IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Design and Implementation of Linear Feedback shift Register based physical unclonable function

A. Nagamalli[1], P. Avinash[2], K.B.S. Akhil[3], K. Manoj Kumar[4]

Assistant Professor, ECE, GVP College of Engineering, Visakhapatnam, India [1]

B. Tech., ECE, GVP College of Engineering, Visakhapatnam, India[2,3,4]

Abstract: In the physical real world, there is a critical problem due to the threats in network security. As a result, there is an infringement of integrated intellectual data. Hence there is a strong necessity to eliminate this discrepancy in Integrated Security Systems (ISS). An LFSR is a commonly used circuit to generate pseudo random sequences. An LFSR is a shift register whose input bit is a linear function of the previous state. A physical unclonable function (PUF) is a physical entity that is embodied in a physical structure and is easy to authenticate but hard to predict. The output bits of a pulse generator are presented in parallel as a challenge input to an Arbiter PUF. PUFs depend on the uniqueness of their physical microstructure. This microstructure depends on random physical factors introduced during manufacturing. These factors are unpredictable and uncontrollable which makes it virtually impossible to duplicate or clone the structure. Therefore this project mainly focuses on providing security by randomly generating different sequences by the implementation of LFSR based PUF which can be decoded only by having master or true authentication of the system.

Keywords: Physical Unclonable Function, True Random Number Generator, Network Security, FPGA, Linear Feedback Shift Register, Information Security, Randomness.

INTRODUCTION

The requirement of information security within an organization has undergone two major changes in the past several years. The security of information felt to be valuable to an organization was provided primarily by physical and administrative documents, before the widespread of data processing equipment. An example of the latter is personnel screening procedures used during hiring process. An example of the former is the use of rugged filling cabinets with a combination lock for storing sensitive documents. With the introduction of the computer, the need of automated tools for protecting files and other information stored on the computer became mandatory. This is required for a system like time-sharing system and also sometime need is even more acute for systems that can be accessed over a public telephone data network or internet.

The second major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer. Network security is required to protect data while in transit. In fact network security term is misleading since all business, government and academic organisation interconnected their data processing equipment with a collection of interconnected networks.

TRUE RANDOM NUMBER GENERATOR

It is the generation of a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance, usually through a Random Number Generator (RNG) [7].Various applications of randomness have led to the development of several different methods for generating random data, of which some have existed since ancient times, including the rolling of dice, coin flipping, the shuffling of playing cards, the use of yarrow stalks as well as countless other techniques. Because of the mechanical nature of these techniques, generating large numbers of sufficiently random numbers [2] (important in statistics) required a lot of work and/or time. Thus, results would sometimes be collected and distributed as random number tables. Nowadays, after the advent of computational random-number generators, a growing number of government-run lotteries and lottery games have started using RNGs instead of more traditional drawing methods. RNGs are also used to determine the outcomes of modern slot machines. The uniqueness in this proposal is the key is assembled from a series of small, secret integers, each being an index into a string of bits produced by the PUF circuits [6]. A PUF unique pattern at each respective index is then persistently sent to exclusive or gates which is sent to Linear Feedback Shift Register circuits which generates complete signal from an extremely random PUF seed [4]. This setup is preferred because of its simple, robust architecture and NIST tests for randomness. The PUF is explained in detail in [5].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

LINEAR FEEDBACK SHIFT REGISTER

An LFSR is a shift register that, when clocked, advances the signal through the register from one bit to the next most-significant bit [1]. Some of the outputs are combined in exclusive-OR configuration to form a feedback mechanism. A linear feedback shift register can be formed by performing exclusive-OR on the outputs of two or more of the flip-flops together and feeding those outputs back into the input of one of the flip-flops [7]. Algorithmically generated test patterns are widely used in recent times. Algorithmically generated test patterns for logic networks, while generally giving good fault coverage, have three disadvantages.

- Test pattern generation can be extremely time-consuming, particularly for sequential circuits.
- A good deal of storage is required by the tester to hold the test patterns.
- The speed at which tests can be applied is limited.

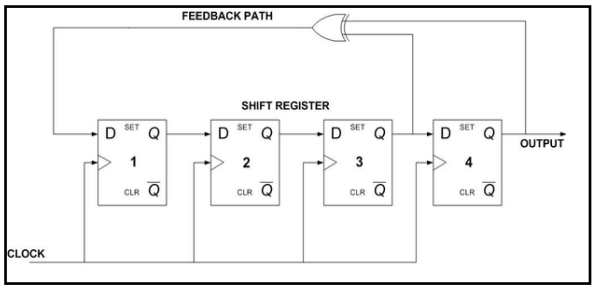

Figure 1. Linear Feedback Shift Register

RO-PUF BASED TRNG

Modified RO-PUF structure used for the construction of entropy source is built as shown in the figure 2. It is built with the combination of 2n+1inverters with a feedback path. The number of inverters should be odd to create a meander output signal. In RO-PUF mode, the output frequency F_Q will be unique, unclonable and unpredictable for each chip. Therefore, this mode can be used to generate random numbers. However, as mentioned earlier, this randomness has low quality [7]. To overcome this problem, the TRNG circuit shown in figure 1 is proposed.

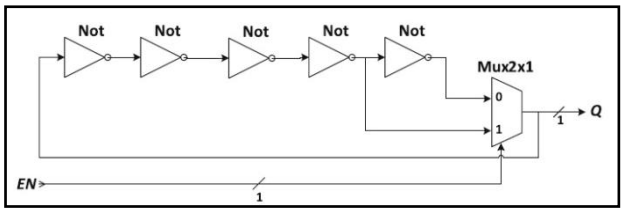

Figure 2. Ring Oscillator based PUF

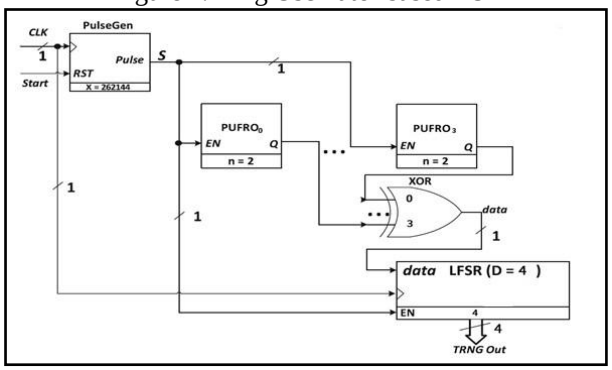

Figure 3. RO based True Random Number Generator (TRNG)

This circuit can be summarized as follows:

- **Single Pulse Generator:** This block generates single pulse with pulse width X. This pulse defines the RO-PUF's behavior.
- **PUF-chain: '**k' number RO-PUF entities are chained to generate the initial random number sequence.
- **XOR-tree:** A k-input XOR-gate is used to obtain one output bit from k PUF response bits.
- **LFSR:** This block is used to generate pseudo random number sequences but with true random seed. A D-digit true random number is produced by this block. It also represents a one-channel signature analyzer.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

IMPLEMENTATION

We implemented this LFSR based PUF onto FPGA Spartan- 3E board. The development tools used is Xilinx ISE 14.3 and Vivado HLS 14.3.

SIMULATED RESULTS

- $(2^n - 1)$ numbers with sufficient time gap are generated, where n is the number of output bits.
- The seed which was obtained from the xor gate is responsible for generating the random numbers.

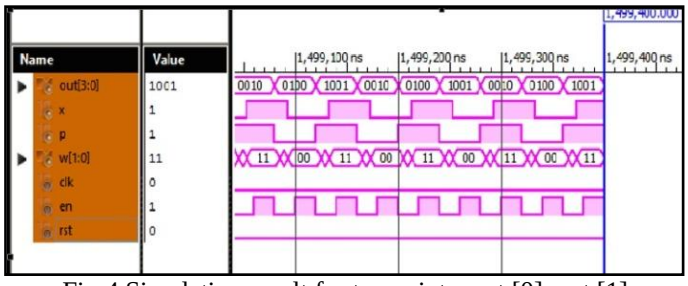

Fig 4 Simulation result for tap points: out [0], out [1]

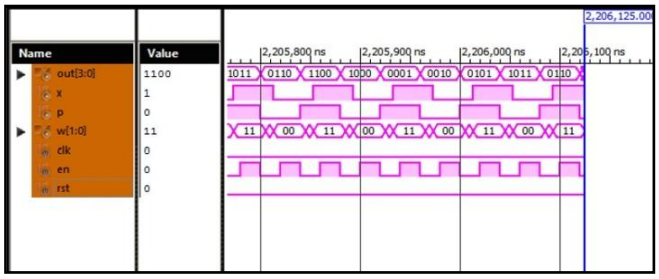

Fig 5 Simulation result for tap points: out [0], out [2]

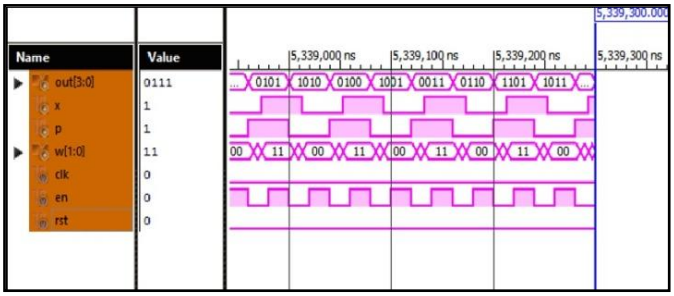

Fig 6 Simulation result for tap points: out [1], out [3]

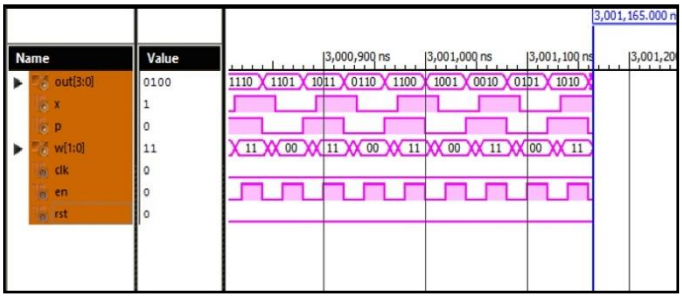

Fig 7 Simulation result for tap points: out [3], out [2]

Depending upon the seed obtained from the PUF circuitry, the random numbers are generated as shown in the figures 4,5,6,7 for various tap positions mentioned. In the above results, out [3:0] indicates the random 4-bit sequence obtained. x indicates output from the XOR gate. p indicates delayed output of the PUF circuit. w(2-bit) indicates the outputs of remaining physical unclonable functions.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

SYNTHESISED RESULTS

Figure 8 Random Sequence 1

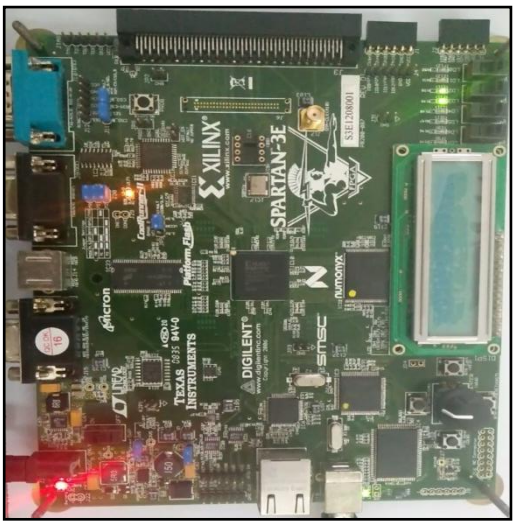

Figure 9 Random Sequence 2

Figure 10 Random Sequence 3

DOI10.17148/IJARCCE.2017.6573

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Figure 11 Random Sequence 4

CONCLUSION

The seed which was obtained from the xor gate is responsible for generating the random numbers. This project reflects the purpose of building a True Random Number Generator (TRNG) based on Physical Unclonable Functions (PUFs). This design increases the randomness of the output sequence as the random seed is unclonable. This seed is fed into Linear Feedback Shift Register resulting in generation of randomness. The usage of Ring Oscillator PUF provides less complexity and gives legit quality of randomness. The output stream is synthesized on Spartan 3E FPGA test board and tested. The results show that the output stream is completely random.

REFERENCES

[1] Ali Sadr, Mostafa Zolfaghari-Nejad, "Advanced Computing: An International Journal (ACIJ)", Vol.3, No.2, March 2012.
[2] (Sid) Paral, Zdenek, and Srinivas Devadas, "Reliable and Efficient PUF-based Key Generation Using Pattern Matching." 2011 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST) 128–133.
[3] M. Ayat, R.Ebrahimi, S.Mirzakuchaki, "On Design Of PUF-Based Random Number Generators" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, pp. 30 -40 May 2011.
[4] M.-D. M. Yu and S. Devadas, "Secure and robust error correction for physical unclonable functions," IEEE Design and Test of Computers, vol. 27, pp. 48–65, 2010.
[5] D. Merli, F. Stumpf, and C. Eckert, "Improving the quality of ring oscillator PUFs on FPGAs," in Proc. 5thWorkshop Embed. Syst. Security, 2010, pp. 9:1–9:9.
[6] J.W. Lee, D. Lim, B. Gassend, E. G. Suh, M. van Dijk, and S. Devadas, "A Technique to Build a Secret Key in Integrated Circuits with Identification and Authentication Applications", Proceedings of the IEEE VLSI Circuits Symposium, 2004.
[7] Chip-Hong Chang and Miodrag Potkonjak , "Design and implementation of High-Quality Physical Unclonable Functions for Hardware Oriented Cryptography" in Secure System Design and Trustable Computing 2nd ed. Springer: ,2016.