ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 8, Issue 4, April 2019

Review on Design Techniques of a Random Number Generator

Aurodeep Mohanty
Mtech Research Scholar in VLSI Engineering
Department of Electronics And Communication Engineering
G.H Raisoni College of Engineering Nagpur.

***Abstract*- Cryptography is the art and science of keeping information secure. Cryptosystem plays important role in securing confidential information. In Cryptography first information is store and then transmit data it in a secret form so that only the person who is intended can read and process it. An array of numbers whose values are not based on its preceding number is called Random numbers. The number is said to be random if it does not depends on any calculative algorithm or any seed value. Earlier, random number is created by dice game method but presently there are various methods to design a (RNG). The generated numeric values or symbols should be unpredictable without any pattern. This paper gives a review of the random number generation methods and analyses the techniques in terms of performance.**

A keywords*-symmetric key, asymmetric key, *RNG (random number generator)

I INTRODUCTION

The rise of security and safety has risen over these years resulting in highly authentication protocols and highly secure algorithms where a cryptographic system is a must. Cryptographic systems provide privacy to data, image or any information related medium which is authenticated and needs to reach the destination without any variations or disruptions. The concept of cryptosystem arises in this point when the source data is being hacked or mislead by an attacker. To avoid such issues cryptographic protocols comes into the picture. These systems need to be very complex and difficult not only from design point of view but also from implementation. This is because more the high security level, less chances of getting hacked. Cryptosystems can be a single device with complex mathematical algorithms or hybrid systems with twice as greater complexity. The main aspect or motive behind the design should be the requirement of the user. Whether it needs to protect some data or testing purpose or simulation checker or any other security uses. A random number generator is an important module in encryption or cryptographic protocol. The security of such systems depends on the assumption that the next values in the sequence cannot be predicted from the observed sequence. Hence RNG used for cryptographic process should be considered as an integral part of the encryption system. Encryption systems are those systems which needs to be highly secure in terms of transmission of data. Hence the random numbers should be unpredictable in nature and also should not depends on any previous data bits. There are many real time applications of random number generators like otp (one time password) generator, captcha generation for web portals, computer simulation, digital gaming and statistical sampling. There are two types of RNGs used for such applications which are TRNG (True random number generator) & PRNG (Pseudo random number generator).

A true random number generator uses entropy sources that already exist instead of inventing them. Entropy here refers to the amount of uncertainty about an outcome. A true random number generator is truly uncertain and unpredictable. It is the source of entropy which makes it unpredictable. The entropy is converted to sequence of binary or numeric bits, unlike their deterministic cousins there is no internal state kept in the generator and the output is based only on the physical process and not any previously produced bits.

Random numbers are useful for a variety of purposes, such as generating data encryption keys, simulating and modeling complex phenomena and for selecting random samples from larger data sets. They have also been used aesthetically, for example in literature and music, and are of course ever popular for games and gambling.

When discussing single numbers, a random number is one that is drawn from a set of possible values, each of which is equally probable, i.e., a uniform distribution.

As the use of digital data is increasing in transmission and processing, data protection is becoming much more important. To meet the safety requirement, cryptography is a common technique which provides security for transmitting electronic data like images, videos. There are two important parameters which are considered while sending information on the public are efficiency and safety. A cryptographic algorithm is widely used today because of its security advantages. Three main requirements of cryptography are authentication, confidentiality, and non-repudiation.

II. CRYPTOGRAPHY GOALS: There are three main goals of cryptography[2].

- Authentication: a process in which a user has to provide their identity to another who does not have personal knowledge of their identity
- Confidentiality: Confidentiality refers to keeping the information secret. The sender encrypts the message using a cryptographic encryption algorithm with a suitable key. The recipient decrypts the message using a cryptographic decryption algorithm with match key that may or may not be the same as the one used by the sender.
- Non-repudiation: Sender or receiver cannot deny a transmitting/received message. The sender of a message cannot later claim he/she did not send it[1].

The cryptographic algorithm has two types which are given below:

a) Symmetric key cryptography algorithm
b) Asymmetric key cryptography algorithm

a) Symmetric (Secret) Key Cryptography

Symmetric key cryptography is also called secret key cryptography as it is the oldest technique which is used by

users. A secret key which is used by the user in this is called the private key. A secret key can be anything it has been a random letter, a number or else just a word. A secret key which is used to encrypt the data can able to change the content in a particular way so that only authorised receiver can see the original information.

Some Asymmetric key cryptographic algorithms which are trending these days are given below:

1)DES (Data Encryption Standard)
It stands for elliptical curve cryptography, it is one of the most powerful and advances cryptographic standard used my modern systems. As the name suggests it uses elliptical curve theory to produce efficient keys used for public key algorithms. Systems like RSA invent their own keys rather than depending on other security systems. Like other cryptographic systems, it is also used for encryption and decryption of data and exchange of keys but the only difference which makes it more advance is the elliptical curve structure which keeps changing and makes it difficult for the attackers to decode the information. It is efficient and powerful but difficult to design. [13].
2)3-DES(Triple–Data Encryption Standard)
It stands for triple data encryption standard and is practically more advance than normal block cipher DES. In such systems, the data is subdivided by blocks. And then the algorithm is applied. In 3 Des the algorithm is applied thrice to each data blocks which further increase the length of the key and also give efficient encrypted output. This block cipher algorithm is an advanced version of the DES system and is used widely where computerized cryptography is needed. Being more advanced, it also requires more processing power for generation of bits. [11].

3)RC4 (Rivest cipher 4):

RC4 is a stream cipher which is developed by Ron Rivest. It is also known as Rivest Cipher 4 used for ciphertext generation. In RC4 a bit-wise encryption/decryption is performed where the key length for this is 40-128 bits.RC4 popularly used in transport layer security. The key generation is basically done by the pseudo-random stream [9].

4)AES (Advanced Encryption Standard):

AES stands for advanced encryption standard. It is made by National Institute standard technology (NIST) in 1997 and invented by Vincent Rijmen. AES replace to DES algorithm because the size of the secret key of DES is only 56 bit. Due to the small size of the secret key DES insecure for many application and unknown person hacks the data easily. AS compare to DES, AES is stronger because the size of the secret key of AES is 128, 192, 256 bits are used for encryption and decryption purpose and block size of AES is 128 bits, which is higher than DES.

5)Blowfish:
Blowfish is symmetric block cipher. Blowfish is unpatented and license-free. It can be effectively used for encryption purpose. The block size of blowfish is 64 bit, was designed in 1993 by Bruce Schneider. Blowfish is unpatented so is available free for all users[19].

6)SHA:
SHA or secure hash algorithm is a symmetric cryptographic hash function. It is developed by NIST along with NSA. In 1993 SHA was published as a federal information processing standard. It has following versions SHA-0,SHA-1,SHA-2,SHA-3[12].

b) Asymmetric (public) Key Cryptography

An asymmetric key is differing from the symmetric key algorithm because in this sender and receiver use different keys that cannot be derived from each other. A public key is distributed freely where the private keys are kept hidden. A public key used for encryption has to be shared by both sender and recipient . A public key which is used to encrypt the data can able to change the content in a particular way so that only authorised receiver can see the original information. An asymmetric cryptosystem is also referred to as public key cryptosystems [1].

Some Asymmetric key cryptographic algorithms which are trending these days are given below:

1)RSA (Rivest, Shamir and Adleman)
RSA is one of the most important cryptographic algorithm used for highly secure devices. This algorithm is widely complex to get through because it works in the factorisation of two or more large prime numbers. It is a known public key asymmetric algorithm, as it consists of both private and public keys. Where one key is kept private and the other is known to both sender at the source and the receiver at the destination. It proves it's security by the amount of data it sends through the digital medium or via modern computers. It is a fast and efficient algorithm but yes difficult to built. Its name RSA is derived from the name of their makers Rivest, Adi Shamir and Leonard Adleman.[9].

2)Diffie-Hellman
When it comes to cryptography, it means two mutual parties will form a secure connection and transfer their key information via a key or data. This algorithm is based on such a simple principle where two parties exchange data which is nothing but a shared secret key. This key is used in symmetric algorithms like AES. The shared secret key is basically a small data or random numbers or password used to unlock the main data bytes. It is quite complex to hack this algorithm because of this difficult structure and mode of exchange. It is different from RSA but similar in solving numeric problems. It is named after it's makers Whitfield Diffie, Martin Hellman and Ralph Merkle. [10].
3)El-Gamal
E1-Gamal is introduced by taher E1-Gamal in 1985. Is the asymmetric public key cryptography which is based on Discrete Logarithm Problems.E1gamal is also used as a digital signature. Each time when the same plaintext is encrypted, it gives a different cipher text. The biggest disadvantage of Elgamal is having cipher text twice the size of the plaintext.
4)ECC
It stands for elliptical curve cryptography, it is one of the most powerful and advances cryptographic standard used my modern systems. As the name suggests it uses elliptical curve theory to produce efficient keys used for public key algorithms. Systems like RSA invent their own keys rather than depending on other security systems. Like other cryptographic systems, it is also used for encryption and

decryption of data and exchange of keys but the only difference which makes it more advance is the elliptical curve structure which keeps changing and makes it difficult for the attackers to decode the information. It is efficient and powerful but difficult to design. [7].

III LITERATURE SURVEY

Anju.P.Johnson, Rajat chakraborty, Debdeep mukhopadhya presents a True random number generators (TRNGs) which is applicable for all modern security applications cryptographic systems. Field programmable gate arrays (FPGAs) form an ideal platform for hardware implementations of many of these security algorithms. In this research, they present a highly efficient and tunable TRNG based on the principle of frequency interpretations, for FPGA-based applications. This TRNG is implemented on Spartan 3 development board and the ring oscillators are replaced with digital clock manager. The circuitry becomes bulky and many other blocks such as RAM and other memory storage components are used to support the DCM working. The results shown in the research are thoroughly checked with NIST tests and the outputs are proven to be random in nature. A comparison is also given in the paper which shows the variations in the result as compared to other designs. [1]

Berk Sunar, William J. Martin, and Douglas R. Stinson.
After complete and through several misconceptions they proposed a generalised designed model which, under certain assumptions, will generate unpredicted random bits with some variations to statistical manipulation and running in the megabit-per second range. A key motive behind the implementation is the fill rate, which measures the fraction of the time domain in which the output signal is proved to be random. Their study shows that a mild increase in the number of oscillators is required to obtain a unique factor improvement in the fill rate. All of their analysis is based on methods, which is proved to be efficient, providing us to develop a network in which they precisely check the performance and the design. [2]

K.H. Tsoi, K.H. Leung and P.H.W. Leong research on RNGs shows two FPGA based design of random number generators intended for embedded based cryptographic algorithms. The first is a true random number generator (TRNG) which employs ring oscillator and uses the phase noise to produce the unpredictable bits, and the second is a serial implementation of a Blum Blum Shub (BBS) pseudorandom number generator (PRNG). Both designs are extremely complicated and can be implemented on any FPGA device. They were designed specifically for use as FPGA based cryptographic hardware cores. The TRNG and PRNG were tested using the NIST and Diehard random number test suites. [3]

"Müstak E. Yalçın, Johan A. K. Suykens, and Joos Vandewalle,. shows a novel true random bit generator (TRBG) based on a double-scroll attractor. The double-scroll attractor is obtained from a simple model which is quite similar to Chua's circuit in order of tunability and throughput. In order to face the challenge of using the proposed design in cryptographic applications, the proposed TRBG is subjected to statistical tests which are the well-known Federal Information Processing Standard and Diehard test suite in the area of cryptography. The proposed TRBG successfully passes all these tests and can be implemented in integrated circuits. This system is designed for creating more complex algorithm based random bits which will be difficult for the attackers to screw [4]

Prof. S. T. Bodkhe [5], shows how to increase the security of image for transmission over a network up to (16) times in consideration of security of a data or information. While using secret information we need more secure information hiding technique. Instead of one in a single information transmission, a number of spitted blocks gives secure information.

Dudhatra Nilesh, Prof. Malti Nagle [6], proposes the new cryptography algorithm for encryption of data along with the study of other highly used algorithms like AES, DES, Blowfish. The key length for this algorithm is 16 bit. The implementation is totally on the software platform and compares it with other algorithms on the basis of the throughput parameter. The author basically encrypts 128-bit data with the size of the 128-bit key with it.

Hrushikesh S. Deshpande, [7], implements the efficient AES Algorithms on FPGA on the Xilinx ISE 14.1 platform. Author design AES-128 bit algorithm. This proposed architecture consists of a 128-bit symmetric key. This AES design is 3 step approach i.e Top, (1-to 9 round), Last round. Total 4 phase accepted for this algorithm which is proceeding sequential manner. The results of this encryption algorithm provide good performance with a less occupied area.

Ghada F. Elkabbany, Heba K. Aslan [8], proposed a fast parallel-pipelined implementation of AES. In this paper, the design of parallel AES on the multiprocessor platform is presented. This design is based on combining pipelining of rounds and parallelization of mix columns transformation. This analysis increases the degree of improvement of both encryption and decryption by approx 95%.

Saurabh Kumar[9], Shows the improved version of S-box architecture for better performance in the area of delay and power consumption. The implementation of this delayed version is done by programming of Xilinx FPGA with VHDL code also this architecture is implemented on ASIC which also gives better performances of about 16 per cent. The structure of S-Box is basically a multiplicative structure. This new version of S-box is comparing with the conventional structure on the basis of delay and area improvement.

Dr Amit Babiker[10] shows the study of various techniques and algorithm like ECC, AES, RSA used for the secured communication has been done for encryption of data if we choose a longer key length it consumes more power. According to the author according to the comparative analysis of the above mention algorithm, RC4 has the redeeming feature of being fast comparatively, than the above mention algorithms. ECC is based on elliptical curve cryptography, is hard to solve but there are many attacks that

can be successfully broken ECC if the chosen implementation is poor for good security one must use safe curves. ECC structure is complex in the calculation so this hybrid structure leads to wastage of memory and which cause unnecessary wastage of electric power.

IV CONCLUSION

From the literature survey, it is concluded that all cryptography algorithms have their own advantages and disadvantages. Many algorithms are available these days for encryption and decryption purpose. Some are very secure for network security but they require more time for encryption and decryption. Whereas some are taking less time, they are easy to crack. We have presented a review on design techniques to implement digital as well as analog random number generator which can be implemented in FPGA platform. All the techniques and operations over VHDL language is properly studied and discussed. And it is suggested to implement a random number generator as per the requirement of the user and keeping the application in the first priority.

V REFERENCES.

[1]A. Johnson, R. Chakraborty and D. Mukhopadhyay, "A PUF-Enable Secure Architecture for FPGA-Based IOT Applications", *IEEE Transactions on Multi-Scale Computing System*, vol. 1, no. 2, pp. 110-122, 2015.

[2]A. Rukhin, J. Soto, J. Nechvatal, M. Smid and E. Barker, "A Statistical test suite for random and pseudorandom number generator for cryptographic applications", *Nat. Inst. Standards Technol. (NIST),Gaitherburg, MD,USA,DTIC Document, Tech. Rep,*, 2001.

[3]N. Tadic, B. Goll and H. Zimmermann, "Laser Diode Current Driver With (1- t/T)-1 Time Dependence in 0.35-µm BiCMOS technology for Quantum Random Number Generators", *IEEE Transactions on Circuits And System-II: Express Briefs*, vol. 64, no. 5, pp. 510-514, 2017.

[4]M. Yalcin, J. Suykens and J. Vandewalle, "True random Bit Generation From a Double-Scroll Attractor", *IEEE Transactions On Circuits And System I Regular Papers*, vol. 51, no. 7, 2004.

[5]B. Sunar, W. Martin and D. Stinson, "A Provably Secure True random Number Generator with Built-In Tolerance to Active Attacks", *IEEE Transactions On Computers*, vol. 56, no. 1, pp. 109-119, 2007.

[6]A. Johnson, R. Chakraborty and D. Mukhopadhyay, "An Improved DCM- Based Tunable True Random Number Generator For Xilinx FPGA", *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 64, no. 4, pp. 452-456, 2017.

[7]D. Liu, Z. Liu, L. Li and X. Zou, "A Low-Cost Low-Power Ring Oscillator- Based Truly Random Number Generator for Encryption on Smart Cards", *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 63, no. 6, pp. 608-612, 2016.

[8]S. Appaji and D. Acharyulu, "Recent Advancements on symmetric cryptography techniques-A comprehensive Case Study", *Global Journal Of Computer Science And TECHNOLOGY: Graphics & Vision*, vol. 14, no. 2, p. 13, 2014.

[9]M. Qamruddin Khizrai and P. Bodkhe, "Image Encryption using Different Techniques for High-Security Transmission over a Network", *ISSN*, vol. 2, no. 4, p. 8, 2014.

[10]Dudhatra, N. (2014). The New Cryptography Algorithm With High Throughput. *2014 International Conference on Computer Communication and Informatics (ICCCI-2014)*, p.5.

[11] Deshpande, H., Karande, K. and Mulani, A. (2014). Efficient Implementation of AES Algorithm on FPGA. *International Conference on Communication and Signal Processing*, p.5.

[12]Elkabbany, G., Aslan, H. and Rasslan, M. (2014). A Design of Fast Parallel-Pipelined Implementation of AES: Advanced Encryption Standard. *International Journal Of Computer Science & Information Technology (IJCSIT)*, 6(6), p.21.

[13]S. Kumar and V. Sharma, "Law latency VLSI Architecture of S-BOx for AES Encrption",p.4,2014.

[14]S. Mohammed Koko and D. Babiker, "Comparison of Various Encryption Algorithms and Techniques for improving secured data communication", *IOSR Journal of Computer Engineering*, vol. 17, no. 1, p. 8, 2015.