Recent Developments in Electronics and Communication Systems
KVS Ramachandra Murthy et al. (Eds.)

doi:10.3233/ATDE221237

Designing a Strong Physically Unclonable Function Using Low Power LFSR

BVDN. Srilakshmi[1,a)], Kiran Mannem [2,b)] , K. Jamal[3,c)], Manchalla.O.V.P. Kumar[4,d)]
[1]M.Tech Scholar, [1]Department of ECE, GRIET, Hyderabad, India.
[234]Department of ECE, GRIET, Hyderabad, India.
[a)]srilakshmi.bvdn@gmail.com
[b)] kiranmannem14@gmail.com
[c)] kjamal24@gmail.com
[d)]pavanomkar81@gmail.com

Abstract. In this new era, security is being the major concern in day to day life. To secure the data many security models are been introduced. Advanced Encryption Systems such as encryption, decryption methods are having a drawback, that it uses a key to store the data in its devices. The key can be easily cloned by any 3rd party person and there is a chance of losing data and the device security. PUF (Physically Unclonable Function) is mainly used for device authentication. It helps to identify the data and its device while performing authentication process. In front-end the PUF is used for device authentication where as in back-end LFSR(Linear-Feedback-Shift-Register) is used to generate random numbers which helps to increase more security. Previously the PUF based LFSR is been implemented and observed the results. In this project the PUF is implemented using LP LFSR (Low power Linear Feedback Shift Register) in order to show more improvement in terms of security by increasing the randomness.

Keywords: Switching activity, LFSR (Linear Feedback Shift Register), Security, Randomness.

1. Introduction

In our daily life telecommunication systems such as mobile phones and embedded system-based devices are playing a crucial role [1]. Each and every task of these devices should be securely authenticated. The sensitive information between end to end user should be handle with care. The user can securely able to store the data. In-fact, electronic gadgets are playing a major role in performing transactions and also acts as a security primitive for storing the users data. The processing of information is enabled through flexibility of software [2]. However, there exists certain problems related to security. To avoid such problems, they came up with the solution named as EEPROM and SRAM. These memories contain security-based keys in It [3]. But there is a threat that the keys can be easily grabbed or cloned.PUF's (Physical unclonable functions) are the innovative security primitive which is utilized for authentication as well as storage of secret information without the requirement of EEPROMs or any other hardware which is described above. PUF is an alternative solution for storing secret information in digital memory. It works according to its physical characteristics of that particular IC [4][5]. It

consumes less area and power when compared to SRAM/EEPROM [6]. The IC should be enabled since the process of encryption is based on chip [7][8].

2. Literature Survey

Kumar,G.S., Saminadan,V have proposed an approach using low power LFSR with 3 ring oscillators along with the concept of fuzzy logic. By using this new version of LFSR, the power consumption got reduced while generating a test pattern. In order to test the circuits BIST(Built-in-self-test) are used. Since Reduction of power is the major requirement in test circuits and design circuits, Low power LFSR helps to achieve great reduction of power. In this project the power got reduced up to 4.5% when compared with existing designs.

Shaer,L., Sakakini,T., Kanj,R., Chehab,A., and Kayssi A, have proposed a design which is efficient in producing more randomness at the output. This design also helps to reduce the power consumption. As the randomness increased at the output there is a great improvement in terms of security. Many techniques are also used to reduce the power. The proposed design is implemented using H-spice tool. Less energy consumption with good security improvement are shown in simulation results.

Kitsos P., Sklavos N., Zervas N, and Koufopavlou o., have proposed a less power LFSR for blue-tooth communication. Simple techniques were also used to reconfigure LFSR. Two methods were also introduced in order to reduce the switching activity of conventional LFSR. Clock gating and gray code representation are 2 types of techniques which help to reduce the power consumption. Advanced encryption /decryption process are also used to widen the bit length.

Brazzarola, M., and Fummi F, have analyzed new characteristics related to power consumption of Built in self-test design connected to circuit under test of combinational circuit. The LFSR is designed using primitive polynomial. Testing play a major role in case of every design. Now a days BIST is been popular for testing. It is embedded in circuits for testing purpose. But there exists an issue related to power consumption. This can be controlled by test pattern which increase more switching activity to reduce power consumption.

3. Background and Related Works

In the present situation security is playing a major role in everyone's life. The device security and data security are being so important. To achieve the best security PUF (Physically Unclonable Function) helps to identify the response and its device while authentication process. PUF's are of various types. It got categorized into two types analog and digital. In analog PUF's. The digital PUF's are of two types they are delay based PUF and memory based PUF. Delay based PUF's are again sub divided into two types such as ring oscillator based PUF and arbiter PUF. Ring Oscillator PUF is a simple PUF circuit, it vibrates at a particular frequency. It helps to produce 0's and 1's by differentiating the frequencies of 2 similar Ring Oscillator circuits. Arbitrary PUF is another type of delay based PUF. It helps to create strong PUF models.

3.1 Introduction to Low Power LFSR

Here in this section let us discuss about Low power LFSR, its operation and how it is used to improve more security. It has great switching activity which increases the randomness. The architecture of Low power LFSR is shown below:

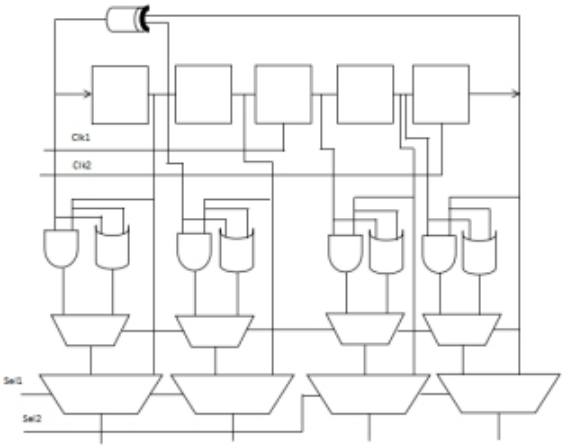

Figure 1. Basic structure of Low power LFSR

The above Figure 1 represents the basic structure of Low power LFSR. It is of 4 bit, so it contains 2 D flip-flops on either side. The middle flip-flop represents the dummy flip-flop which is used to connect the 4 flip flops. It is also called as "Bipartite circuit". To each flip-flop an RI (Random Injection) circuit is connected. The RI circuit consists of AND gate and OR gate both connected to the multiplexer which can be seen in the figure.

3.2 Concept of PUF based LFSR

Physically Unclonable Function (PUF) based LFSR is used as a security primitive device. It helps to identify the output response coming out from a particular device. It's working mainly depends upon features such as flexibility, reliability and randomness. The architecture of PUF based LFSR is given below.

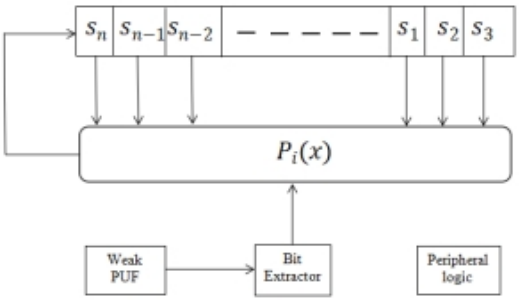

Figure 2. PUF based LFSR

The above Figure 2 is the architecture of PUF based LFSR. The output of weak PUF is given to the Bit extractor which of 1-bit response. The output of bit extractor is given to Pi(x), where Pi(x) is the array of PUF responses. The Pi(x) is given as a feedback response to the basic LFSR. Finally, the random numbers are being generated.

3.3 Existing Design

The existing design is of 16-bit LFSR based PUF.The architecture of existing design is shown below:

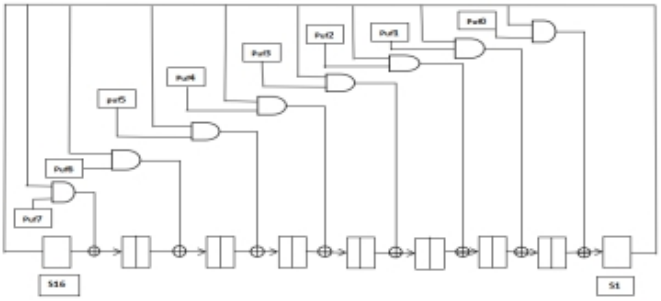

Figure 3. Existing 16 Bit LFSR Based PUF

The above Figure 3 shows the existing 16 bit LFSR based PUF. In the existing design the PUF is designed and connected to the shift registers through AND gate. In order to reduce area, shift registers are divided into two in the middle sections and are connected with the help of xor gates.

3.4 Proposed Design

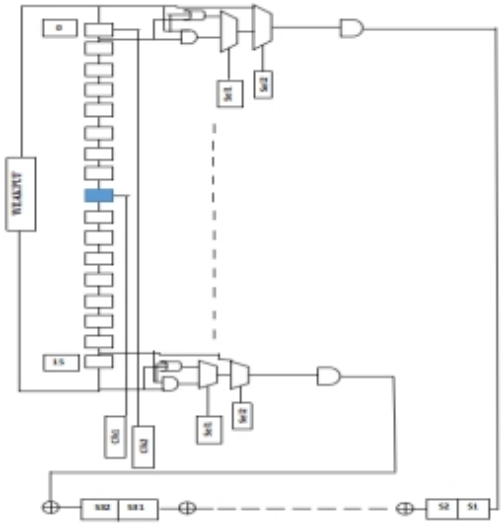

Figure 4. Proposed 32 Bit Low Power LFSR based PUF

The above Figure 4 represents the proposed 32-bit Low power LFSR based PUF. Here the weak PUF is connected as a feedback to the low power LFSR. The weak PUF is of 16 bit. This 16-bit PUF is connected to 32-bit LFSR. The 32-bit LFSR is taken as a pair of shift registers to reduce the area of the circuit. Thus, the weak PUF is connected to these 16 xor gates. The output produced is of 32 bit from each shift register of the pair.

4. Results and Discussion

In this section, the simulation results, comparisons between randomness, power, area and delay of existing and the proposed structures will be discussed.

4.1 Simulation Results of Existing and Proposed Design

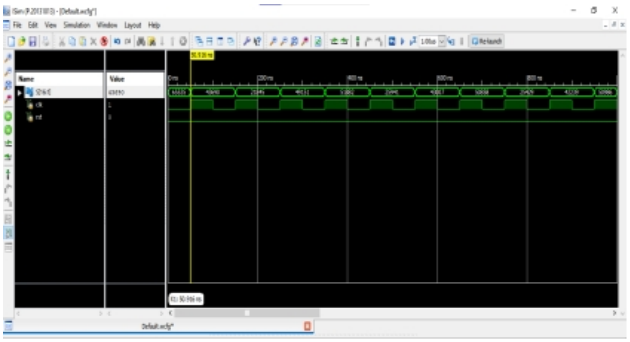

Figure 5. Simulation results of Existing 16-bit PUF Based LFSR

The above Figure 5 represents the simulation results of 16 Bit PUF. It shows that for every 50 nano seconds of clock, the randomness in the output increases.

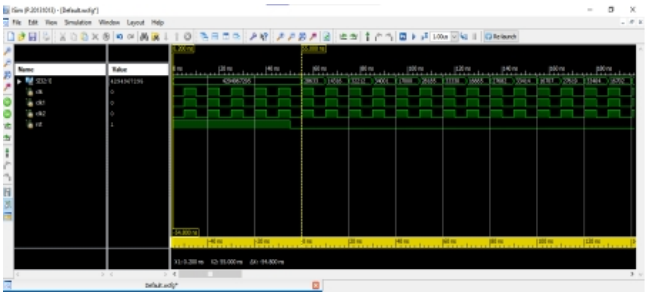

Figure 6. Simulation result of 32-bit LP LFSR based PUF

The above Figure 6 represents the simulation results of proposed 32-bit Low Power LFSR based PUF. For every 50ns the randomness in bits is increased.

4.2 Comparison Table of PAD & Randomness

Table 1: Comparison of PAD (Power, Area, Delay) & Randomness

	POWER (W)	AREA (LUT's)	DELAY (ns)	RANDOMNESS for every 50ns	
				50ns	100ns
Basic LFSR	133.93mw	1 out of 1920 LUTs	1.997ns	14	29
Low Power LFSR	91.34mw	6 out of 63400 LUT's	0.864ns	15	255
Existing 16bit LFSR Based PUF	85.04mw	10 out of 63,000 LUT's	0.981ns	65535	43690
Proposed Low Power LFSR Based PUF	125.63mw	16 out of 63,400 LUT's	0.981ns	4294967295	2863311530

The above Table 1 shows, the comparison of proposed design with the existing design.

5. Conclusion

In this project, the implementation of the proposed 32-bit Low Power LFSR Based PUF design is carried out by using the software tool XILINX ISE DESIGN SUITE 14.7 version. The proposed work shows great improvement in generating randomness which leads to better security while authentication. This is achieved due to its switching activity in the proposed circuit. The project can be further extended by improving the parameters such as the power consumption and area to get better results.

References

[1] Physical Unclonable Functions and Applications: A Tutorial Charles Herder ; Meng-Day Yu ; Farinaz Koushanfar ; Srinivas Devadas Proceedings of the IEEE Year: 2014 — Volume: 102, Issue: 8 — Journal Article — Publisher: IEEE

[2] J.W.lee, Daihyum lin "A technique to build a secret key in integrated circuits for identification and authentication applications", Proceedings of 15h Annual computer science and artificial intelligence Applications Conference, December 2004

[3] K. Sahithi and Dr. N.S. Murty, "Physical Unclonable Functions Implementation for Hardware Security and Trust", in Symposium on VLSI Design and Embedded Computing (VDEC'18), co-affiliated with Seventh International Conference on Advances in Computing, Communications and Informatics (ICACCI-2018), PES Institute of Technology, Bengaluru, South Campus, India, 2018.

[4] Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in Cryptographic Hardware and Embedded Systems, vol. 4727, P. Paillier and I. Verbauwhede, Eds. Berlin, Germany: Springer, 2007, pp. 6380.

[5] B. Gassend , D. Clarke, M. van Dijk, S. Devadas, "Physical random Functions and applications", Proceedings of 18th Annual Computer Security Applications Conference, December 2002.

[6] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging physical unclonable functions with nanotechnology," IEEE Access, vol. 4, pp. 6180, 2016

[7] Srikanth vyas, Naveen kumar uppala, "Improving the efficiency of PUF based key generation in FPGAs using variation-aware placement", 26th international conference on field programmable logic and applications, September 2016.

[8] S. R. and Dr. N.S. Murty, "Feedback Oriented Xor ed Flip-Flop Based Arbiter PUF", in 2018 Third International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), 2018.

[9] Sravya, G., Kumar, M. O. V. P., Sudarsana Reddy, Y., Jamal, K., & Mannem, K. (2020). The Ideal Block Ciphers - Correlation of AES and PRESENT in Cryptography. 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS).

[10] Sravya, G., Kumar, M. O. V. P., Merlin Sheeba, G., Jamal, K., & Mannem, K. (2020). Hardware lightweight design of PRESENT block cipher. Materials Today: Proceedings.