Journal of Engineering and Applied Sciences 11 (4): 805-809, 2016
ISSN: 1816-949X

Improving Reliability of Physically Unclonable Function Using Error Correcting Code

Nima Ali Mohammadi and Shahriar B. Shokouhi
Faculty of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran

Abstract: Physically Unclonable Function (PUF) is a promising solution to satisfy hardware security demands. Several structures have been proposed to generate a unique and unclonable key from a silicon chip. Delay-based and Memory-based PUFs are the most popular FPGA implementation of a PUF construction. In thisstudy we implement Anderson PUF, RO PUF and SR Latch PUF on several FPGA platforms and perform an analysis on their performance metrics such as Reliability, Uniqueness and Bit-aliasing. Changes in temperature and supply voltage can affect reliability of PUF. Since a noiseless key is required in applications such as secret key generation, a new Error Correcting Code (ECC) is presented to address this issue.

Key words: Physically unclonable functions, ECC, reliability, hardware security, bit-aliasing

INTRODUCTION

The demand for more security to resist against physical attacks is becoming more popular these days (Zhang *et al*., 2015). Different types of cryptographic algorithms have been proposed in which most of them use stored cryptographic keys. These keys are mostly saved in a non-volatile memory that can be accessed by attackers (Suh and Devadas, 2007). Traditionally tamper-proof devices have been used to address this problem which is very expensive and power consuming solution. Physically Unclonable Function (PUF) is a new approach to solve these problems (Merli *et al*., 2010). Cryptographic Key Generation, Hardware Identification and intellectual property protection are the most common application for PUFs which are based on chip unique Challenge-Response Pair (CRP) function of a PUF (Maiti *et al*., 2012).

Because of we do not have complete control in manufacturing process of a silicon chip, it is nearly impossible to clone PUFs therefore they are unique from one chip to another in the same manufacturing condition (Maiti *et al*., 2013). These complex inherent variations can be used to create and generate a key instead of saving the key in a memory.

In secret key generation application, the generated key must be noiseless and stay stable at different times and under different conditions. But PUFs responses change with changing operation temperature and supply voltage. Even aging will affect PUF responses (Maiti and Schaumont, 2014). To satisfy the need of noiseless key, error correcting schemes have been introduced. In conventional approach, BCH codes have been used. In the other hand, neural networks are known for their ability in data processing that can be used in pattern recognition. We take these advantages to use neural network based error correcting for secret key generation.

MATERIALS AND METHODS

Physically unclonable function: As mentioned before Delay-based and Memory-based PUFs are main FPGA implementation of a PUF construction (Maiti *et al*., 2014). In thisstudy three structures has been selected from these types Anderson and RO.

Glitch PUF is one of the delay-based PUF. Anderson proposes a glitch-based PUF construction specifically for FPGA platforms (Anderson, 2010). The random glitches on the output of the circuit can be converted into unique and random response bits. Figure 1 shows the structure of Anderson PUF.

The RO PUF is a delay-based PUF (Suh and Devadas, 2007). It has been experimentally proved that RO

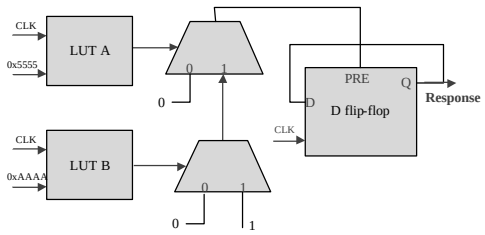

Fig. 1: Anderson PUF

Corresponding Author: Nima Ali Mohammadi, Faculty of Electrical Engineering, Iran University of Science and Technology, Tehran, Iran

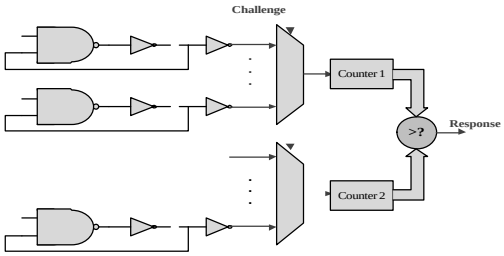

Fig. 2: RO PUF

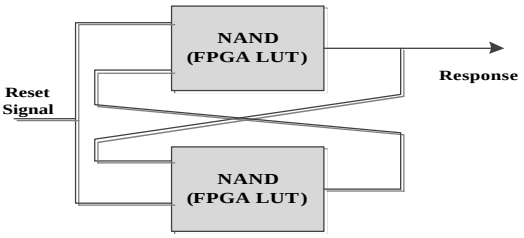

Fig. 3: SR Latch PUF

PUF has advantages over the other delay-based PUFs (Yu *et al*., 2011). In an RO PUF, two ring oscillators with exactly identical layout create two clocks. Due to process variations the frequency of these ring oscillators are not equal. Therefore, this frequency difference can be compared to produce a bit of response. As shown in Fig. 2, an RO PUF consists of n completely identical ring oscillators, two multiplexer, two counters and a comparator. Each challenge selects two ring oscillators and the two counters will start to count and measure the frequency of each ring oscillator. Then, the outputs of the counters are compared and response bit will be generated. SR Latch PUF is a memory-based PUF which has certain practical benefits over other memory-based PUFs while being implemented on FPGA (Maes *et al*., 2008). The main idea behind these kinds of PUFs is to force a bi-stable memory to go into its unstable state where because of process variations the return state cannot be predicted (Maes, 2013). Figure 3 shows a NAND-based SR latch PUF which produce one bit of response. By asserting a reset signal, we force the SR Latch into its unstable state and when released based on random mismatch between internal cross-coupled NAND gates, the response bit will be create.

RESULTS AND DISCUSSION

In this study we implement RO and SR Latch PUF with response length of 128 bits. Responses are evaluated using Xilinx Spartan XC3S400 development board. Reliability, uniqueness and Bit-aliasing are the main quality metrics which show performance of a PUF (Maiti *et al*., 2012). Reliability of a PUF means how much the response bits are stable and fixed over times and under different environmental conditions (Maes *et al*., 2008). Ideally PUF must produce the same response to a given challenge with environmental changes. Therefore, the reliability of an ideal PUF is 100% and it is defined as follows:

$$\text{Reliability} = 1 - \frac{2}{m \times (m-1)} \sum_{i=1}^{m-1} \sum_{j=i+1}^{m} \frac{HD(r_i, r_j)}{a} \times 100\% \quad (1)$$

Where:

HD = The Hamming distance between two responses

r_i and r_j = A is the number of response bits (128 in our study)

m = The total number of data points

Uniqueness of a PUF is also an important parameter that shows the randomness of a PUF. In other words, two identical PUF must produce different responses to the same challenge (Cao *et al*., 2015). Ideally this value should be 50%. For g instances of PUF the study uses the following formula to evaluate the uniqueness of PUFs:

$$\text{Uniqueness} = \frac{2}{g \times (g-1)} \sum_{i=1}^{g-1} \sum_{j=i+1}^{g} \frac{HD(r_i, r_j)}{a} \times 100\% \quad (2)$$

Another quality factor of a PUF which show the randomness of the PUF response is bit-aliasing. Bit-aliasing of a given bit position in the PUF response is its percentage Hamming Weight (HW) across several PUF instances. Again, this value should be ideally 50% for all response bit positions and it is calculated as:

$$\text{Bit} - \text{aliasing} = \frac{1}{g} \sum_{i=1}^{g} r_{i,j} \quad (3)$$

The effect of environmental temperature on reliability of PUF structures is shown in Fig. 4. As mentioned previously, uniqueness is one of the most important factors of a PUF. This value ideally should be 50%.

In Fig. 5-7, the distribution histogram of the Hamming distance between three structures are compared as well. In the best case, a PUF would have a normal distribution with the mean value of 0.5 and in our study, we have 128 bits of response. Thus, the peak of distribution must occur in the range of [61:65]. It can be observed that the mean value of the RO PUF is closer to the center. It shows that the RO PUF has a better performance in term of randomness.

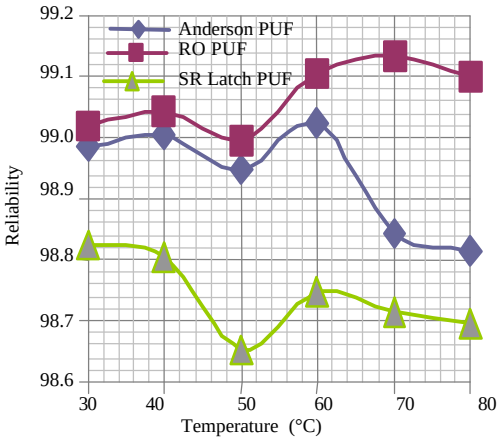

Fig. 4: The effect of the ambient temperature on the reliability

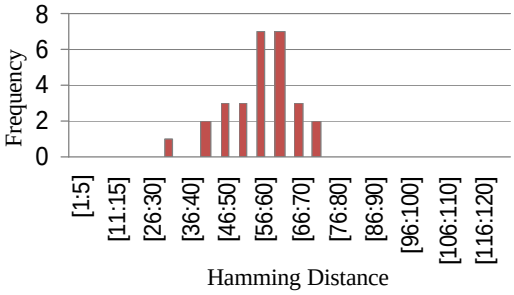

Fig. 5: Uniqueness of the Anderson PUF

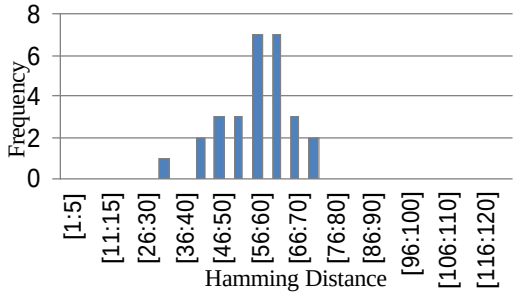

Fig. 6: Uniqueness of the RO PUF

As shown in Fig. 4, changing ambient temperature will affect the reliability of PUF. Variation in chip supply voltage and aging may also cause the response bits to flip for an identical challenge. Figure 8 presents a comparison of bit-aliasing between different implemented structures. As mentioned before in an ideal condition this value should be 50%.

Error correcting code: Conventionally BCH or other classical codes have been used for correcting PUF

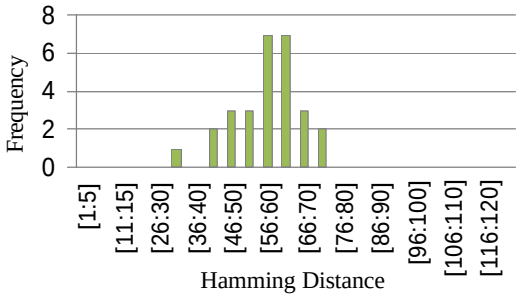

Fig. 7: Uniqueness of the SR Latch PUF

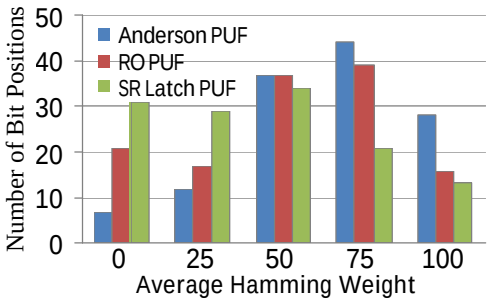

Fig. 8: Comparison between different schemes in terms of bit-aliasing

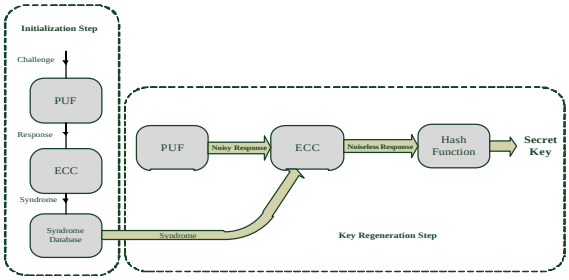

Fig. 9: Different phases of error correction process

responses (Yu and Devadas, 2010). One of the main problems in BCH codes is its complex computations. When BCH codes are being used as multiple error correction code, the amount of calculation will be increased by the growth of error bits (Wallace, 2010). An error correcting scheme is proposed using neural networks.

The error correcting process is done in two stages. In the first step, the produced responses are applied to the network for calculating the weight matrix. This step is the learning phase. In the next step, a noisy response is applied to the network and it will regenerate the key using the calculated weight matrix. Figure 9 presents the basic block diagram of the mentioned steps. Hopfield and auto-associative networks have been tested using MATLAB Software with several 128 bits lengths

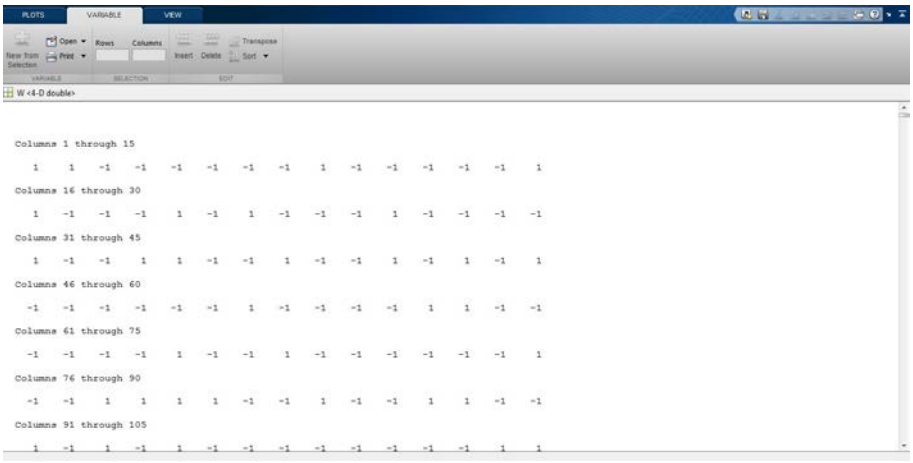

Fig. 10: MATLAB simulation of the error correcting code

Table 1: Quality metrics for three implemented PUFs

PUF	Reliability	Uniqueness
Anderson	98.987	40.004
RO PUF	99.019	39.883
SR Latch PUF	98.823	36.264

responses. Both networks are able to correct the noisy keys and successfully regenerate noiseless responses. The results show that Auto-associative memory is faster and more stable than Hopfield network. Comparing to the conventional error correction coding, the main advantage of using neural networks is that unlike the conventional ECC like BCH codes, no information about the challenge-response pairs is revealed from the syndromes (in this case, the weight matrix) shown in Table 1. Another advantage of neural network is its low computational complexity that speeds up the error correcting process. In Fig. 10 weight matrix has been calculated using MATLAB Software.

CONCLUSION

Anderson PUF, RO PUF and SR Latch PUF are implemented on several Xilinx Spartan XC3S400 and we compare the performance of both structures in terms of reliability, uniqueness and Bit-aliasing. Results show that RO PUF has a better performance in every aspect but SR Latch PUF has less area consumption. Because PUF responses will be affected with changing temperature and supply voltage we present an error correcting code to address this issue. The proposed model is based on neural networks that can be used as an error correcting scheme which generate secure syndrome and also have computing advantages over traditional solutions like BCH.

REFERENCES

Anderson, J.H., 2010. A PUF design for secure FPGA-based embedded systems. Proceedings of the Asia and South Pacific Design Automation Conference, January 18-21, 2010, Taiwan, pp: 1-6.

Cao, Y., L. Zhang, C.H. Chang and S. Chen, 2015. A low-power hybrid RO PUF with improved thermal stability for lightweight applications. IEEE Trans. Comput. Aided Design Integrated Circ. Syst., 34: 1143-1147.

Haykin, S.S., 1994. Neural Networks: A Comprehensive Foundation. MacMillan Publishing, New York, ISBN: 9780023527616, Pages: 696.

Maes, R., 2013. Physically Unclonable Functions Constructions, Properties and Applications. Springer Science and Business Media, New York, ISBN: 9783642413957, Pages: 193.

Maes, R., P. Tuyls and I. Verbauwhede, 2008. Intrinsic PUFs from flip-flops on reconfigurable devices. Proceedings of the 3rd Benelux Workshop on Information and System Security, Volume 17, November 13-14, 2008, Eindhoven -.

Maiti, A. and P. Schaumont, 2014. The impact of aging on a physical unclonable function. IEEE Trans. Very Large Scale Integration (VLSI) Syst., 22: 1854-1864.

Maiti, A., I. Kim and P. Schaumont, 2012. A robust physical unclonable function with enhanced challenge-response set. IEEE Trans. Inform. Forensics Secur., 7: 333-345.

Maiti, A., V. Gunreddy and P. Schaumont, 2013. A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions. In: Embedded Systems Design with FPGAs, Athanas, P., D. Pnevmatikatos and N. Sklavos (Eds.). Springer, New York, pp: 245-267.

Merli, D., F. Stumpf and C. Eckert, 2010. Improving the quality of ring oscillator PUFs on FPGAs. Proceedings of the 5th Workshop on Embedded Systems Security, October 28, 2010, Scottsdale, AZ. -.

Suh, G.E. and S. Devadas, 2007. Physical unclonable functions for device authentication and secret key generation. Proceedings of the 44th annual Design Automation Conference, June 4-8, 2007, San Diego, CA., pp: 9-14.

Wallace, H., 2010. Error detection and correction using BCH codes. Atlantic Quality and Design.

Yu, S. and S. Devadas, 2010. Secure and robust error correction for physical unclonable function. Secure and Robust Error Correction for Physical Unclonable Function, pp: 48-65.

Yu, S., M. Raihi, R. Sowell and S. Devadas, 2011. Lightweight and secure PUF key storage using limits of machine programming. Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, September 28-October 1, 2011, Nara, Japan.

Zhang, J., Y. Lin, Y. Lyu and G. Qu, 2015. A PUF-FSM binding scheme for FPGA IP protection and pay-per-device licensing. IEEE Trans. Inform. Forensics Secur., 10: 1137-1150.