A Design of CMOS PUF Based on Ring Oscillator and Time-to-Digital Converter

Van-Phuc Hoang(✉), Quang Phuong Nguyen, Van Trung Nguyen, Thanh Trung Nguyen, and Xuan Nam Tran

Le Quy Don Technical University, 236 Hoang Quoc Viet, Hanoi, Vietnam
phuchv@lqdtu.edu.vn

Abstract. Physical unclonable functions (PUF) is a promising technique in the field of hardware security with the main principle based on the random variations of inherent semiconductor devices during the fabrication process to provide the secret keys for cryptography or IC identification/authentication. In this paper, we present a new, efficient design of CMOS PUF based on ring oscillators and a time-to-digital converter (TDC). The proposed PUF design provides higher number of respond bits for each challenge, better reliability and uniqueness compared with conventional RO PUF designs. The proposed PUF design is implemented with TSMC 180 nm CMOS process using Cadence Virtuoso tool. The detailed design, simulation and evaluation results are also presented and discussed. The experimental results have clarified the efficiency of the proposed PUF design.

Keywords: PUF · Ring oscillator · TDC

1 Introduction

The issue of information system security is becoming emerging, especially in the context toward the smart cities based on Internet of Things (IoT). Especially, in IoT systems, with huge number of resource constrained nodes, the security threat (in both hardware and software aspects) becomes critical. There have been many studies reporting the possibility to use hardware circuits and tools to collect the information illegally and attack the information systems. Moreover, integrated circuit (IC) fabrication technologies have developed quickly so that it could implement complicated algorithms and intelligent processing techniques, but also leads to the hardware security threats at any step of the IC design and fabrication flow. Besides, the issue of IC counterfeit is becoming emerging when the outsourcing is more and more popular in semiconductor industry today. Hence, the research topics on hardware security assurance for IoT systems are becoming emerging.

Physical unclonable functions (PUF) is a new technique in hardware security with the main principle based on the random variations of the inherent semiconductor devices during the IC fabrication process. A PUF is considered as the hardware implementation of a mathematical one-way function with the basic operating principle based on the

N.-S. Vo et al. (Eds.): INISCOM 2021, LNICST 379, pp. 233–242, 2021.
https://doi.org/10.1007/978-3-030-77424-0_19

relationship of challenge-respond pairs (CRPs) as shown in Fig. 1. PUFs can be used to provide the hardware based secret keys for cryptography applications by exploiting the random characteristics of PUFs. Moreover, a PUF provide an efficient means for IC identification/authentication since it can be considered as the fingerprint of the IC chip [1–4]. PUF is also a promising solutions for device authentication in IoT systems with resource constrained nodes.

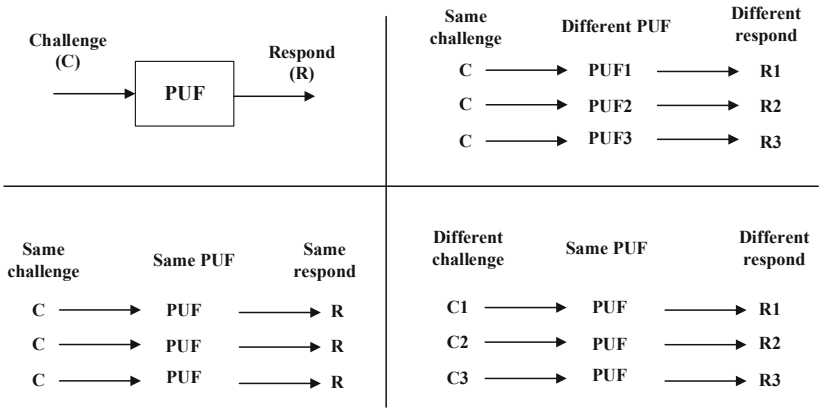

Fig. 1. Basic operating principle of PUFs based on CRPs.

Among number of PUF design structures, Ring Oscillator (RO) based PUFs provide an efficient tool for the issue of IC counterfeit in semiconductor industry [5]. RO PUF utilizes the difference in the frequencies of two identical ROs. One of the disadvantages of RO PUF is that it requires very larger hardware resources to provide enough CRPs for key extraction applications. Hence, there have been many papers presenting RO based PUF designs with the solutions to maximize the number of challenge-respond pairs (CRPs) which can be extracted. However, there are very few papers aiming to provide minimal number of extracted bits per challenge while remaining the PUF performance [5]. Moreover, there is not any paper mentioning the use of TDCs for RO based PUFs.

Therefore, in this paper, we aim to propose a new RO PUF design using a time-to-digital converter (TDC) to improve the CRPs and number of bits for each challenge. With n ROs used, the maximum number of CPRs is 2 C_2^n and the respond bit number depends on the frequency or the number of RO stages used. The proposed PUF design is implemented with TSMC 180 nm CMOS process using Cadence Virtuoso tool.

The rest of this paper is organized as follows. The conventional RO based PUF designs and related works are described in Sect. 2. In Sect. 3, we will introduce the proposed TDC based RO PUF and its operation principle. Then, in Sect. 4, we present the implementation results of the proposed PUF design and compare with previous ones. Finally, the paper is concluded in Sect. 5.

2 Conventional RO Based PUF Designs and Related Works

Firstly, we consider the operating principle of the ROs. When an even number of inverters are connected in series with suitable initial condition (such as active enable signal), the output of the RO will provide one signal with a specific frequency. The RO PUF utilizes the special characteristics that the frequencies of the ROs with identical layout are random but with static differences which are caused by the variations in the semiconductor fabrication process. The output of RO PUF is created by comparing the frequencies of the RO pair [5]. A conventional RO Based PUF structure is presented in Fig. 2 in which the frequencies of a random pair of oscillators are selected by the challenge input (C). Due to the random variations in the IC fabrication process, the frequencies of this pair are different and they are compared so that one output bit is generated (as the respond, or R) to show their relationship (smaller or greater) [4]. The signed function style of this method causes the information lost and requires a large number of ROs to extract the reliable and unique chip identification information. In addition, the fluctuation in absolute RO frequencies caused by operating conditions and other sources make this conventional scheme not practical.

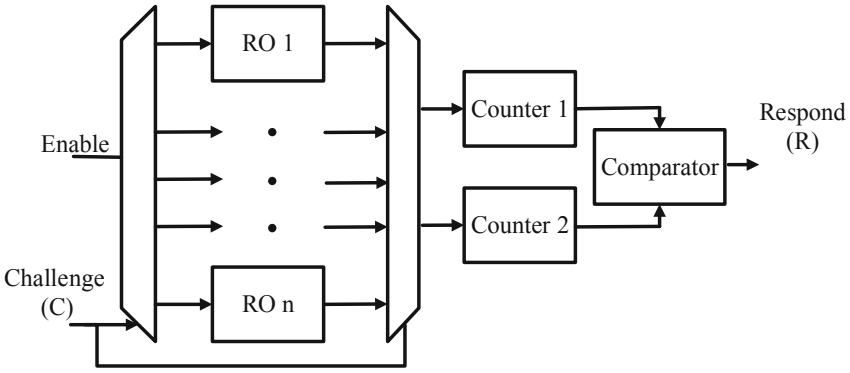

Fig. 2. Traditional RO PUF architecture.

Many works have been carried out to improve the conventional RO PUF by two main directions. The first direction is to increase the flexibility in RO PUF hardware configurations, so equivalent to retrieve more RO pairs (ROp), and the second direction is to improve data processing technique to enhance the efficiency of RO PUF data extraction. Authors in [5] proposed the configurable FPGA-based RO PUFs that allow the inverters to be flexibly selected by a multiplexer (Fig. 2). Accordingly, a N stage ROs could be configured to generate 2^N different frequencies. Gao *et al.* in [6] proposed a similar structure, where the number of stage inverters can be adjusted by multiplexer. Therefore, metastable outputs can be avoided. Moreover, C. Gu et al. from Queen's University Belfast proposed and evaluated the efficiency of two PUF design types based on ring oscillator (RO) and PicoPUF including 127 Xilinx Artix-7 28 nm FPGA boards [7]. Moreover, our research team has successfully developed an FPGA based PUF design using ring oscillator and proposed a new ID extraction scheme for IC with the proposed

RO PUF. The proposed ID extraction scheme in FPGA has fully employed the local variations independent with the fabrication technology [8].

Authors in [9] produced longer PUF output using less ROs by latching the counter value in Gray code of slower RO (Fig. 2) of each pair. The disadvantage of this method locates in the complexity of data processing caused by choosing the significant bit string locations. In general, these designs lead to the high complexity in the circuit layout caused by the integration of many multiplexers so maintaining the layout symmetry and regularity is especially challenging. In addition, the evaluation methods in those works follow the conventional way as described in [6]. On the other hand, J. Agustin et al. [10] proposed a RO PUF exploiting the variability of the duty cycle instead of measuring deviations of the output frequency so that the number of ROs needed to implement a robust PUF is decreased.

It can be seen that one disadvantage of the conventional RO PUF designs is the small number of respond bits. Hence, it needs to be replicated to provide high key length in modern cryptographic applications, such as AES, so that the circuit complexity becomes very high. Besides, the number of independent CRPs is very low. As mentioned above, the previous papers focus on improving the maximum number of independent CRPs which can be extracted from one challenge. There are very few papers concerning the issue of respond bit number for each challenge [5]. Hence, in the next part of this paper, we will introduce a new technique of TDC based RO PUF to solve this issue.

3 Proposed TDC Based RO PUF

In this section, we describe the proposed PUF based on ROs and TDC. It is well known that a TDC converts each time period to a digital word. Our proposed idea of using TDC for RO PUF, as shown in Fig. 2, is based on the time characteristics of RO PUFs. In this PUF design, the MUXs are used separately and ROs are configured by K scaling method [7]. Instead of using an edge counter, the proposed structure employs the TDCs to convert the delay time of two oscillators to digital words. The CRP in the proposed TDC based RO PUF is composed by the pair (C_1, C_2/R) where C_1 and C_2 are the MUX selecting signals enabling two stages to work among n oscillator stages. The use of the synchronous DEMUX and MUX signals in this RO PUF approach helps to reduce the power consumption since only two ROs work among n oscillator stages. The first stage with the minimal duty cycle is used as the comparator.

Due to the random variations in the IC fabrication process, the frequency and duty cycles of two outputs o_1 and o_2 (at two MUXs) are not the same. Basically, a TDC works properly if the Start signal arrives before the Stop signal [11]. Hence, two TDCs are required with the crossed connection as shown in Fig. 3. These TDCs work sequentially to measure the delay time values of o_1 and o_2 signals controlled by RESET signal (at '0' value). The bit sequence at the TDC output is encoded into the binary format by a tree encoder [12], then passed through the binary subtractor to provide the respond sequence R. In this proposed RO PUF, the TDC with Vernier delay line structure is used as shown in Fig. 4 [11]. This structure includes N stages in which each stage comprises of two delay units (τ_1, τ_2) and one D-FF. With this operation principle, the resolution of the TDC is LSB $= \tau_1 - \tau_2$.

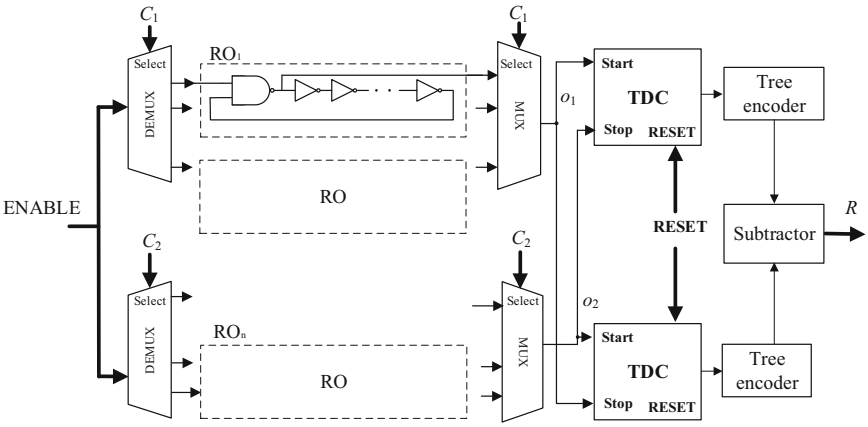

Fig. 3. Proposed TDC RO PUF structure.

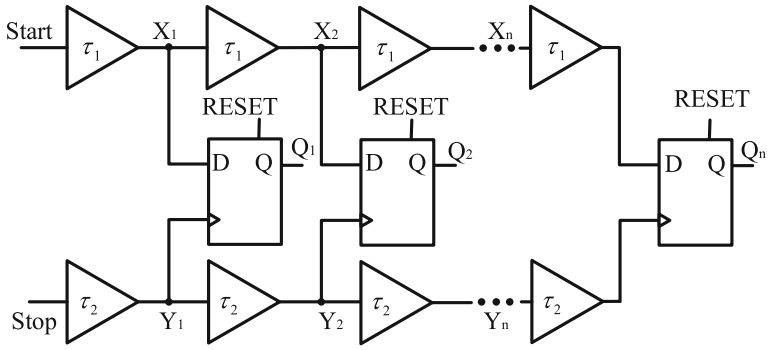

Fig. 4. TDC with Vernier delay line structure.

Figure 5 illustrates the operation principle of the TDC with Vernier delay line structure. The Start and Stop signals are fed to the D and Clock inputs of the D-FF element. Both signals are then propagated through each stage of this TDC provided that the condition of ($\tau_1 > \tau_2$) is satisfied. Hence, after each stage, the Start signal tends to be in-phase with the Stop signal. If its phase is lower, the value of the output D is '1'. Otherwise, the output value becomes '0'.

In this design, the Vernier TDC output is in the form of the thermometer code. It can be converted into the binary format (such as in Gray or ordinary binary form) by the tree encoder [9]. This tree encoder converts from the 2^k bit thermometer code to the k-bit binary format.

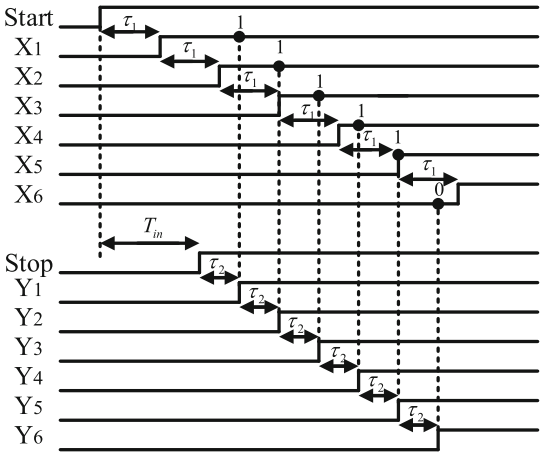

Fig. 5. Operation of the TDC with Vernier delay line structure.

Figure 6 presents the RESET signal generation circuit in which the truth table of the logic function block is presented in Table 1. Figure 7 depicts the simulated waveform of RESET signal generated by the circuit in Fig. 6. By employing the adaptive RESET signal generator, the PUF outputs are extracted with high level of the stability.

Table 1. Truth table of the logic function block used in the adaptive RESET signal generation circuit.

Input	Output
0..000	0
0..001	1
…	…
1..110	1
1..111	0

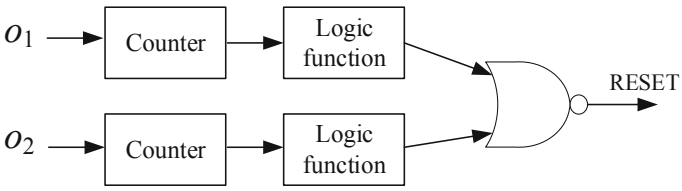

Fig. 6. Adaptive RESET signal generation circuit.

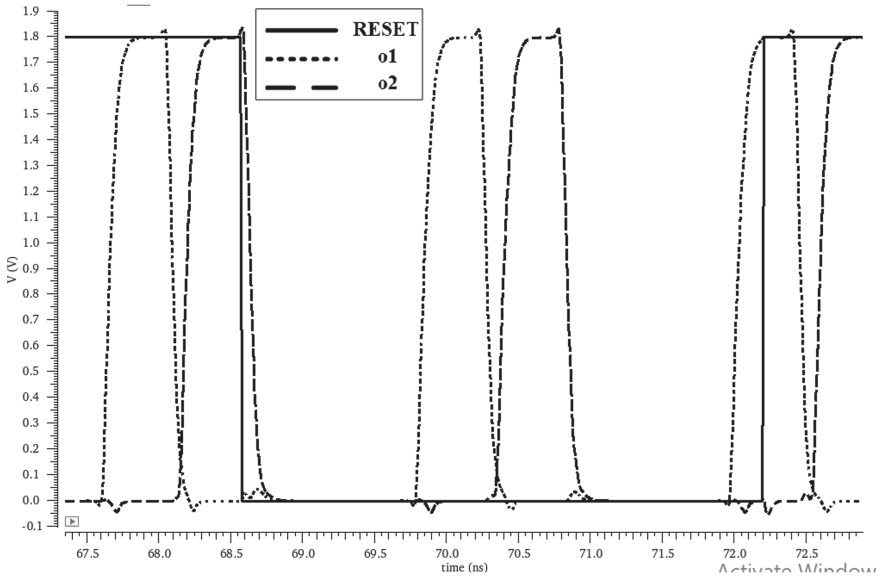

Fig. 7. Simulated waveform of RESET signal.

4 Implementation Results

In this section, we evaluate the performance of the proposed TDC based RO PUF with $K = 5$ and implemented with TSMC 180 nm CMOS process. The PUF output is extracted by Cadence Virtuoso tool, then processed by Matlab software to provide the performance evaluation metrics. In this work, we use two performance metrics including uniqueness and reliability for the proposed and previous PUF designs.

For the uniqueness, when the same challenge sets are given to different PUFs, the PUF outputs should be different. In other words, the uniqueness indicates how different the generated IDs are among the devices with PUF designs. Specifically, the uniqueness is calculated by the different bits in the respond (R) generated by different PUFs with the same C input and evaluated by the mean Hamming distance (HD) of R values. With k different PUFs having the n-bit respond, the uniqueness is expressed as:

$$\textbf{Uniqueness} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \tag{1}$$

Monte Carlo simulation is used with device mismatch models based on (1) at typical temperature condition (25 °C). As a results, the uniqueness of the proposed PUF design is 48.56%. Moreover, the reliability evaluates the stability of the PUF respond under variations of different parameters including temperature, supply voltage and device aging. If the PUF_i generates an n-bit respond (R_i) at the normal condition, it also generates the respond R_i' at different conditions. We perform this measurement m times with one

PUF for one challenge C and the reliability can be evaluated as:

$$\textbf{Reliability} = 1 - \frac{1}{m}\sum_{t=1}^{m}\frac{HD(R_i, R_{i,t}^{'})}{n} \tag{2}$$

We have performed the Monte Carlo simulation with different design corners and temperature in the range of (25, 35, 45, 55, 65) °C. Figure 8 shows the output waveform of the proposed TDC based PUF with the 4-bit respond by Monte Carlo simulation. Moreover, Table 2 shows the experiment results of the proposed PUF compared with other RO PUF designs. It can be seen that the proposed TDC based RO PUF achieves higher value of the uniqueness with an acceptable value of the reliability. The challenge bit C selects 2 among n RO stages randomly, hence the number of CRPs in the proposed TDC based RO PUF is C_2^n. By using C_1 independent with C_2 for selecting the first and second RO stages, combined with a full binary subtractor, the higher number of CRPs can be provided as above. With the achieved results, the proposed PUF design shows its high potential for the application in data encryption using symmetrical algorithms such as the Advanced Encryption Standard (AES) [13]. However, for authentication applications, more improvements are required so that they becomes the topics for our future works.

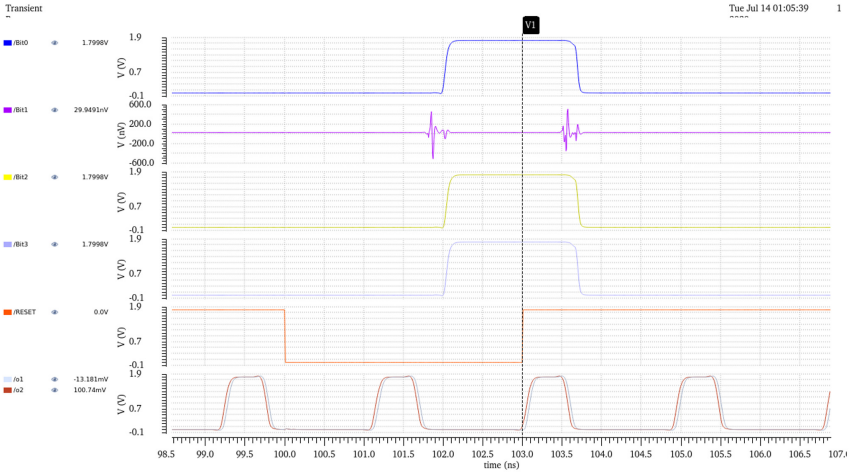

Fig. 8. Output waveform of proposed TDC based PUF with Monte Carlo simulation.

Table 2. Comparison with other RO PUF designs.

Parameter	Number of CRPs	Number of generated bits per challenge	Uniqueness (%)	Reliability (%)
Idea value	2^n	n	50	100
[4]	$\frac{n}{8}$	1	46.15	99.52
[9]	$n-1$	1	47.31	99.14
Proposed PUF	$2 \times C_2^n$	4	48.56	96.56

5 Conclusion

In this paper, we have presented a new, efficient design of CMOS PUF based on the ring oscillators and a time-to-digital converter. The proposed PUF design provides more respond bits for each challenge, higher reliability and uniqueness compared with other works. The proposed PUF design is implemented with TSMC 180 nm CMOS process using Cadence Virtuoso tool. The detail design, simulation and evaluation results are also presented and discussed. The implementation results have clarified the efficiency of the proposed PUF design. In the future work, we will propose other methods to increase the respond bit-width, complete the layout design for the proposed PUF and perform the comprehensive PUF evaluation analysis. Moreover, the applications of the proposed PUF design in the authentication and data encryption will be considered in our future work.

Acknowledgment. This research is funded by Vietnam National Foundation for Science and Technology Development (NAFOSTED) under grant number 102.02–2020.14.

References

1. Halak, B.: Physically Unclonable Functions: From Basic Design Principles to Advanced Hardware Security Applications, 1st edn. Springer (2018). https://doi.org/10.1007/978-3-319-76804-5
2. Herder, C., et al.: Physical unclonable functions and applications: a tutorial. Proc. IEEE **102**(8), 1126–1141 (2014)
3. Rührmair, U., Holcomb, D.E.: PUFs at a glance. In: 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, pp. 1–6 (2014)
4. Suh, G.E., Devadas, S.: Physical unclonable functions for device authentication and secret key generation. In: Proceedings of 44th ACM/IEEE Design Automation Conference (DAC), pp. 9–14, June 2007
5. Delavar, M., et al.: A ring oscillator-based PUF with enhanced challenge-response Pairs. Can. J. Electr. Comput. Eng **39**(2), 174–180 (2016)
6. Gao, M., Lai, K., Qu, G.: A highly flexible ring oscillator PUF. In: Proceedings of the 51st Annual Design Automation Conference. ACM (2014)
7. Gu, C., Chang, C.H., Liu, W., Hanley, N., Miskelly, J., O'Neill, M.: A large scale comprehensive evaluation of single-slice ring oscillator and PicoPUF Bit cells on 28 nm Xilinx FPGAs. In: IEEE Workshop on Attacks and Solutions in Hardware Security (ASHES), pp.1–6 (2019)

8. Tran, V.-T., Trinh, Q.-K., Hoang, V.-P.: Enhanced ID authentication scheme using FPGA-based ring oscillator PUF. In: 2019 IEEE 13th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC), Singapore, pp. 320–327 (2019)
9. Kodýtek, F., Lórencz, R., Buček, J.: Improved ring oscillator PUF on FPGA and its properties. Microprocess. Microsyst. **47**, 55–63 (2016)
10. Agustin, J., Lopez-Vallejo, M.L.: A temperature-independent PUF with a configurable duty cycle of CMOS ring oscillators. In: 2016 IEEE International Symposium on Circuits and Systems (ISCAS), Montreal, QC, pp. 2471–2474 (2016)
11. Henzler, S.: Time-to-Digital Converters, Springer (2010). https://doi.org/10.1007/978-90-481-8628-0_2
12. Madhumati, G.L., Rao, K.R., Madhavilatha, M.: Comparison of 5-bit thermometer-to-binary decoders in 1.8 V, 0.18 μm CMOS technology for flash ADCs. In: 2009 International Conference on Signal Processing Systems, Singapore, pp. 516–520 (2009)
13. Phan, T., Hoang, V., Dao, V.: An efficient FPGA implementation of AES-CCM authenticated encryption IP core. In: 2016 3rd National Foundation for Science and Technology Development Conference on Information and Computer Science (NICS), pp. 202–205 (2016)