better known security tool used for safety of electronic devices. Among several PUF designs, Ring Oscillator Physically Unclonable Function (ROPUF) is one of the most favoured PUF design and it can be easily implemented in Field Programmable Gate Array (FPGA). It is evident from the literature that change in the temperature causes more error in the PUF responses. In this work, our aim is to make a ROPUF which can be implemented on FPGA with better temperature performance in output PUF bit generation. Designs are implemented on same FPGA and its reliability is checked at varying room temperatures. In fact, due to temperature variations further uniqueness can be achieved which will help to build stronger ROPUF. Spartan 6 FPGA boards were used to test the proposed PUF architecture and the system outputs were statistically evaluated proving the suitability of the proposed PUF design for device identification in real world.

Keywords

Physically Unclonable Function (PUF), FPGA, Ring Oscillator

Introduction

Mobile and various electronics devices are omnipresent as they are interconnected for several day to day tasks. Overwhelming growth in Electronics and Internet of Things (IoT's) has resulted in multiple issues regarding security. IoT will become established element of our life making security concern more important.

Hence to resolve this problem Cryptography is used, which uses a secret key but Cryptography is a classical approach. Cryptography uses a secret key, which is stored in non-volatile memory. As the secret key is stored in Non-Volatile memory, the secret key is domitable. This eventually means that such security measures are not reliable and there is a necessity of a safer and indomitable method.

In past few years Physical Unclonable Function (PUFs) is considered as propitious security application. The interest in PUF has increased exponentially which has made it a talking point in the field of hardware security. It works on the principle of Process Variations and these Process Variations can neither be duplicated nor they are controllable but can be evaluated and used for device identification effectively.

Ring oscillator PUFs use an approach toward measuring small random delay deviations caused by manufacturing variability. The output of a digital delay line is inverted and fed back to its input, creating an asynchronously oscillating loop, also called a ring oscillator. The frequency of this oscillator is precisely determined by the exact delay of the delay line. Measuring the frequency is hence equivalent to measuring the delay, and due to random manufacturing variations on the delay, the exact frequency will also be partially random and device dependent. Frequency measurements can be done relatively easy using digital components: an edge detector detects rising edges in the periodical oscillation and a digital counter counts the number of edges over a period of time. The counter value contains all the details of the desired measurement and is considered as the PUF response. If the delay line is parameterizable, the particular delay setting is also considered as the challenge.

Over the year numerous ROPUFs are being introduced. Ever since the ROPUF concept is explored, the type of methodology and construction used in different types of RO PUF is being studied.

ROPUF architectures which were proposed earlier before had mechanism that compares the frequency between two different ROs, and if there are substantial variations in frequency then it results in robustness of ROPUFs. In their work, G. E. Suh and S. Devadas [10] chose the best RO pair with very high change in frequency out of many other ROs, which in result requires very large count of ROs. RO frequency is dependent on the placement of the RO on the FPGA, and improvement in the reliability of an ROPUF by implementing every Ring Oscillator in a single configurable logic block was founded by Maiti and Schaumont [12]. Merli *et al.* explained that the frequency is enhanced by chainlike structure using the frequency difference of nearest neighbour ROs [13]. Habib *et al.* proposed a RO-PUF which has more efficiency by taking in to the account the delay lines which can be programmed [14]. The development of improvised RO-PUF is done by C.E. Yin and G. Qu [15] and L. Bossuet *et al* [16]. Especially the ROPUF by Bossuet *et al.* [16] is unaffected to the locking phenomenon of the ROs. Apart from ROPUF there are several other proposals of PUFs which are designed over FPGA. Tuyls *et al.* proposed the butterfly-PUF [17] and also flip-flop (FF)-PUF was proposed [18]. Very good performance of the Hamming distance (HD) and small temperature dependence is shown by the butterfly-PUF .Yamamoto *et al.* proposed a PUF using reset/set (RS)-FF [19], in which the inhibition input of RS-FF is used to reflect the chip identity. Filip Kodýtek and Róbert Lórencz

[1] presented RO based PUF, which uses 16-bit counter values generated by RO pairs by selecting suitable bit positions from these values for PUF. The advantage of this design is that it is easy to implement, since the ROs no longer need to be symmetric, and it produces more output bits from one RO pair. Results show that this ROPUF design is suitable for device identification and can be even used for cryptographic key generation, when it is combined with error correction code. But it was observed due to temperature change i.e. change in room temperature and change in temperature due to measurements, more errors occur in PUF responses. Even though the measurements were performed under fixed environmental conditions (stable temperature), it was observed that the temperature on all FPGAs was increased during the measurements and this temperature variation is caused by the ROs themselves.

Methodology

In this paper ROPUFs are implemented and their output bits are calculated at different room temperature i.e. 16^{o}C, 27^{o}C, 38^{o}C. It is said that the change in temperature also changes output bits. If there is change in room temperature and along with that temperature on FPGA changes whilst measurement then this will definitely change output bits, but we aim to prove that this variation in the output bits is relative as per the temperature. We exploit this fact that the ambient temperature is present as common mode variation to all the ROS in our differential topology.

Since there is differential structure in the proposed architecture, common mode disturbances (ex. change in Room Temperature and change in Temperature of FPGA during measurements) in operating conditions are cancelled out. It is also not dependent on placement of RO on FPGA implying that it is easy to implement under any operating conditions. This way output bit patterns which are more immune to environmental variations is obtained. This ROPUF design selects suitable bits for PUF from counter values obtained from the measurements on various RO pairs. Using this technique, bits from each RO pair are obtained which as a result are more stable and unique as proved in analysis. Hence reliable PUF can be realised.

Implemented Ring Oscillator PUF

In this design RO pair is selected and the PUF output will also be obtained based on that pair selection. To construct PUF using Ring Oscillator a five stage RO consisting of one NAND gate and four Inverters is used as basic building element shown in Figure 1 (a). One RO pair is chosen and their oscillations are counted rather than measuring frequency of each RO using reference clock simultaneously using two counters. The measurement is stopped immediately after one of the two selected counters reaches the optimum value of counter and it overflows while at the same time other counter does not overflow. The value in the counter that is yet to reach the optimum value which did not overflow is used as an output of the Ring Oscillator PUF for further processing. This approach is shown in Figure 1(b).

The proposed architecture shown in the Figure 3 is designed using Verilog structural coding with the help of Xilinx ISE. At first a single ring oscillator pair is designed and tested, this design is then instantiated in a top module PUF along with other 15 pairs of ring oscillator to form a complete PUF architecture.

The system is then implemented in the DigilentAtlys Spartan 6 kit and the output bits are recorded using chipscope pro.

The outputs recorded are then used as an input to the formulae designed in Matlab to calculate Bit stability, Entropy, Bit error rate mentioned in the section given below.

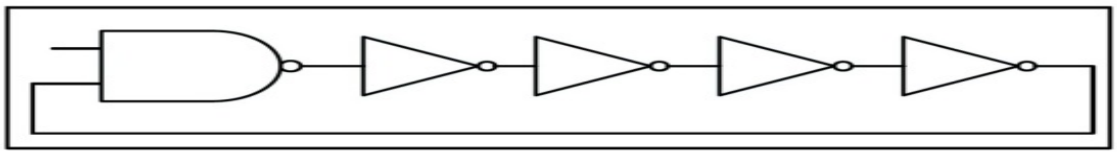

Figure 1(a): Five Stage Ring Oscillator

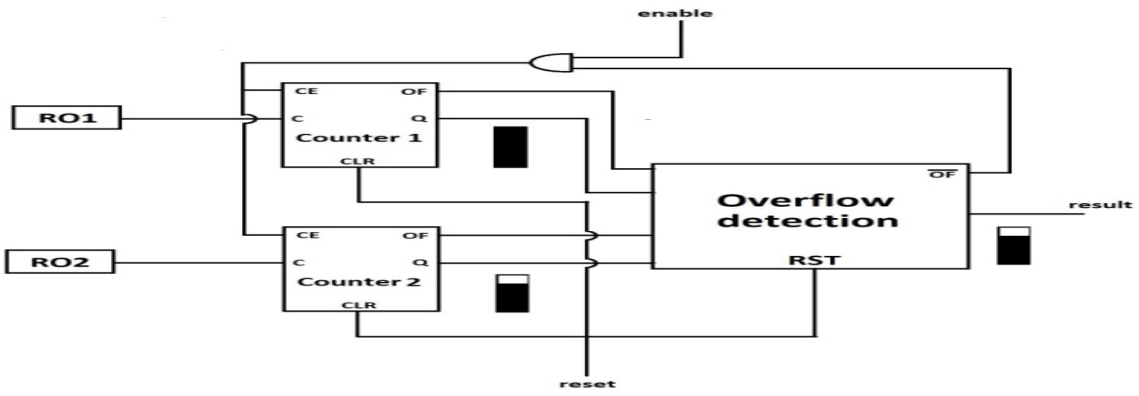

Figure 1(b): Counting of Cycles of Two Ring Oscillators which are run simultaneously and Counter Overflow Detection in the Proposed ROPUF Design

Formulae Used and ROPUF Proposal

A. Bit stability

The stability of a bit position is based on the probability of occurrence of 1 or 0 at that given position.
Stability *si*(RO) from the value measured of ith bit position from a particular RO pair is determined as follows:

$$s_i(\mathbf{RO}) = \begin{cases} P(bi = 1) if P(bi = 1) & \geq 0.5 \\ 1 - P(bi = 1) if P(bi = 1) & < 0.5 \end{cases} \quad (1)$$

In the above equation the term P(bi = 1) is used to give the probability of occurrence of value 1 at position i .The probability of occurrence of 1 is obtained by calculating the average of the values obtained at the particular position of a particular RO for executed measurements. The formula is given as follows:

$$P(b_i = 1) = \frac{1}{k} \sum_{j=1}^{k} b_{j,i} \quad (2)$$

In the above equation the term k is the number of executed measurements and the term bj,i indicates the i-th bit of j-th measured value. As the ROs in the design are mutually asymmetric, stability will vary for each RO pair, thus, average stability of a particular position is calculated to determine the best suitable bit positions from all the bits for the PUF output for all RO pairs. Let us assume that if we have RO pairs, then the average stability *si* of position i is determined as:

$$s_i = \frac{1}{n} \sum_{j=1}^{n} s_j(RO_j) \quad (3)$$

In the above equation the term ROj is j-th pair of ROs.
Depending upon the average stability *si* for every position it is possible to determine which bits can be used for desirable PUF output. Ideally, stability *si* should be equal to one for the bit position we wish to, but such value of stability may not be achieved, and even if we manage to achieve such stability it can be for bits near to MSB. Hence, it would be feasible to assign a threshold value *sth* depending on which we can select suitable bit positions. For example, if we consider *sth* = 0.95, then all the bit position from the MSB to the first position will be selected which are having *si* < 0.95.

B. Entropy

Bit stability helps in choosing a particular bit position for a PUF but it cannot be the sole selector, as along with stability we have to consider uniqueness in different FPGAs and hence two set of bits can have same value for different FPGAs. Thus, in order to have better precision in selection of bits, entropy of bit position is taken into account.
Entropy is the measure of uniqueness of bits among different FPGAs. It may be assumed that the most significant bits (MSBs) will not differ from one other respectively, it is also expected that the least significant bits (LSBs) will fail the stability criteria. The bits close to the middle between the MSB and LSB will be more stable and unique for different FPGAs. It is not wise to consider bits position close to LSB as there will be a lot of variations resulting in unstability.
The following formulas define the mean entropy of a bit position in a FPGA:

$$H_{intra}(i) = -\frac{1}{m} \sum_{j=1}^{m} \sum_{k=0}^{1} p_j(k) log_2(p_j(k)) \quad (4)$$

Where "*Hintra"* is the Intra-chip Hamming Distance and in the above equation the term m defines the total count of FPGAs and the probability of k^{th} message within the j^{th} FPGA is defined by $p_j(k)$.
The possibilities of a bit position are only 0 and 1 and are calculated by the use of following formula:

$$p_j(1) = \frac{1}{n} \sum_{k=1}^{n} maj(RO_{j,k}, i), \; p_j(0) = 1 - p_j(1) \quad (5)$$

The term ROj,k shows the k-th of the RO pairs on the j-th FPGA, where number of RO pairs is represented by n. Maj(RO,i) shows the majority of the i-th position determined from the total of k measurements which are evaluated for each RO pair. The result can be either 1 or 0 and is defined as:

$$maj(RO, i) = round\left(\frac{1}{k} \sum_{j=1}^{k} b_{j,i}\right) \quad (6)$$

For each of the n different RO pairs through different FPGAs, average entropy of bit position I is given as:

$$H_{inter}(i) = -\frac{1}{n} \sum_{l=1}^{n} \sum_{k=0}^{1} pl(k) log_2(pl(k)) \quad (7)$$

Where "*Hinter"* is the Inter-chip Hamming Distance and in the above equation pl(k) → probability of the message k of the lth RO pair in FPGAs. The way the probability is calculated is similar to as in the case of Hintra, pl(k) is defined as:

$$pl(1) = \frac{1}{m} \sum_{k=1}^{m} maj(RO_{k,b}, i), \; pl(0) = 1 - pl(1) \quad (8)$$

The maximum entropy of 1- bit message i.e 1 is the ideal value for *Hintra* and *Hinter*. The ideal value represents zero correlation between bits on the same positions among different FPGAs.

C. Method of selecting suitable bit positions for PUF

Stability and entropy should be necessarily considered whilst selecting suitable bit positions for PUF. The stability is increased and the entropy is decreased towards the most significant bit. As discussed the stability and entropy are both required as high as possible. Thus, a very crucial compromise is to be made between good entropy and high stability, where both the parameters attain high enough value. The selection of appropriate bits may look as follows:

• Stability *si* will be analysed from MSB to LSB till the point its value is the threshold value *sth* which is predetermined.
• Then to analyse entropy ,it is checked from LSB to MSB, now entropy *Hintra* and *Hinter* threshold value *Hth* is considered ,bits are chosen when both entropies satisfy the criteria (*Hintra(i) > Hth ∧ Hinter(i) >Hth*).This whole procedure is shown in Fig. 2.

D. Proposed ROPUF architecture

The architecture of the proposed design is shown in the figure below. In total, 16 ring oscillators pairs that are described in the Figure 3 are wrapped in a module and a single pair is then selected on the basis of select input. Two sixteen bit counters are used as measurement circuit in our architecture whose value are measured.

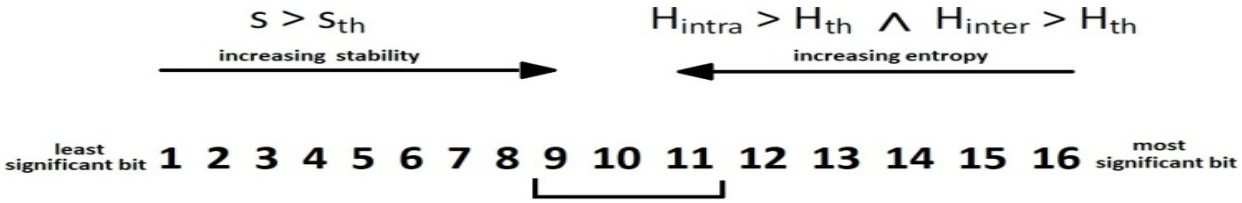

Figure 2: The Example Selection of Suitable Bit Positions for PUF

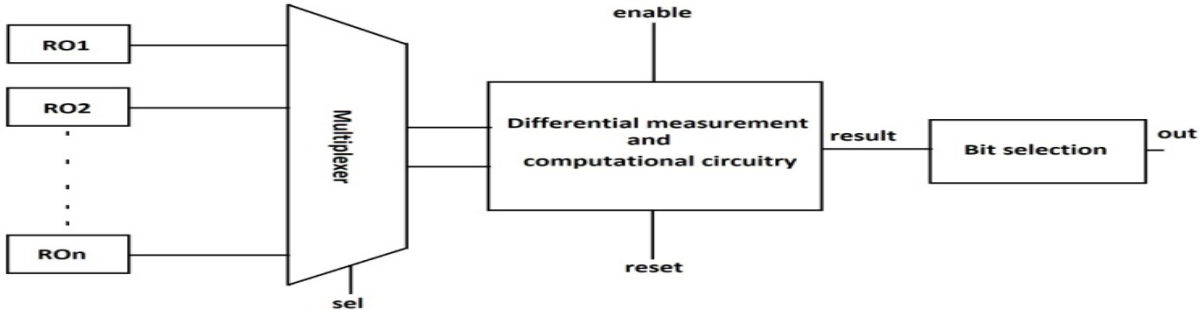

Figure 3: The Design of the Proposed ROPUF

E. Bit Error Rate

The verification of bit stability in this ROPUF design can be done by calculating the bit error rate. Percentage of bits which contains errors with respect to the total number of bits is the bit error rate (BER). For n-bit responses of the i-th FPGA we define BER as follows:

$$\mathbf{BER} = \frac{1}{n*k}\sum_{j=1}^{k} HD(R_{pi}, R_{i,j}) \quad (9)$$

In the above equation the term k is the number of responses from the PUF, HD is the Hamming distance between two bit strings, Ri,j is the j-th response from PUF on the i-th FPGA and Rp is the "mean" response made from k responses. We determine Rp from majorities for each position in n-bit responses.

The average bit error rate for m FPGAs is calculated as:

$$\mathbf{BER} = \frac{1}{m}\sum_{i=1}^{m} BER(i) \times 100[\%] \quad (10)$$

Results and Discussion

In this section, the results of evaluated measurements, which were all realized on Spartan 6 FPGA boards, are presented. The experiment is performed in three different room temperature i.e. 16°C, 27°C and 38°C. Under each temperature measurements are taken 10 times for each RO pair. These measurements were used to evaluate parameters using the formulae shown in the section above. Analysis of these evaluated results are used to determine the most stable bit out of total 16 bits on the basis of which uniqueness of the PUF is determined. Evaluation done is displayed in the graphs below for all the 16 bit position of the PUF output. As seen in Figure 4 the stability increases from LSB to MSB and almost reaches the ideal value 1. Whereas *Hintra* and *Hinter* are been evaluated which decreases towards MSB, considering these parameters the most stable bits position as discussed in the method of selecting suitable bit position are found to be bit 9,10,11. From Figure 5 it is also evident that Bit Error Rate is very small and it further reduces from LSB to MSB which makes the PUF response to be desirably stable and helps in selecting suitable bit position having as less as possible bit error rate.

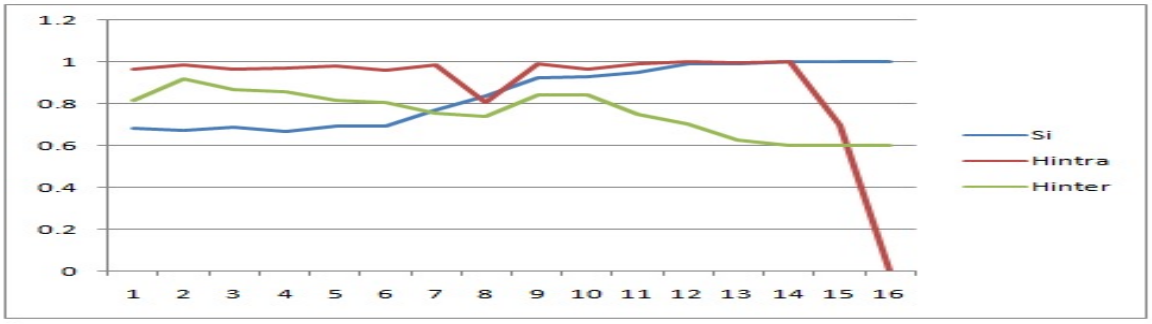

Figure 4: Graph Plotted with bit Position on X-axis and Value of *si*, *Hintra* and *Hinter* on –axis

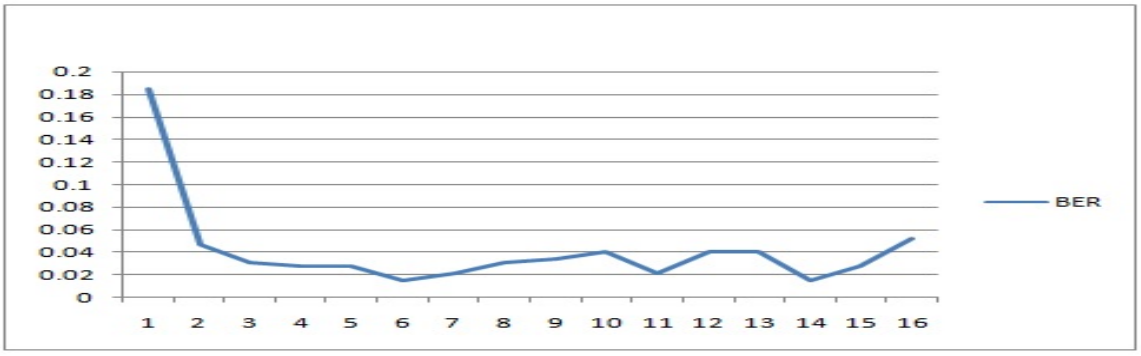

Figure 5: Bit wise Value of BER and Graph Plotted with bit Position on X-axis and value of BER on Y–axis

Conclusion

In this paper, RO based PUF with improved temperature performance is proposed, which is providing unique output bits despite change in room temperature or change in temperature due to operation of device. Hence this ROPUF is not strongly dependent on change in temperature. Since there is differential structure in architecture, this cancels out common mode disturbances (ex Temperature) in operating conditions. ROPUF is also not dependent on placement of RO on FPGA implying that it is easy to implement under any operating conditions. This way output bit patterns which are more immune to environmental variations is obtained. This ROPUF design selects suitable bits for PUF from counter values obtained from the measurements on various RO pairs. Using this technique, bits from each RO pair were obtained which as a result are stable and unique bit. Therefore more reliable PUF can be implemented. According to the results, it is evident that this ROPUF design is suitable for addressing problem of identification of Integrated circuits in real world as PUF runs with full effectiveness even under environmental variations in temperature.

References

[1] Filip Kodýtek and Róbert Lórencz , "A design of ring oscillator based PUF on FPGA," 2015 IEEE 18th International Symposium on Design and Diagnostics of Electronic Circuit & Systems 2015.
[2] R.S. Pappu, "Physical One-Way Functions", Ph.D. thesis, Massachusetts Institute of Technology,2001
[3] J.D.R. Buchanan, R.P. Cowburn, A.V. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson,K. Fenton, D.A. Allwood, M.T. Bryan, "Forgery: 'fingerprinting' documents and packaging" , Nature 436(7050), 475 (2005)
[4] Blaise Gassend, Dwaine Clarke, Marten van Dijk and Srinivas Devadas, "Silicon Physical Random Functions", CCS'02,Nov 2002
[5] Anju P. Johnson, Rajat Subhra Chakraborty and Debdeep Mukhopadhyay, "A PUF-Enabled Secure Architecture for FPGA-Based IoT Applications" ,IEEE 2015
[6]Masoud Rostami, James B. Wendt, Miodrag Potkonjak, and Farinaz Koushanfar, " Quo Vadis, PUF?",2014
[7] P. Tuyls, G.J. Schrijen, B. Škori´c, J. van Geloven, N. Verhaegh, R. Wolters, in "Read-Proof Hardware from Protective Coatings". Cryptographic Hardware and Embedded Systems Workshop. Lecture Notes in Computer Science, vol. 4249 (Springer, New York, NY, 2006),pp. 369–383
[8] Ahmad-Reza Sadeghi, David Naccache "Towards Hardware-Intrinsic Security", January 2010
[9] Charles Herder, Meng-Day (Mandel) Yu, Farinaz Koushanfar and Srinivas Devadas, "Physical Unclonable Functions and Applications: A Tutorial," Proceedings of the IEEE, vol. 102, no. 8, pp. 1126-1141, August 2014.
[10] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. IEEE 44th DAC*, 2007, pp. 9–14.

[11]Naini Satheesh, Abhishek Mahapatra, Sudeendrakumar K, Sauvagya Sahoo, K.K.Mahapatra , "A Modified RO-PUF with Improved Security Metrics on FPGA," IEEE International Symposium on Nanoelectronic and Information Systems, 2016.
[12] A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in *Proc. 19th Int. Conf.FPL*, 2009, pp. 703–707.
[13] D. Merli, F. Stumpf, and C. Eckert, "Improving the quality of ring oscillator PUFs on FPGAs," in *Proc. 5th WESS*, 2010, pp. 1–9.
[14] B. Habib, K. Gaj, and J.-P.Kaps, "FPGA PUF based on programmable LUT delays," in *Proc. Euromicro Conf. DSD*, 2013, pp. 697–704.
[15] C.E. Yin and G. Qu, "LISA: Maximizing RO PUF's secret extraction", in *Proc. IEEE HOST*, 2010, pp. 100–105.
[16] L. Bossuet *et al.*, "A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon," *IEEE Trans. Emerg. Topics Comput.*,vol. 2, no. 1, pp. 30–36, Mar. 2014.
[17] S. Kumar, J. Guajardo, R. Maes, G.-J.Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proc. IEEEHOST*, 2008, pp. 67–70.
[18] R. Maes, P. Tuyls, and I. Verbauwhede, "Intrinsic PUFs from flip-flops on reconfigurable devices," in *Proc. WISSec*, 2008, pp. 17–26.
[19] D. Yamamoto *et al.*, "Uniqueness enhancement of PUF responses based on the locations of random outputting RS latches," in *Proc. IEEE HOST*,2011. pp. 390–406.

