Design and Implementation of TRNG for HighlySecure Data Transfer in ASIC

Vangala Satya Sirisha
Department. of ECE
Aditya Engineering College, Surampalem
sirishasvangala96@gmail.com

Gulivindala Suresh
Department. of ECE
Aditya Engineering College, Surampalem.,A.P.India.
dean_sb@aec.edu.in

Abstract— In today's world, data security is crucial to everyday digital life. Any organization should secure its data from external attacks since it is a valuable asset. Data protection from unauthorized access requires information security, which is not only essential but also necessary. An essential part of data security is key management of keys, data encryption, and decryption. By using analog circuitry and random number generators, every communication system's confidentiality is boosted. The power and space requirements for this kind of analog model are higher. As a result, digital RNGs are preferred over analog circuit-based hardware RNGs. It's crucial to get the appropriate data protection to handle the difficult challenges provided by illegal entry. For cryptosystem applications, such as security applications, space applications, military applications, and smart cards, among others, implementation of the cryptosystem and the Random Number Generator is crucial. The desire to design a system that is highly secretive, unexpected, non-deterministic, and truly random is growing. Because PRNGs are deterministic and not truly random in nature, it is possible to forecast their behaviour. While the key is known, CSTRNGs, on the other hand, are truly random, non-deterministic, and unpredictable. This research focuses on the usage of an Application Specific Integrated Circuit and a Really Random Number Generator to produce digital signatures (ASIC). An n-bit signature can be generated and validated using the suggested. Use the produced and validated 10 bit signature here. The Xilinx ISE emulator was employed to produce the job.

Keywords— Xilinx Vivado · Video processing and Image Processing architecture, · Xilinx System Generator, · Matlab/Simulink, · IIR filter.

I. Introduction

Security is more important than ever in the era of digital technology. Electronic data transport is faster than conventional data transfer methods. Data security is just as crucial in the modern world as data transport speed. A major component of data security is the creation of keys. Historically, keys were sent across a transmission media that was more vulnerable to data hackers along with data. Key generation is therefore of utmost importance in safe data transmission. Key generation can be done in a variety of ways, including using source obfuscation, binary delivery techniques, and crypto systems. Source obfuscation, the oldest data security technique, involves swapping out significant data in an IP source for intentionally illegible information. That is not a very secure procedure as a result. Binary delivery is an additional technology-dependent data security technique. The person, the system, and the technology all have an impact on how it operates. A novel method of transmitting data is referred to as a cryptosystem, also known as a hybrid cypher. (Asymmetrical and Symmetrical Together). A key with prolonged sequences is the result of this. Data is a valuable asset for every business, therefore safeguarding it from outside threats is essential. To prevent unwanted access to data, information security is not only essential but also required. Important elements of data security include key management, data encryption, and decryption. Random sequence generation is one such technique for data security. Using the pseudorandom property of LFSR, random numbers can be generated for use in a variety of cryptographic applications. The creation of random numbers is done by pseudo-random number generators and random number generators (RNGs) (PRNGs). (PRNGs).

Although most applications require random numbers, their production is frequently disregarded. In contrast, key generation is extremely important in cryptosystems. Depending on the application, several key generation techniques are used. Due to their deterministic nature, PRNGs are used by the majority of digital systems. Each possible combination of the input devices is saved in a pool of integers, from which the seed is chosen. The keys in the PRNG scheme are created using this seed. Despite the fact that the key is created, there is a potential that an attacker will be able to guess the data due to the deterministic nature of PRNGs. The production of keys using a cryptographically secure true random number generator (CSTRNG), which is non-deterministic and genuinely random in nature, is one such approach. RNGs must not be vulnerable to prediction in order to ensure absolutely random results. In this study, CSTRNG has been used to generate keys that are nondeterministic and have greater data lengths.

Data security is a hugely complex and interesting subject. IT experts deal with the main management difficulties and information security issues every day. Aadhar information, customer lists, credit card details, online banking passwords, stock holder data and addresses are just a few examples of the privileged data that organisations may have access to. Corporate fraud, Dummy Corporation, internet fraud, insider trading, microchip fraud, accountant fraud, boiler rooms or brokerage houses, etc. are all examples of securities fraud, often known as stock fraud.

Fig.1 Topology of a simple network

The rush to open up their network as seen in Fig. 1 is forcing companies to reconsider their security needs because the purpose of yesterday, which was to limit access to these information resources, is no longer applicable in the new digital economy. The best categories for assaults on the network or security system are:

Interruption: An attack on availability is when a resource belonging to the organization is destroyed, rendered inaccessible, or rendered useless.

Interception: Attacking confidentiality is gaining unauthorized access to an asset of the organization.

Modification: Integrity attacks involve tampering with data or changing an organisation’s asset.

Fabrication: Attacks on authenticity occur when an unauthorized person introduces fictitious communications into a network or security system.

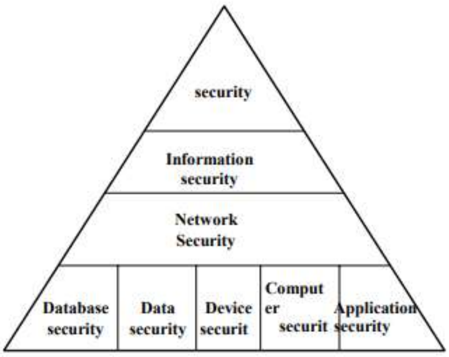

Fig.2 hierarchy of level of security.

Over the past ten years, data security procedures have undergone significant development. Academic and governmental organizations devised procedures in the field of computer security that is still in use today. Security is the first priority for any system, as shown in Fig. 2's hierarchy of security levels. It may be broken down into four different levels of security as it moves from bottom to top. Whereas the foundational level of the security system is covered by database security, data security, device security, computer security, and application security. Information security is the branch of security at the second level of security, where network security predominates.

II. Literature Survey

According to Daniel Morrison et al. (2019), a linear feedback shift register is employed to produce pseudo sequences. It is low power, quick, and simple to implement in hardware. Binary counters are used in place of LFSR Counters to improve performance. Speed plays a crucial role in single photon detection, which is where LFSR counters are primarily used. By using decoding logic scaled logarithmically in stages before increasing exponentially, depending on the number of bits, the LFSR-generated pseudo random sequence is transformed into a binary sequence. Due to the decoding logic, the design necessitates additional circuitry that uses more power than usual and takes up more space on the device.

Aysha S. Shanta et allow .'s weight reconfigurable PRNG leveraging the prior work's 3T chaotic map was published in 2019[2]. Using a chaotic map, discrete temporal chaotic signals can be produced. The chaotic oscillator is necessary for the creation of these signals. Because it contains two branch parameters that are used to produce multiple random sequences, this design is reversible. The proposed work can make use of the two chaotic oscillators, analog mux, 10-bit ADC, 2-bit shift register, and XOR gates. With a 1.2V power supply, this job can be implemented utilizing 65nm CMOS technology. It was used in an IOT device because of its small size and high-performance requirements.

Adriaan Peetermans, et al.'s[3],(2019) study makes use of TRNGs' importance in contemporary cryptosystem applications. Implementing TRNGs is a highly difficult task that frequently necessitates hand placement and routing. to make certain that the generated numbers are very entropic. The dynamic TRNG (COSO-TRNG) based Coherent Sampling Ring Oscillator used in this work by the designer makes it easy to include the entropy source into intricate frameworks. As a result, the TRNG arrangement approach selects a configuration that meets the security requirements.

Key generators, digital signatures, and IoT securities are only a few examples of cryptographic systems that depend on PRNGs, according to Bikram Paul et al[4] .'s discussion from 2019. Two PRNG approaches based on Blum-Blum-Shub (BBS), XOR shift, and Permuted Congenital PRNGs were proposed by the authors in this paper. The earlier one is used for general-purpose applications, whereas the latter one is chosen for IoT applications that require little power. Both PRNG algorithms calculate the total dynamic powers at New for the True Random Number Generator (TRNG) generation based on analog RRAM is Bohan Lin, et al[5], .'s (2019). For the IoT protection application, a high-speed and high-reliability TRNG based on analog RRAM can be constructed. The current memory square and circuit utilization benefit

greatly from the high-speed and high-reliability TRNG design, which makes it suitable for potential IoT applications.

III. Random Number Generation Principles

Real random sequence creation is challenging to produce, and the sources are only somewhat useful in other applications. On the other hand, it is crucial that a sequence that displays statistical unpredictability is created. Moreover, methods that produce random numbers are used in cryptography applications; these algorithms are deterministic in nature. Yet, if a competent technique is used, the produced sequence would pass several randomness tests. Pseudorandom numbers are the terms used to describe the numbers in such sequences. Encryption and decryption are the fundamental building blocks of any cryptosystem. the schematic representation of the widely used cryptographic scheme. Cryptography, often known as cryptanalysis or cryptosystem, is the process of encrypting or decrypting data to safeguard sensitive information. The combination of a key and plain text makes the cryptosystem operation functional. Here, a phrase, a number, or a combination of both is the key. Based on the system's robustness and key isolation, this key is utilised to encrypt plain text or individual message bits.

Any digital machine's output sequence must typically follow some well-defined statistical rules. This claim is supported by the principles of independent and uniform distribution. The sequence of numbers created in a uniform distribution is firstly uniform and well-defined, meaning that the frequency of occurrence is nearly constant. When in the independent distribution, it is impossible to interpret any one number in the sequence from the others. The distribution of the resulting sequence is tested using a number of stated algorithms. The sequence is subjected to a variety of these tests to demonstrate that it does not exhibit independent distribution. The approach behind this is to run such tests up till the independent sequence creation is robust enough.

Unpredictability in the production of a random sequence is defined as the succeeding numbers in the series being independent of one another or not having a definite arrangement between the numbers in the sequence. Each number generated in such a sequence is statistically independent of the numbers generated before it, making it unpredictable. When creating a cryptosystem or for applications involving network security, this trait is highly helpful. Sadly, very few algorithms are capable of comprehending this genuine unpredictability. In reality, random sequence generation is extremely uncommon and has only limited applicability in cryptosystems. Many different techniques have been put up to produce the sequence that seems random. A tool that produces random number sequences is known as a random number generator. RNG generates a series of random numbers, but it doesn't produce any particular pattern. It can be used for numerous things, including security, gambling, sampling, and lotteries. Have a variety of ways to create random data for various uses. the RNGs that are included into software to improve the hardware's security and speed. Based on LFSR's unique trait of randomness, which is also a property of LFSR, LFSR has been introduced. The creation of randomness is reliant on the original value. The seed value is that starting point. The random number generator in Figure 3 is a straightforward block that produces a range of values. Depending on the circuit of random number generators employed, the stream of bits might be either completely predictable or completely deterministic.

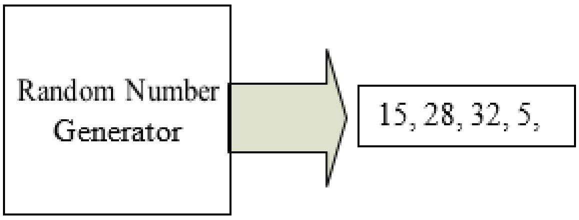

Fig. 3 Random Number Generation.

A number is used as the initial seed to start the random number generation process. Based on a probability distribution technique, seeds can be produced. If the seed value is present at each step of the random number generation process, the sequence will always start at the same value and provide the same results. So the initial seed determines the RNG's sequence.

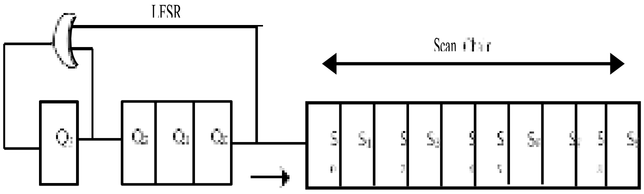

Fig. 4. Kick off process of RNG.

The original procedure for creating pseudorandom numbers was put forth by Lehmer, and it is still the method most frequently employed today. The Linear Form of Congruence is the name of the algorithm. The algorithm makes use of the next four variables.

m-modulus, generally $m>0$;

a-the multiplier $0 \leq a < m$;

c- the increment $0 \leq C < m$;

X_0- the seed or starting value $0 \leq X_0 < m$;

3.1 Cryptographically Random Number Generator:

Here, we will solely take into account the benefit of using encryption logic to generate RNGs in this way. Fig. 4 depicts the configuration. A counter with the period "N" serves as the input to the encryption algorithm in this pseudorandom number generation method. The basic idea is that the master key provided to the encryption logic block is used to generate session keys. The counter value is increased by one when each key is generated. As a result, the stream produced by this technique cycles through completely. As a result, the sequence has a maximum length. However, the outputs generated are $X_0 \neq X_1 \neq X_2 \neq X_{3...} \neq X_n$. The counter values are independent of one another and do not depend on one another. It is challenging to side any of the secret keys created using encryption logic since the master key is secured. This system is strengthened by replacing the counter input with a fully period PRNG.

3.2. ANSI Pseudorandom Number Generator:

There are many defined methods for producing PRNG sequences. One such technique for producing the strongest PRNG sequence is ANSI PRNG. Many applications, primarily financial security applications, are used with this technique. As depicted in Fig. 4. The Inputs for it are two. One input, input DT, denotes the current date and time, whereas input Si denotes the initial seed. Together with the creation of the sequence, both inputs are updated. Where EDE stands for the Encrypt-Decrypt-Encrypt (EDE) sequence, which employs the two keys K1 and K2 as shown.

The outputs are

$$R_i = EDE_{K1,\ K2}\,[S_i \oplus EDE_{K1,\ K2}\,[DT_i]];$$

$$S_{i+1} = EDE_{K1,\ K2}\,[R_i \oplus EDE_{K1,\ K2}\,[DT_i]];$$

IV. Design and Implementation of Random Number Generator:

The creation of genuinely random numbers is one of the most secure methods for data transmission. Digital systems are susceptible to disruptions that can cause data bits to switch from encrypted to unencrypted and vice versa while being transferred and processed. Online games like Rummy, Tic-Tac-Toe, dice games, and other games can all be played using RNGs in gaming software. RNGs can produce random events for critical hits or for selecting random chances in games where the goal is to shoot the target. They are kept by the website that is used to deliver cards, shuffle data, and shuffle the cards in the game of rummy. Similar to this, in a dice game, RNG can be used to roll the dice or flip a coin after the outcomes can be determined by unpredictable possibilities, as seen in fig. 5.

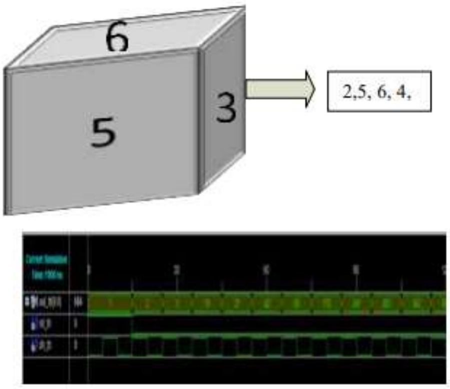

Fig. 5. RNGs in Gaming Application

The creation of OTP is fully dependent on all financial services. For the sake of consumer security, this OTP should be more random. Let's say that in order to accomplish a money transfer through mobile banking or net banking, an OTP is required. Similar to this, all services such as ATM card pin generation, MPIN, and all i-mobile services OTP can be used. In this case, CSTRNGs are safer than using only RNGs. For instance, how to utilise the RNG in a login page for any banking login home page, in which the user must first provide personal data before it can create the OTP, is demonstrated in the part below.

Starting the ISE Software

Start -> All Programs -> Xilinx ISE 14.5 -> Project Navigator

Creating a New Project

For the creation of a new project

1. Select the **New Project** option in the **File** menu, it opens a New Project Wizard.
2. Enter the Project Name field as a **tutorial.**
3. Enter or browse to a location (path of a directory) for the new project. A subdirectory with a name tutorial is automatically created.
4. Verify that HDL is selected from the top-level source type list.
5. Click on **Next**, and it moves to the device properties page.
6. Fill the properties in the table by leaving the default values for the remaining fields.

V. Results And Analysis:

The LFSR counter serves as both a key generator and a pseudo-random number generator in the current work. The key in the proposed method can be produced using a real random number generator.

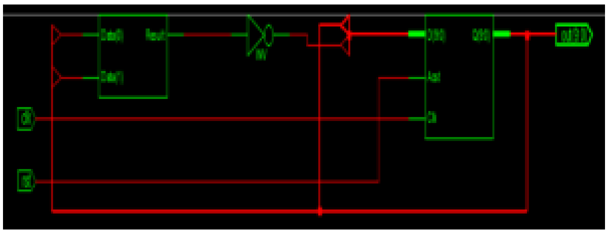

Fig. 6 Pin diagram for PRNG

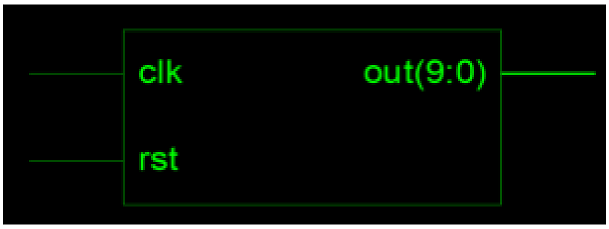

Fig. 7 RTL schematic for PRNG

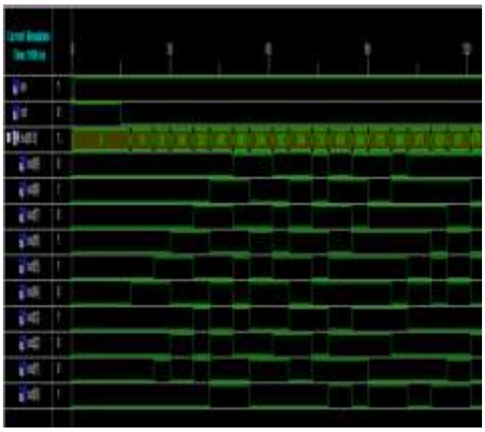

Fig. 8 Simulation Result for PRNG

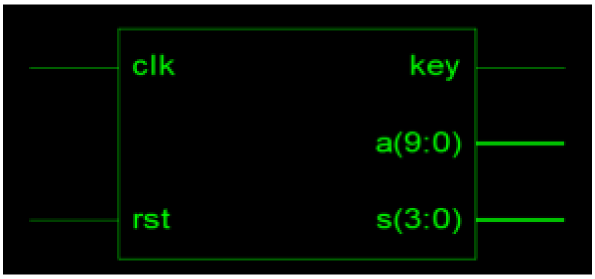

Fig. 9 Pin diagram for LFSR Counter

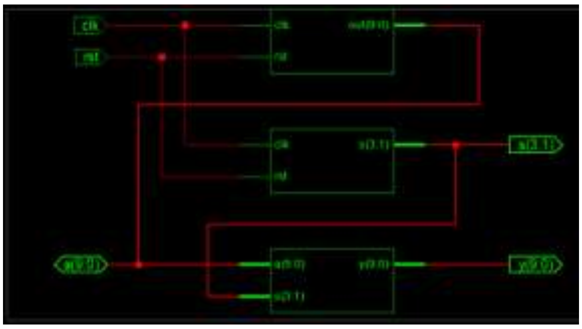

Fig. 10 RTL schematic for LFSR counter

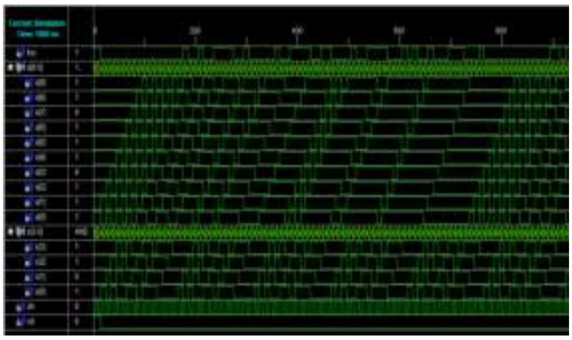

Fig. 11 Simulation Results for LFSR counter

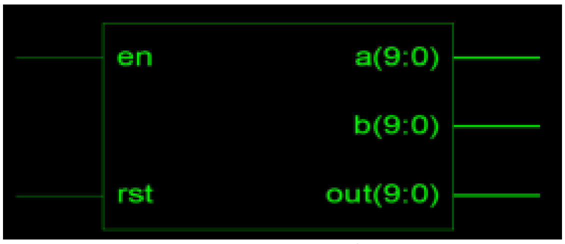

Fig. 12 Pin diagram for CSTRNG

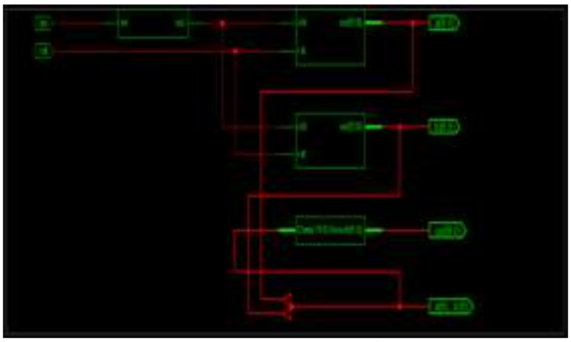

Fig. 13 RTL schematic for CSTRNG

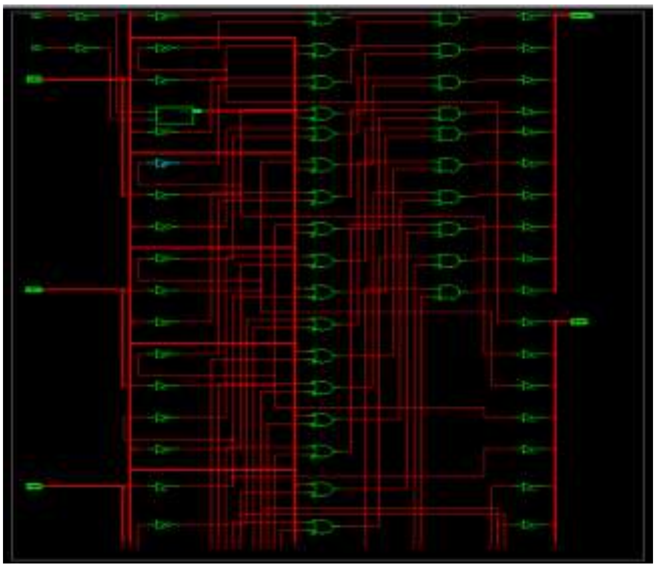

Fig. 14 Technology schematic for CSTRNG

Table I: Comparison between PRNG, LFSR counter and TRNG:

	PRNG	LFSR counter	CSTRNG
Leakage power	48.531 nw	82.125 nw	113.060 nw
Dynamic power	27222.682 nw	47607.764 nw	71003.993 nw
Total power	27271.214 nw	47689.889 nw	71117.052 nw
Area	1315	2689	2947
Delay	348 ps	416 ps	367 ps
cells	22	85	59
Fan out	38	38	40

VI. CONCLUSION

The comparison of the proposed generators and the traditional generators has been the focus of this report. These methods for generation were created, put into practise, and the measurement results and simulation results were contrasted. The CSTRNG and PRNG methods were both created with high speed and minimal power consumption in mind. The simulation results show that because the CSTRNG method of randomness generation is unpredictable, it has higher security. For 8, 16, 32, 64, and 128 bit generators, simulations were run.

As can be observed, the CSTRNG uses a little bit more space than a typical PRNG. This is as a result of the minimal routing complexity of PRNG. A brief report is supplied regarding the space used by the RNGs, PRNGs, and CSTRNGs. This is explained by the fact that the PRNG requires less reasoning than the CSTRNG does. However the CSTRNG has two clear benefits over its rival: lower power consumption and greater security.

REFERENCES

[1] P. W. A. J. Qiu, “A Pseudo random bit generator based on mixing of state variable of CML,” IEEE 2nd Informationa Technology Networking Electronics and Automation Control Conference, 2017.

[2] l. C. V. A. G. E. A. B. V. l. Chugunkov, “Methods for Improving the Statistical Properties of Psedo -random Number Generators,” IEEE Conference of Russian Young Researches in Electrical and Electronic Engineering, 2019.

[3] Y. Z. J. J.A. N. Guan, “A Self -Timed Ring based True Random Generator on FPGA,” IEEE International Conference onSolid state and Integrated Circuit Technology, 2018.

[4] C. Y. Huang, W. C. Shen, Y. -H. Tseng, Y.-C. King and C.-S. Lin, “A Contact -Resistive Random -Access-Memory-Based True Random Number Generator,” IEEE Electron Device Letters, vol. 33, no. 8, p. 60, 2012.

[5] F.Massodi, S.Alam and M.U.Bukhori, “An analysis of Linear Feedback Shift Registers in stream chippers,” International Journal of Applications, vol. 46, pp. 46-49, 2012.

[6] H.Rahimov, M.Babaei and M.Farhadi, “Cryptographic PRNG based on Combination of LFSR and Chaotic Logistic Map,” Applied Mathematics, vol. 2, pp. 1531-1534, 2011.

[7] M. Goresky and A. Klapper, “Pseudo Noise Sequence based on Algebric Feedback shift registers,” IEEE Transactions on Information Theory, vol. 52, pp. 1649-1662, 2006.

[8] S. Haykin, “Pseudo Noise Sequences,” Communication Systems Newyork:John-Wiley&Sons, 2001.

[9] P.Li, Z.Li and W.A.Halang, “Analysis of a multiple output Pseudo-random-bit generator based on a spatiotemporal chaotic system,” International Journal of Bifurcation and chaos , vol. 18, pp. 2949-2963, 2006.

[10] S.Wang, W.Liu and H.Lu, “Periodicity of chaotic trajectoriesin realisation of finite computer precisions and its implications in chaos communication,” International Journal of Modern Physics, vol. 18, pp. 2617-2622, 2005.

[11] A.Akhshani and A.AkhavanA.Mobaraki, “Pseudo random number generator based on quantum chaotic map,” Communication in Non-linear science nad Numerical Simulation, vol. 19, pp. 101-111, 2014.

[12] F. A. S.Liu, “Cryptographic pseudo random sequencefrom the spatial chaotic map,” Chaos Solitons Fractals,vol. 41, pp. 2216-2219, 2009.

[13] F. C. A. S. Li, “A double scroll basedtrue random number generator with power and throughput adjustable,” International conference on ASIC, 2009.

[14] M. Han and Y. M. Kim, “Un predictable 16 bit LFSR based true random number generator,” International SOC design Conference, 2017.

[15] J. Genoff, “A floating gate array based discrete true random stream generator,” International Scientific Conference Electronics, 2017.

[16] O.A.A.H.A. Mohammed Abumuala, “A New Method for Generating Cryptographically Strong Sequences of Pseudo Random Bits for Stream Cipher,” International conferences on Computer and Communication Engineering,2010.

[17] R.D.P.A.A.D. Santis, “On the Relation of Random Grid and Deterministic Visual Cryptography,” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, vol. 9, p. 4, 2014.

[18] S.A.R.A.Guinee, “Random NumbersGeneration Using Pseudo Random Binary Sequences For Data Encryption Applications,” Irish Signals and Systems Conference, 2001.

[19] J.A.J. M.E.Yalcin, “True Random Bit Generation from a Double Scroll Attractor,” IEEE Transcations on Circuit and Systems, vol. 51, 2004.

[20] H.R.Simpson, “Statistical properties of a class of pseudorandom sequences,” PROC.IEEE, vol. 113, 1966.