A Modified RO-PUF with Improved Security Metrics on FPGA

Naini Satheesh, Abhishek Mahapatra, Sudeendra kumar K, Sauvagya Sahoo, K.K.Mahapatra
kumar.sudeendra@gmail.com, sauvagya.nitrkl@gmail.com, kmaha2@gmail.com
National Institute of Technology, Rourkela

Abstract- **: Physical Unclonable Functions (PUF) are an emerging hardware security primitives proposed by various researchers in last one decade. PUFs are useful security architectures used for identification, authentication and cryptographic key generation. Many PUF topologies are proposed in the past targeting both ASIC and FPGA. It is nearly impossible to get two PUF circuits with same characteristics for the same design. PUFs make use of random process variation occurring during manufacturing of IC which is uncontrollable. The most versatile PUF is ring oscillator (RO) PUF, in which the frequencies of ring oscillators are compared to produce the PUF response. The conventional approach consumes large number of ring oscillators and requires all RO's to be mutually symmetric. In this paper, we have proposed a RO-PUF for FPGA devices, which is capable of generating multiple output bits from each ring oscillator with better security metrics in comparison with PUF designed with similar technique. The PUF is implemented on Xilinx Spartan 3E FPGA boards and the challenge-response pairs (CRP) are verified for statistical properties.**

Keywords: **Physical Unclonable Function, Hardware Security, Reliability**

I. INTRODUCTION

The tremendous growth in the number of electronic gadgets and emergence of Internet of Things (IoT's) applications, has led to several security related issues like data privacy and denial of service etc. And also several hardware security issues like IP protection, counterfeit devices and hardware Trojans are affecting the reliability and security of modern electronic gadgets. There is a need for concrete solutions to address the security related issues from the hardware abstraction level. The important aspect in IoT security is establishing the identity of a device. The device identification and authentication is crucial in mitigation of counterfeit parts in supply chain. The counterfeit parts/devices are unreliable and can be catastrophic in critical applications. In general, hardware security mechanisms use cryptographic techniques to implement authentication, integrity etc. The strength of security depends upon the secrecy of the key used for encryption and attackers target to reveal the key to break the system. So cryptographically generated keys are predictable and attackers are becoming more sophisticated in breaking the systems. Physical Unclonable Functions (PUFs) are promising hardware security primitives, which can used to address the issues related to anti-counterfeiting solutions and cryptographic key generation. PUF circuit produce a unique response (output) for a given stimulus (challenge or input). PUF circuit in each integrated circuit (IC) will produce unique response for a given stimulus. The each challenge-response pair is called CRP. The unique CRP in PUF is generated due to process variation occurring during the manufacturing of IC. The relationship between challenge and response of a PUF circuit is defined by deep sub-micron level variations inside the chip occurring across interconnects and logic. It is nearly impossible to have two similar chips with same PUF CRP's. The circuits which can pick the random process variations are chosen to design PUF circuits. Many PUF circuit topologies can be found in literature [1]. The prominent PUF architectures are: Ring Oscillator (RO) based PUF; Arbiter based PUF, SRAM PUF etc [1].

The PUF circuits for FPGA need to be designed carefully, so that circuit will pick-up the actual process variation on an already fabricated FPGA device. The most versatile circuits for designing PUF in FPGAs are RO-PUF, Butterfly PUF [1] etc. In this paper, we mainly focus on RO-PUF. Many PUF constructions based on ring oscillators are proposed in the past [3]. The ring oscillator measures the delay in a self-oscillating loop and delay is directly affected by process variations. The process/manufacturing variations are reflected in frequency of the oscillations. Ring oscillator frequency is measured using counters. The logic 1 or logic 0 is produced at the output based on the difference between the two counter values connected with two different ring oscillators. The ring oscillators will have different frequencies due to manufacturing variation. The Figure 1 shows the circuit diagram of conventional RO-PUF [2]. The RO-PUF was proposed by Gassend et al [3] for the first time and several modifications to the RO-PUF were proposed to improve the security metrics. The common security metrics used to measure the quality of PUF circuit are: - uniqueness, reliability and uniformity [1] [2]. The environmental conditions like temperature and circuit aging will affect the security metrics. Another important RO-PUF construction was proposed by Suh and Devadas in [2]. RO-PUF in [2] consists of 'n' number of symmetric ROs connected to multiplexer in a similar way shown in Figure 1. In [2], it is necessary to have ring oscillators in RO-PUF should be symmetric, such that frequencies of ring oscillators are dependent mainly on process variations. RO-PUF needs two ring oscillators for a challenge size of 1-bit to generate the one-bit PUF output. The challenge is fed through the select lines of multiplexer to choose the ring oscillators. For a challenge size of two bits, the PUF circuit must have four ring oscillators and for challenge size of three, the number of ring oscillators will go up to eight. And irrespective of number of ring oscillators in the PUF circuit, the output will be 1-bit response based on the values in the counters. To design the PUF circuits with this

conventional RO-PUF, a large number of ring oscillators are required and it will consume more area in chips.

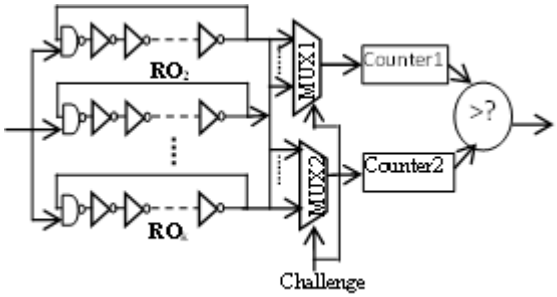

Figure 1: Conventional RO-PUF in [2]

And also all ring oscillators used in RO-PUF must be symmetric for better security metrics. Kodytek et al [5][8] propose a modified version of PUF circuit for FPGA's to overcome disadvantage of large area and symmetricity requirement of ring oscillators used. The PUF proposed by Kodytek et al in [5] is shown in Figure 2. The output response of the PUF is determined directly by selecting few bits from the output of the counter. The output of ring oscillators is fed as clock input to the two counters as shown in Figure 2. The increment in the counters is stopped, when any one of the counter overflows. The value resulted in the counter that did not overflow is used for processing. This technique proposed by Kodytek et al in [5] [8] does not need symmetricity of ring oscillators during design. In the counter output taken for further processing, MSB bits of the counter output will have more stability. The bit selection scheme (not shown in Figure 2) will select bits from the central portion of the counter output between MSB and LSB to get required randomness or entropy of the PUF output. In this technique, it is possible to get larger PUF response with less number of ring oscillators. This technique is suitable for FPGA, because designing ring oscillators exactly symmetric is very difficult in FPGA. It is difficult to get symmetricity in ring oscillators either through manual placement and routing or inbuilt optimization methods used in FPGA design tools.

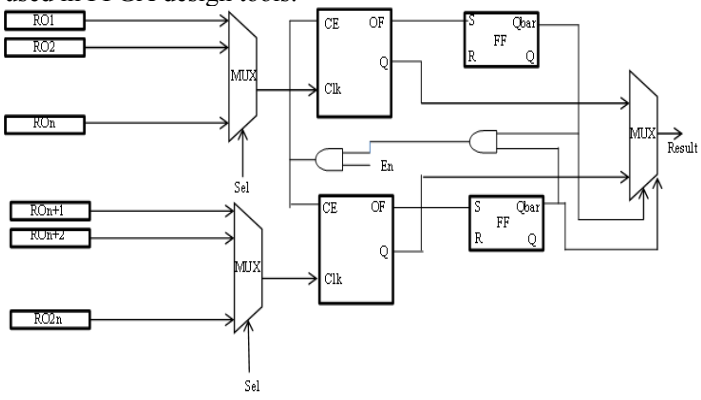

Figure 2: RO-PUF Proposed by Kodytek et al in [5]

In this paper, we propose an improvement to the PUF circuit presented in [5] [8] for better reliability and for a large challenge space. The proposed PUF circuit is targeted for FPGA devices and need characterization of PUF before deploying them in applications. The contributions of this work are:

- Improvement of reliability of CRPs of multi-bit output PUF proposed in [5].
- The proposed PUF topology also provides user with large number of challenges and increases the challenge space significantly.

The next section describes the proposed PUF and its functionality. Section III discusses the implementation and results, and finally section IV concludes the paper.

II. Proposed Physical Unclonable Function

The Figure 3 shows the circuit diagram of the proposed basic PUF component. A standard clock source is connected to run-time counter as a reference clock, based on which it increases its count from the value loaded into it. The challenge to the PUF circuit comprises of a load value to the run-time counter and select line to the multiplexer. Once the challenge is fed, the single enable signal will trigger the ring oscillator and run-time counter at the same time sample. The run-time counter will run from load value and overflow. Upon overflow, run-time counter will drive logic '1' to signal 'OV', and in-turn, it will drive the signal 'STOP', which will stop the PUF-counter. The bit selection scheme will select the appropriate bits from the counter output to produce the PUF response. The bit selection scheme is discussed in detail in next section. The difference between the PUF presented in [5] and PUF proposed in this paper is instead of two ring oscillators, only one ring oscillator is used to generate the PUF response. The counters driven by two different ring oscillators are used in [5]. In the proposed PUF, one counter is driven by ring oscillator and another by a standard clock source. The single ring oscillator is sufficient to pick the random process variations occurring during manufacturing [9].

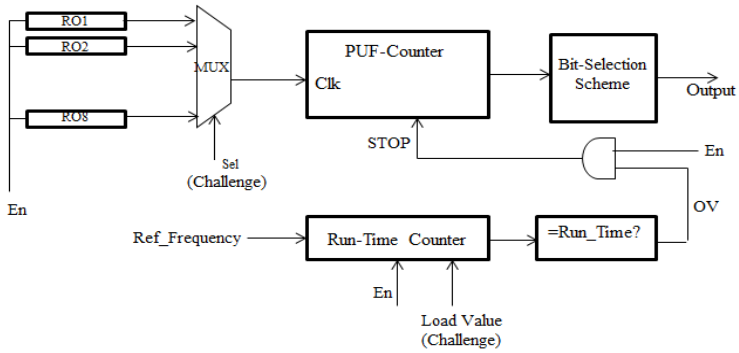

Figure 3: Proposed modified RO-PUF

III. Implementation and Results

The basic PUF circuit diagram of proposed PUF is shown in Figure 3. The basic PUF circuit comprises of eight ring oscillators, PUF-counter and bit selection unit. The basic circuit of proposed PUF is instantiated eight times. A single run-time counter can be shared by all eight PUF instances. The single run-time counter increases the routing complexity. An individual run-time counter for each instance will increase

the area. In our implementation, we have used individual run-time counters for all eight instances of PUF circuit. After the overflow of the run-time counter, which has started counting from the load value, the STOP signal generated by run-time counter will stop the counting in PUF-counter. The bit selection scheme selects the bits from the central portion of the output of the PUF-counter. To minimize the routing issues and to maintain the constant offset in delays, an individual run-time counter is used for each PUF instance.

Manual routing is performed to place and route the cells in each CLB (configurable logic block) of Xilinx Spartan 3E FPGA device. The Xilinx Spartan 3E CLB consists of four slices and each slice comprises of two LUTs (Look-Up Tables). The NOT gate for RO design is implemented using one LUT. The number of NOT gates used in each RO is five. So each RO use five slices in one CLB. The RO with five NOT gates is created as macro and instantiated into the design of a proposed PUF.

The multiplexer in the basic PUF circuit will have three select lines to choose the RO to drive the PUF counter. The multiplexer selection lines are part of the challenge input to the PUF. The challenge to the proposed PUF comprises of all select lines of multiplexers of eight PUF instances and the 32-bit load value which is fed into the run-time counter. The total bit-size of the challenge will be 56 bits (24 bits to multiplexer and 32 bit load value into run-time counter). The bit-size of the response of the PUF is 32-bit. The bit selection scheme is similar to the bit selection technique used in [8]. The PUF-counter size is 32-bit. Bit selection scheme selects the four bits from the counter output. In the 32-bit output from the PUF-counter, 15th, 16th, 17th and 18th bits are selected to produce the PUF response. From the each instance, four bits are taken and concatenated to produce the PUF response. The concatenation of four bits from all eight instances will make the PUF response 32-bit size.

Results: The performance of the PUF is determined based on the quality of challenge-response pairs (CRP's). The measurement of quality is performed using standard security metrics discussed in PUF literature. Abranil Maiti et al in [6] discuss the systemic method to evaluate the performance of PUFs. The widely discussed security metrics are: uniqueness, reliability and uniformity. In this paper, we present the modest discussion on security metrics and detailed discussion can be found in [6].

Uniqueness: Uniqueness is a measurement of an ability of a PUF to distinguish itself in a group of similar PUFs through its unique challenge-response pairs. It is a measure of inter-die variation. Uniqueness is considered as primary security metric considered while choosing the PUF for applications like anti-counterfeiting etc. Let S_i and S_j are the responses obtained by two PUF circuit having n-bit response. The average uniqueness for 'C' number of PUF chips is calculated using the equation:-

$$\frac{2}{C(C-1)}\sum_{i=1}^{C-1}\sum_{j=i+1}^{C}\frac{HD(S_i,S_j)}{n}\times 100\ \% \qquad (1)$$

In equation (1), the HD is the Hamming Distance between any two responses for same challenge. The Hamming Distance (HD) between the two PUF responses is determined as below:-

$$HD(S_i,S_j)=\sum_{t=1}^{m}(S_{i,t}\oplus S_{j,t}) \qquad (2)$$

In equation (2), the $S_{i,t}$ is the t[th] response bit of the n-bit response of the S_i of the PUF_i.

Reliability: Reliability is a measurement of an ability of a PUF to reproducing the same response for a same challenge. Reliability also means a consistency of a PUF reproducing the same response for a given challenge. Reliability is affected by environmental variations like changes in supply voltage and temperature. Suppose an n-bit response is obtained from PUF_i for a given challenge. The same challenge is applied on the same PUF several times (on the same chip) and responses are recorded to check the consistency, whether the same response is reproduced for a given challenge. Reliability of PUF circuit should be 100% ideally. Let n-bit response (S_i) is obtained from a PUF_i and S_i is taken as reference response. The same challenge is applied responses are collected. The reliability of the PUF is calculated using the equation below:-

$$(100-\frac{1}{x}\sum_{y=1}^{x}\frac{HD(S_i,S_{i,y}')}{m}\times 100)\% \qquad (3)$$

Whereas the $S_{i,y}'$ is the y[th] sample of S_i

Uniformity: Uniformity measures the how uniform the 0's and 1's are distributed in the response. The ideal value of uniformity is 50%. For an n-bit response the uniformity is calculated using the following equation:-

$$(uniformity\ )i=\frac{1}{n}\sum_{l=1}^{n}R_{i,l}\times 100\ \% \qquad (4)$$

Where the $R_{i,l}$ is the lth binary bit of an n-bit response from a given chip 'i'.

The four binary bits from the central portion of the counter is directly taken as PUF output. The least significant bits (LSB) will vary more frequently and most significant bits (MSB) will change less number of times in comparison with LSB. The entropy of LSB bits will be more than MSB bits. To balance between the stability and entropy, it is better to choose the bits from the central portion of the PUF-counter. This technique is used in the work presented by Kodytek [5] and Bossuet et al [7].

The comparative analysis of security metrics is performed to determine the quality of PUF. In the paper [5], performance is analysed using intra-hamming distance, intra hamming distance and bit error rate. The intra-hamming distance is synonym with reliability and inter-hamming distance is a

synonym with uniqueness [6]. The measured security metrics of proposed PUF is presented in Table I. The ten Spartan 3E FPGA boards are used to perform the measurements. The 2^{56} combinations are possible in the input challenge space. In this experiment, 65536 CRP's are collected from 10 FPGA boards to calculate the security metrics presented in Table I. The measurements of security metrics presented and discussed are for standard room temperature and stable supply voltage. Xilinx Spartan 3E FPGA is used in our experiment operated at 50MHz frequency. From Table I it is clear that the proposed PUF has got better security metrics in terms of uniformity and reliability than the PUF presented by Kodytek et al in [5][8].

Discussion: In the PUF presented in [5], the challenge to the PUF will select the any two ring oscillators output to increment the counters. An overflow in any one of the two counters will stop the other counter. The bits for the PUF response are extracted from the counter which did not overflow. A basic PUF shown in Figure 3 comprises of eight ring oscillators and a complete PUF circuit (eight instances) contains 64 ring oscillators. The challenge to the PUF selects two ring oscillators in the PUF presented in [5] and in the proposed PUF challenge will select only one ring oscillator. The frequency of 64 ring oscillator is measured using Agilent Logic Analyzer and frequency varies from 26 MHz to 34 MHz on 10 FPGA boards. The challenge to the PUF in [5] chooses a two ring oscillators to drive two counters. The chance of ring oscillators having proximal frequency is high in the same die, which results in high probability of bit-flipping which will affect the reliability of the PUF CRPs. In the proposed PUF, only one ring oscillator is used to determine the response and clock of the reference frequency to drive the run-time counter is 40MHz. The 40MHz clock can be derived from the main clock and digital clock manager (DCM) can be used. In this paper, reference clock for run-time counter is derived from main clock using divider counter. The 40MHz reference frequency is chosen after characterizing the ring oscillators in 10 FPGA boards. The highest frequency of ring oscillators observed during characterization at room temperature is 34MHz. The 5MHz higher frequency than the ring oscillator frequency avoids the bit-flipping. The run-time counter always get overflow before the PUF-counter in the proposed PUF. Based on the challenge loaded, run-time counter will overflow before PUF-counter. The improvement observed in reliability of PUF CRPs in Table I in the proposed PUF is due to avoidance of bit-flipping. The PUF response in [5] is a concatenation of 3 bits from the central portion (7^{th}, 8^{th} and 9^{th}) of the 16-bit counter. The number of RO pairs used in [5] is 150 to 450, which is very huge and consume very large area in FPGA. In the proposed PUF, 32-bit response from 56-bit challenge is generated.

TABLE III
COMPARISON OF SECURITY METRICS OF PROPOSED PUF WITH PUF PROPOSED IN [8]

Sl.No.	Security Metrics	Ideal Value	PUF proposed in [5]	Proposed PUF
1	Uniqueness	50%	47.5%	45.2%
2	Reliability	100%	49%	89%
3	Uniformity	50%	39%	43%

IV. CONCLUSIONS

A RO based PUF providing more number of bits at PUF output with better security metrics is proposed in this paper. The RO-PUF suitable for FPGA selects the bits from the central portion of the counter which did not overflow. Instead of pair of ring oscillator, a single ring oscillator is used to pick up the required process variation. Counter running from a known standard clock source is used to stop the counter running on output of ring oscillator. Frequency of standard clock source is chosen higher than the frequency of ring oscillators to avoid bit flipping. The avoidance of bit-flipping will improve the reliability of the PUF CRPs. The overall security metrics shows that the proposed PUF topology is better than the earlier PUF designed using similar technique. The effect of temperature and supply voltage variation on reliability of PUF CRPs is our future work.

.

REFERENCES

[1] Charles Herder, Meng-Day Yu, Farinaz Koushanfar, Srinivas Devadas, "Physical Unclonable Functions and Applications: A Tutorial" Proceedings of the IEEE, Volume-102, 2014.

[2] G.E.Suh and S.Devadas, "Physical Unclonable Functions for device authentication and secret key generation," In Proc. of ACM/IEEE Design Automation Conference, pp. 9-14, 2007.

[3] B.Gassend, D.Clarke, et al "Silicon physical random functions," Proccedings of the ACM conference on computer and communications security, CCS-2002, ACM, New York,NY, USA, pp. 148-160.

[4] Ji-Liang Zhang,Gang Qu, et al "A Survey on Silicon PUFs and Recent Advances in Ring Oscillator PUFs," Journal of Computer Science and Technology, July 2014, Volume 29, Issue 4, pp 664–678.

[5] Filip Kodytek, et al "Improved Ring Oscillator PUF on FPGA and its properties," Journal of Microprocessor and Microsystems, Elsevier-2016.

[6] Abhranil Maiti, Vikash Gunreddy, Patrick Schaumont "A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions". IACR Cryptology ePrint Archive, 657, 2011.

[7] L. Bossuet , X.T. Ngo , Z. Cherif , V. Fischer , "A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon", Proceedings of the IEEE Transactions on Emerging Topics in Computing, 2014, pp. 30–36 .

[8] Filip Kodytek, et al "A design of ring oscillator based PUF on FPGA," IEEE 18th International Symposium on Design and Diagnostics of Electronic Circuits & Systems-2015.

[9] M.Bhusan et, al, "Ring oscillators for CMOS process tuning and variability control," IEEE Transactions on Semiconductor manufacturing, Feb-2006.