A new method for generating key for cryptography using Deterministic random number generator

P PAVAN KUMAR[1], J MADAN KUMAR[2], M NEELIMA[3]

[1,3]Student, [2]Assistant professor, [1,2,3] ECE department, [1,2,3]Sri Venkateswara College of Engineering and technology, Chittoor, Andrapradesh, India-517127

***Abstract*— Now a day's communication has played a key role in each and every aspect of life. In communication the main problem is security and privacy of sensitive data. The data should be transmitted from sender to receiver without any loss of original information. There are many ways of secure communication. One of those techniques is Cryptography.**

In cryptography there are mainly two mechanisms. They are Encryption and Decryption. In Encryption the sender will convert the original message called plain text into cipher text which is unreadable. Encryption needs encryption key. This cipher text will be send through communication channel to receiver. The receiver needs to decrypt the cipher text into plain text by using decryption key. Here key plays main role. The security of the encrypted message depends on key (encryption and decryption keys, in symmetric encryption both keys are same). The key should be unpredictable, random, and nonlinear and hardware cost for generating key should be less.

There are many ways to generate random keys. In this paper we are proposing a technique called Reseeding mixing Pseudo Random number generator simply RM-PRNG. Advantages of this RM-PRNG are low hardware cost, non linearity, and high throughput. This technique can be used in digital electronics & embedded testing, debugging, stimulation of digital signal processing hardware and digital to analog converters stimulations.

***Keywords*— PRNG-pseudo random number generator, LFSR-linear feedback shift registers, LCG- linear congruential generators, MRG-multiple recursive generator, RCU- reseeding control unit, RC- reseeding counter, ALG- auxiliary linear generator, PG- propagation and generation, EAC- end-around-carry, IC- internal carry, CLA- carry look ahead adder.**

I. Introduction

Cryptography:

The branch of mathematics that investigate the code language and method is called "Cryptography"

Cryptography consists of the following terms. They are plain text, encryption algorithm, secret key, cipher text and decryption algorithm.

Plain text:

It is the original message which is input to the encryption algorithm.

Encryption algorithm:

It performs various substitutions and transformations on the plain text. Encryption is the process of converting plaintext to cipher text.

Secret key:

It acts as input to the encryption algorithm. The algorithm will produce different output depending on the secret key. The exact substitutions and transformations performed by an algorithm depend on the key.

Cipher text:

It is coded message produced as output of encryption algorithm. It depends on plain text and secret key.

Decryption algorithm:

It is an encryption algorithm run in reverse. It takes cipher text and secret key and produces original message. The key need not be same for both encryption and decryption.

Cryptography services are confidentiality, integrity, authenticity, non-repudiation, access control.

Based on the key Cryptography can be classified into two types. They are symmetric encryption and asymmetric encryption.

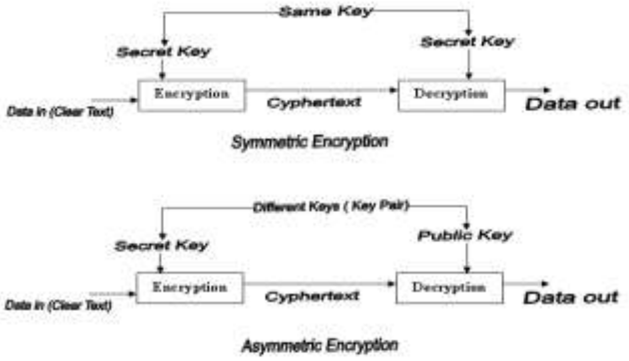

Figure: Symmetric and Asymmetric Encryption.

In Symmetric encryption same key is used at both encryption and decryption system. Same key should be shared between sender and receiver. This will cause key distribution problem. Symmetric encryption is fast action. It will provide only confidentiality. Shared key should be keep secure and distributed through secure channel and Key management headaches from large number of key pairs to maintain N (N-1)/2. Examples: DES, AES, Blowfish, RC4, RC5

In Asymmetric encryption different keys are used at encryption and decryption systems and these keys are mathematically related to each other. Public and private keys used here. Here, large mathematical operations make it slower than symmetric algorithms. It will provide both authentication and non-repudiation. Examples: RSA, El Gamal, ECC, Diffie-Hellman

II. KEY

In cryptography there are so many encryption systems are there. They are substitutions ciphers, transposition ciphers, mono alphabetic ciphers, poly alphabetic ciphers, modular mathematics and one-time pad etc. Whatever the method of cryptography the main issue is Key. Based on the Kickoffs's principle, the security of cryptographic system depends on key only. It doesn't matter how well and how strong the cryptographic system is designed. If the key is week or small the intruders can easily crack the information. many chaotic secure communication schemes explain what the key is, how it should be chosen, and what the available key space is. So, we can't say a cryptographic system is protected without key.

III. DETERMINISTIC RANDOM NUMBER GENERATOR

A PRNG (pseudo random number generator) refers to an algorithm that uses mathematical formulae to produce a sequence of random numbers. PRNGs are also known as deterministic random number generator. A PRNG is a program written for, and used in, probability and statistics application when large quantities of random digits are needed. Many algorithms have been developed to produce truly random sequence of number and endless strings of digits. Theoretically the sequence of numbers is unpredictable because of, randomness. We can't predict next sequence. This system is called pseudo random. PRNGs are a key component of cryptographic system. Because, in cryptography we should not use same key more than one time and key should be unpredictable. PRNGs will generate new key every time and those are impossible to predict. Cryptography needs steady supply of high quality random numbers.

PRNGs start from an arbitrary starting state using seed state. If the starting point in the sequence knows, then with in short time we can generate many numbers that can also be reproduced later. So, these numbers are deterministic and efficient.

PRNGs used in cryptography to generate key are called "Cryptographically Secure PRNGs" (CSPRNGs). The main requirement for a CSPRNG is that it should pass all statistical tests restricted to polynomial time in the size of the seed.

Characteristics of PRNGs are long period random number sequence, should satisfy statistical properties, high throughput rate and unpredictability.

Why RM-PRNG?

Some of the PRNGs are Linear feedback shift register (LFSRs), linear congruential generators (LCGS), and multiple recursive generators (MRGS). PRNGs are good for hardware cost and has high throughput. But, the main disadvantages with PRNGs are due to linear structure easily predictable.

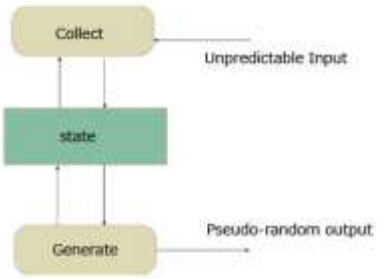

Figure: modal of PRNG.

To overcome this drawback nonlinear Chaos-based PRNGs (CB-PRNGs) are invented. Hardware cost of CB-PRNGs is less expensive and due to nonlinearity output is not predictable. But, due to quantization error key will be short period. Hence, only 1 bit can be generated for one iteration. So, it gives low throughput.

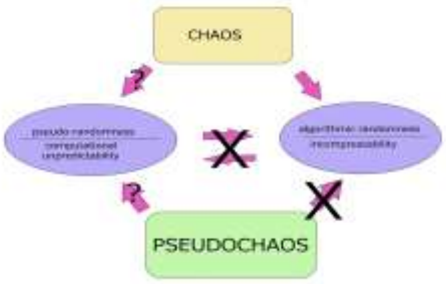

Figure: chaotic and pseudo-chaotic systems.

For high throughput reseeding and mixed techniques are used. This technique is called Reseeding and mixed pseudo random number generator. RM-PRNG is the combination of Chaos based PRNG and multiple recursive generator.

IV. RESEEDING AND MIXED DETERMINISTIC RANDOM NUMBER GENERATOR

RM-PRNG consists of three modules. They are non-linear module, reseeding module and vector mixing module.

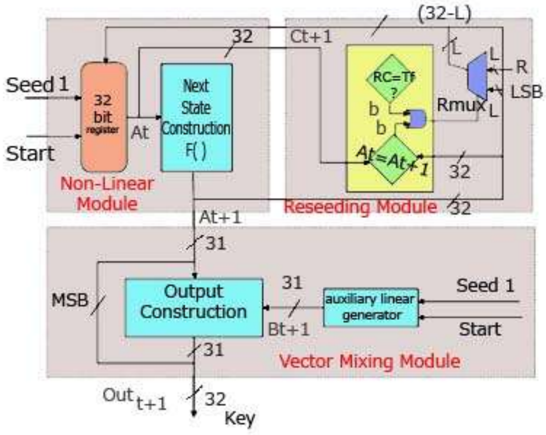

Figure: RM-PRNG.

Nonlinear module

Non-linear module consists of 32-bit register and next state construction function. This module provides the non-linearity behaviour to the key.

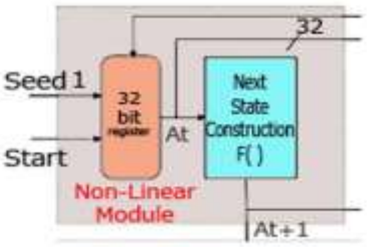

Figure: non-linear module.

Here, 32-bit state register stores the present state value (A_t). In this module by using start command we can set the state value to seed1. The function of next state construction is to produce next state value (A_{t+1}). The recursive formulae in next state is

$$F(A_t)=A_{t+1} = f\,A_t\,(1-A_t),\ t>0 \quad \rightarrow 1$$

So, inputs to 32-bit register are seed1, start and B_{t+1} and output is A_t which is given to next state construction and reseeding module. Output of next state module is A_{t+1} which is given to reseeding module and vector module.

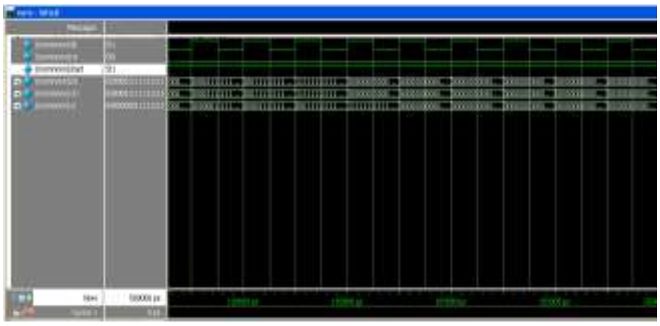

Fig: simulation result for nonlinear module

Reseeding module

Reseeding module consists of Multiplexer and reseeding control unit (RCU). RCU consist of reseeding counter (RC) and comparator. Reseeding counter will count the number of operations until it reaches the fixed point condition. If it reaches fixed point (T_f) it will resets to initial point and state register will loaded through multiplexer, if not reset to fixed point A_{t+1} is directly loaded into state registe

$$C_{t+1} = \begin{cases} A_{t+1}[j], & 1 \leq j \leq 32-1 \\ R[i], & 33-L \leq j \leq 32,\ i=j+L-32 \end{cases}$$

Where, i-bit index and L-integer

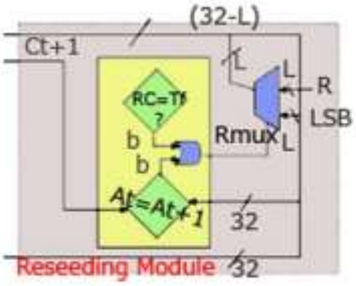

Figure: reseeding module.

Reseeding module will removes the short period in key generation. So, it will increases the throughput.

Fig: simulation result for reseeding module

Vector mixing module

Vector mixing module consists of Multiple recursive generator (MRG) and output construction. An efficient MRG is called as DX generator serves as the auxiliary linear generator (ALG).

$$B_{t+1}=B_t+Y_{DX}.B_{t-1}|M|,\ \ t>7$$

B_{t+1} & A_{t+1} are mixed by XOR operator as follows to form full 32-bit output vector

$$OUT_{t+1}[1:31]=A_{t+1}[1:31]xor\ B_{t+1}[1:31]$$

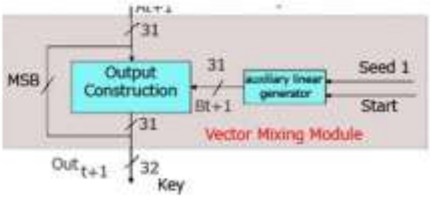

Figure: vector mixing module.

ALG

ALG consists of eight word registers, circular left shift (CLS) operators, circular 3-2 counter and end around carry (EAC) addition operators.

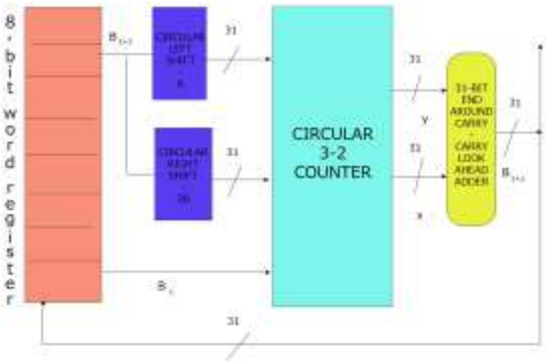

Figure: ALG.

Here, the multiplication and modulus operations are replaced by circular-left shift(CLS) and end-around-carry (EAC) addition operations. The eight-word register is implemented by flip-flops. The Signal B (t-7) is circular-left-shifted 28 and 8 bits for generating two partial products, using module CLS-28 and CLS-8, respectively. A circular 3-2 counter combines three 31-bit operands into two 31-bit operands. Finally, a 31-bit EAC carry look ahead adder (CLA) will add the two 32-bit signals.

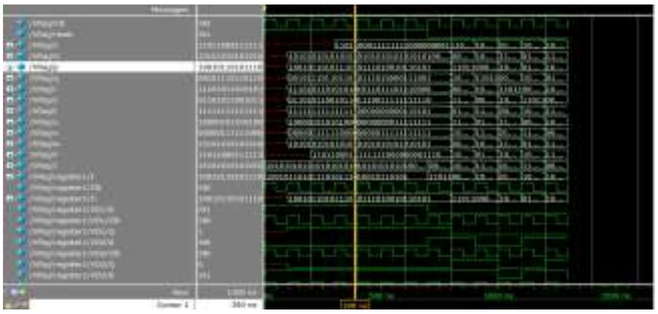

Fig: simulation result for ALG

EAC carry look ahead adder (CLA)

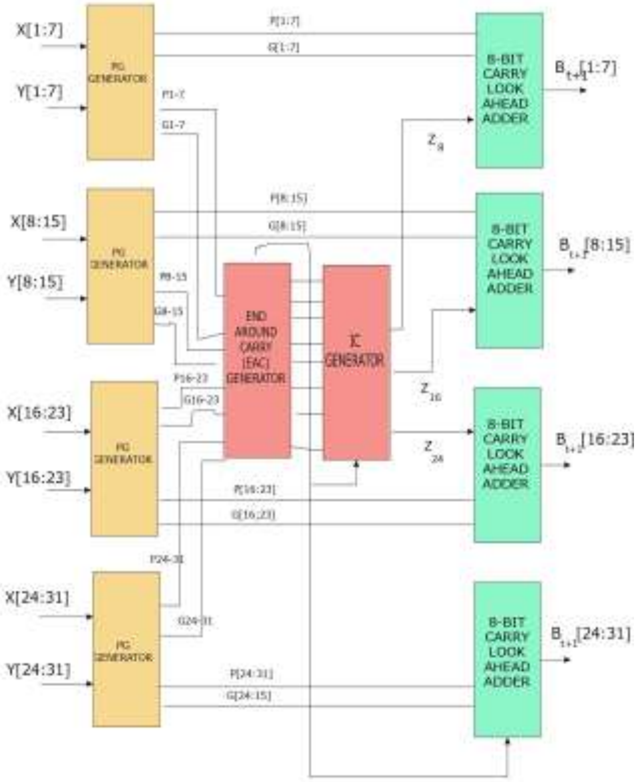

Fig: Structure of the 31-Bit EAC-CLA

EAC-CLA includes four units. They are propagation and generation (PG) generator, end around (EAC) generator, internal carry (IC) generator and CLAs. EAC is generated by group-PGs. EAC is then fed to the IC generator and the least-significant 8-b CLA. The final addition is performed on CLAs.

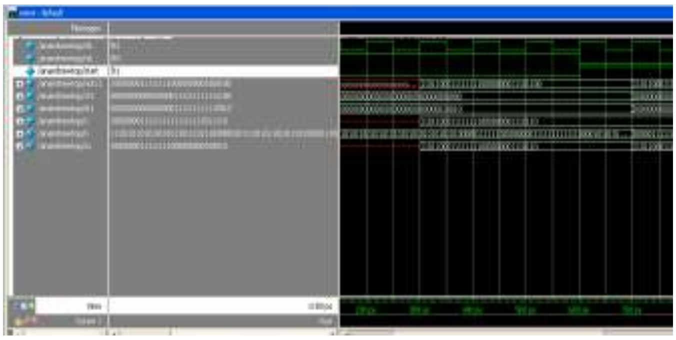

Fig: simulation result for RM-PRNG

V. PROPOSED CRYPTOGRAPHIC SYSTEM

Encryption and decryption technology is where security engineering meets mathematics. It provides us with the tools that underlie most modern security protocols. It is probably the key enabling technology for protecting distributed systems, yet it is surprisingly hard to do right. Encryption and decryption technology is the practice and study of techniques for secure information sharing in the presence of adversaries in encryption and decryption technology.

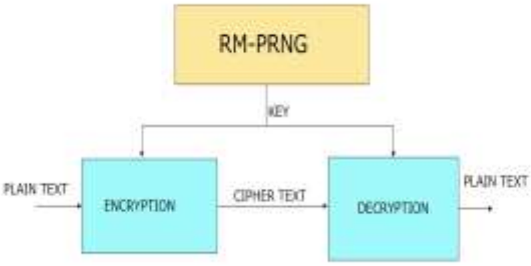

Figure: 4.9Encryption and decryption using non-linear RM-PRNG

Encryption is the process of encoding messages or information in such a way that hackers cannot read it. Encryption and decryption technology is designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. Encryption is the process of converting plain text or information into unintelligible cipher text. Any adversary that can see the cipher text should not know anything about the original message. Decryption is the reverse, in other words, moving from the unintelligible cipher text back to plaintext. The statistical properties of cryptographic methods are the reason for the excellent pseudorandom testability of encryption and decryption technology processor cores and finally the RM-PRNG key using an Encryption and decryption in as shown figure.

In this paper we are proposing one of the cryptographic techniques called Transposition cipher.

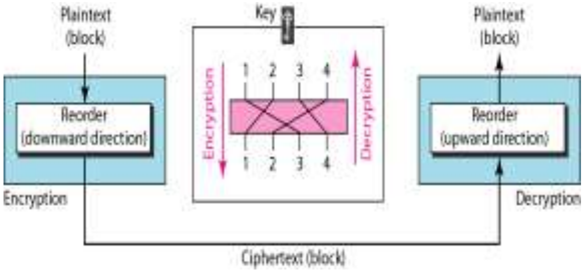

Fig: Encryption and Decryption using RM-PRNG key

The process of mapping by performing some sort of permutation on plain text letters is called Transposition cipher. The simplest such cipher is rail flex in which the plain text written out as a sequence of diagonals and then readout as a sequence of rows. The more complex scheme is to write message in rectangles row by row and read the message of column by column. But, permits the order of columns the order of column then becomes the key of the algorithm. The transposition cipher can be made more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed. Thus, the forgoing message is re-encrypted using same algorithm. To visualise the result of double transposition designate the letters in original plain text message by numbers designating their position.

Figure: simulation results for encryption

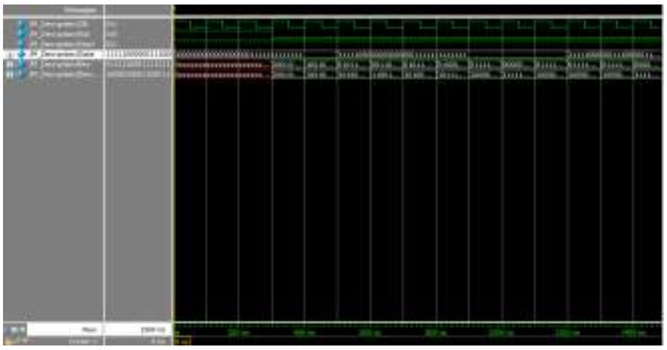

Figure: simulation results for decryption

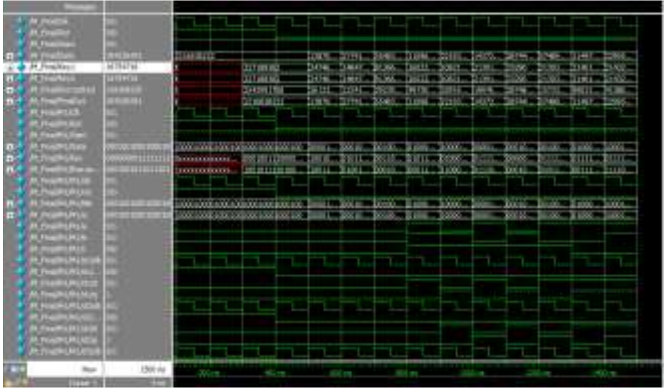

Figure: simulation results for final report

CONCLUSION

Hence, we designed a cryptographic system in transposition technique and the key for this system is given by Reseeding and Mixed Deterministic Random Number Generator method. So, it will offer non-linearity, high throughput and less expensive. The reseeding mechanism solves the short-period problem, while mixing a CB-PRNG with a long-period DX generator extends the period length. Hence, Simulation and Synthesis is observed by ModelSim 6.4b and Xilinx ISE 10.1

REFERENCES

[1]. Chung-Yi Li, Yuan-Ho Chen, Tsin-Yuan Chang, Lih-Yuan Deng and Kiwing To, "Period Extension and Randomness Enhancement Using High-Throughput Reseeding-Mixing PRNG" transactions on (vlsi) systems, vol. 20, no. 2, february 2

[2]. T. Sang, R. Wang, and Y. Yan, "Clock-controlled chaotic keystream generators," Electron. Lett., vol. 34, no. 20, pp. 1932–1934, Oct. 1998.

[3]. D. Mukhopadhyay, "Group properties of non-linear cellular automata," J. Cellular Autom., vol. 5, no. 1, pp. 139–155, Oct. 2009.

[4]. D. Mukhopadhyay,D. R. Chowdhury, and C. Rebeiro, "Theory of composing non-linear machines with predictable cyclic structures," in Proc. 8th Int. Conf. Cellular Autom. Res. Ind., 2008, pp. 210 219, Springer.

[5]. J. E. Gentle, Random Number Generation and Monte Carlo Methods,2nd ed. New York: Springer-Verlag, 2003.

[6]. D. Knuth, The Art of Computer Programming, 2nd ed. Reading, MA: Addison-Wesley, 1981.

[7]. Klapper and M. Goresky, "Feedback shift registers, 2-adic span, and combiners with memory," J. Cryptology, vol. 10, pp. 111– 147, 1997.

[8]. D. H. Lehmer, "Mathematical methods in large-scale computing units," in Proc. 2nd Symp. Large Scale Digital Comput. Machinery, Cambridge, MA, 1951, pp. 141–146, Harvard Univ. Press.

[9]. S. Li, X. Mou, and Y. Cai, "Pseudo-random bit generator based on couple chaotic systems and its application in stream-ciphers cryptography," in Progr. Cryptol.-INDOCRYPT, 2001, vol. 2247, pp. 316–329, Lecture Notes Comput. Sci.

BIOGRAPHIES

	P PAVAN KUMAR, M.Tech, (VLSI) student, Sri Venkateswara College of Engineering and Technology, Chittoor, Andrapradesh, India-517127
	J MADAN KUMAR, M.Tech, Assistant Professor (ECE department), Sri Venkateswara College of Engineering and Technology, Chittoor, Andrapradesh, India-517127
	M NEELIMA, M.Tech, (VLSI) student, Sri Venkateswara College of Engineering and Technology, Chittoor, Andrapradesh, India-517127