

Furtherance In Encryption Algorithm

(Clocking Rule of A5/1)

Rosepreet Kaur Bhogal, Ajmer Singh
School of Electronics and Electrical engineering
Lovely Professional University
Phagwara, India

rosepreetkaur12@gmail.com, ajmersinghbhinder@gmail.com

Abstract— The digital mobile network uses an encryption algorithm known as A5/1. It is basically used to encrypt while transmitting selective information starting from mobile station to base station during an activity of conveying information. A5/1 is one of the strong algorithms but it can analyze and decipher by intruders. A5/1 use linearity complexity, clocking taps etc. based methods for cryptanalysis. However, in this paper the modified algorithm has been given, which enhance the efficiency of A5/1 encryption algorithm based on the clocking mechanism of LFSRs (Linear-feedback shift register). The modified technique of A5/1 is become fast and easy to carry out which improve something for future. National Institute of Standards and Technology (NIST) has defined some statistical tests which used to verify the security of A5/1. These test results in context to assure the choice of generated bit stream acquire by LFSR.

I. INTRODUCTION

The transmission is the essential and best suited for sharing useful information during the Wireless communication technology [7]. It is set up nice example of the wired free communication. However, every information could be secure that nobody can detect what actual is the information. For this protection, cryptography plays a vital role. For transmitting information from the one place to other station, an air interface where severe security is requires between the communicating parties [10]. The point come to attention, how can assist while communicating? For that, an encryption algorithm has been using in the GSM as with series of A5/x. These algorithms are using to encrypt important information over the link. The required execution of encryption/decryption design are like, A5/0 has not having any inscribe, A5/1 is called the strong version for securing the content, A5/2 is called as weaker variant attention in rest of the world except Europe and third is A5/3 which is based on block ciphering called well-built version made as part of the 3rd generation partnership project (3GPP) [5].

The research explores about A5/1 that is promising edition but has some weakness due to the cryptanalysis. A5/1 is using stream ciphering process [1] that is using the bit-by-bit Exoring. It involves two processes that are encryption and decryption. Encryption is that which alter our useful information like nobody can detect our actual information. It is performing with the help of a secret key. Consider an example of encryption that performs by taking a plaintext in the form of binary data and then XOR with a key. This is cipher text and the process is called encryption. Similarly, the reverse process is called decryption in which get plain text back by using the key.

In cryptography, the correlation is one of the attacks that is a group of plaintext attacks. During the deciphering process, stream ciphers (SC) generated the stream, these streams uses as key. Correlation attacks [6] having an analytical weakness. It is possible to choose a function which avoids correlation attacks, so this

type of cipher is desirable secure. This is necessity to study the way which easily affected the correlation attacks when generating the stream ciphers through encryption algorithm.

The encryption algorithm which is built using linear feedback shift register (SR). The starting values of SR is known as seeds. The operation of the SRs [12] can be determine stream values generated by SRs is finding by its present or past state bits. But, SR is the common feedback function (FF) which can generate a series of bits this generated bit stream is random in nature and large repeating cycle [2].

This paper is about modification in the clocking mechanism of stream cipher which is determining on majority rule. The description of encryption algorithm has been given in section 2. In section 3 is contain the description of correlation attack analysis. The enhanced structure of A5/1 key stream generator (KSG) has been detail explained in coming sections. In section 5, about statistical testing with a brief description of all test considered by NIST test suite. The last section, is having the comparsion between the existing and modified version of A5/1.

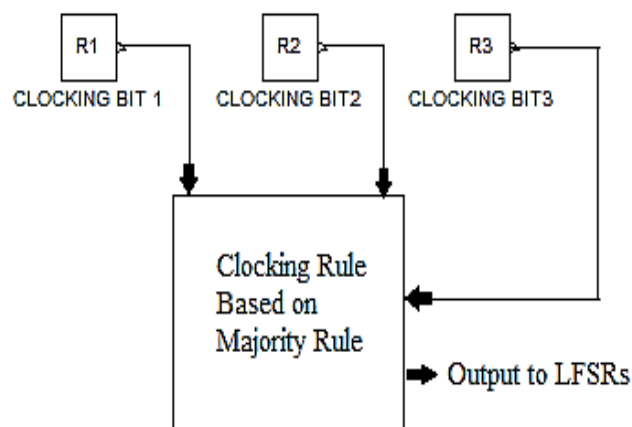


Figure 1. Clocking mechanism using M-rule for A5/1.

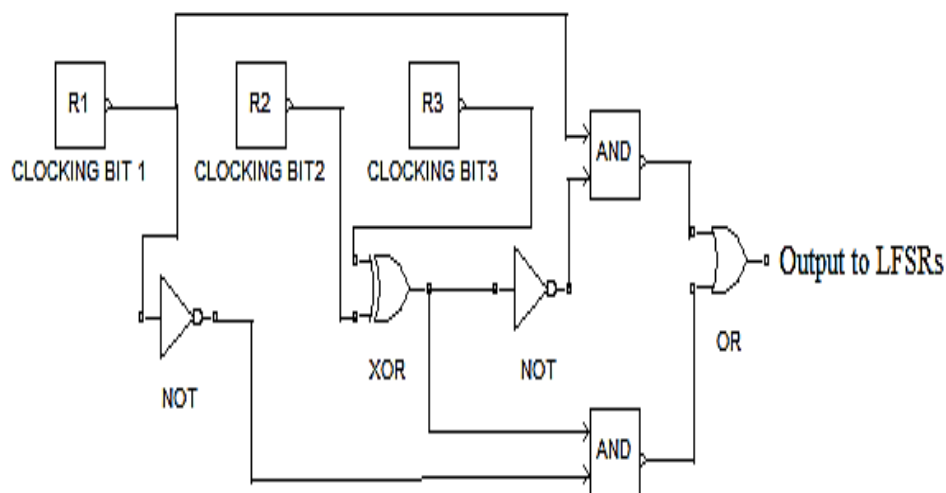


Figure 2. Clocking mechanism of modified A5/1 stream cipher based on 'y'

II. STRUCTURE OF A5/1

A5/1 is the SC [11] which provide key bit sequence. It contains three SR with length of 19 bits, 22 bits and 23 bits uses to create a long binary sequence. The 228 bits length of data being used during communication, where 114 bits are used for both encrypted and decrypted data [4]. A5/1 initialize the 64 bit length of key combine with 22 frame number, the tapping position of register R1 is 13th, 16th, 17th & 18th for R2 is 20th & 21th and for R3 is 7th, 20th, 21th & 22th. Clocking of every LFSR is based on majority rule. Variable A, B, C represent the clocking bit of register R1, R2 and R3 respectively, where 8th, 10th & 10th position bit are uses for clocking bit of R1, R2 & R3 respectively as mentioned in Figure 3. To select the register/s to clock, the clocking bit of all three register are given to the Boolean function given in equation 1. The value of X will compare with each clocking bit, where it matched the respective register will clock to generate the next bit. Then, leftmost bit of selected register will shift to the right, the new generated bit will store at the leftmost locations in figure 2. According to the majority rule every LFSR will clock with the probability of 0.75 [8]. Table 1 shows the possible instance for a register to clock. This clocking rule have more probability of correlation attack [3].

$$X = A.B \oplus B.C \oplus A.C \quad (1)$$

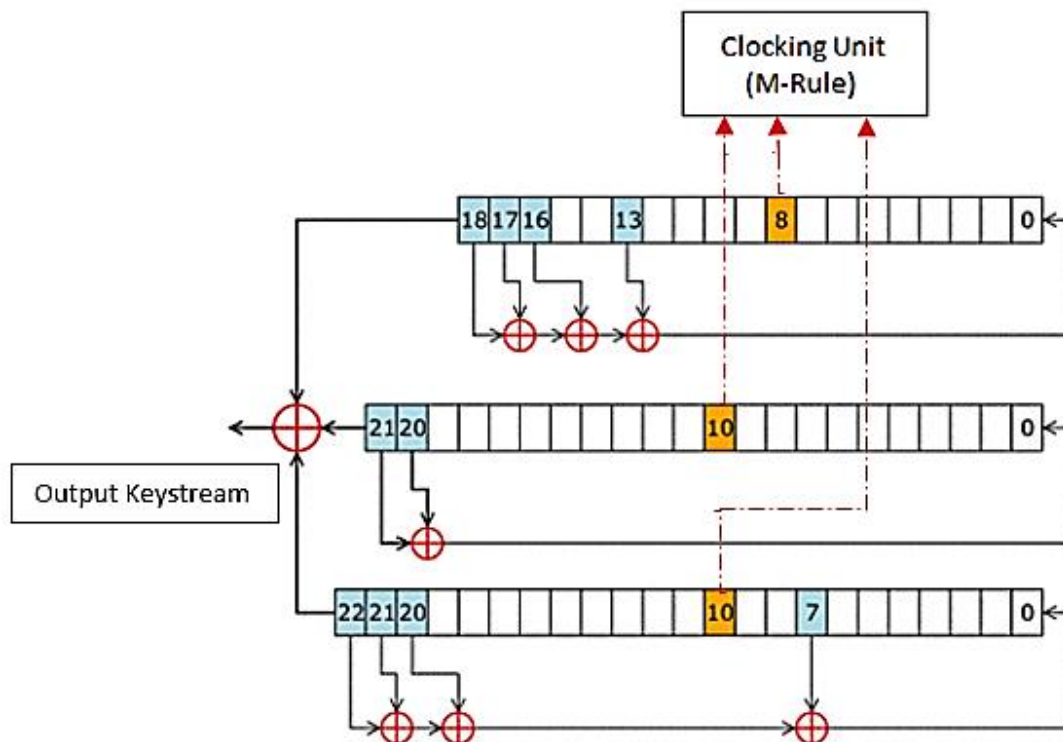


Figure 3: Basic A5/1 stream cipher

III. BRUTE FORCE AND CORRELATION ATTACK

A stream cipher is considered to be good, if the correlation of generated bit stream is less and the linear complexity of generated bit stream is high. High linear complexity is very important factor because low linear complexity will lead to the success of Berlekamp Messey algorithm, which can predict the bits are related to the generated sequence of LFSR. Less correlation and high linear complexity will lead to the more non-linear behavior of the generated sequence. So, the probability of getting a success correlation attack increase if the final output of stream cipher is correlated with the output of any one LFSR. If the internal states output is relating with final output sequence then the entire stream cipher can break. This stream cipher is using three LFSRs and clocking feedback polynomials look strong but using cryptanalysis it is weak cryptographically. If information about feedback is known, then the starting bit of any LFSR can be determine by intruders. With increase in matching percentage of any LFSR with the output bit sequence, the probability of right guess will increase also. So, in existing A5/1 algorithm 75% of output bit sequence is matching with the internal state sequence [8], which is known as plaintext attack. Like, the brute force attack takes place on individual LFSR.

So, to reduce the success of brute force attack the clocking probability should be 50% instead of 75%. Because 50% probability of clocking feedback scheme will yield to more randomness in output sequence of bits.

IV. MODIFIED A5/1 STREAM CIPHER

The modified clocking scheme has been made to reduce the probability of 0.75 to 0.5. The modified A5/ 1 structure of stream cipher is shown in figure 4.

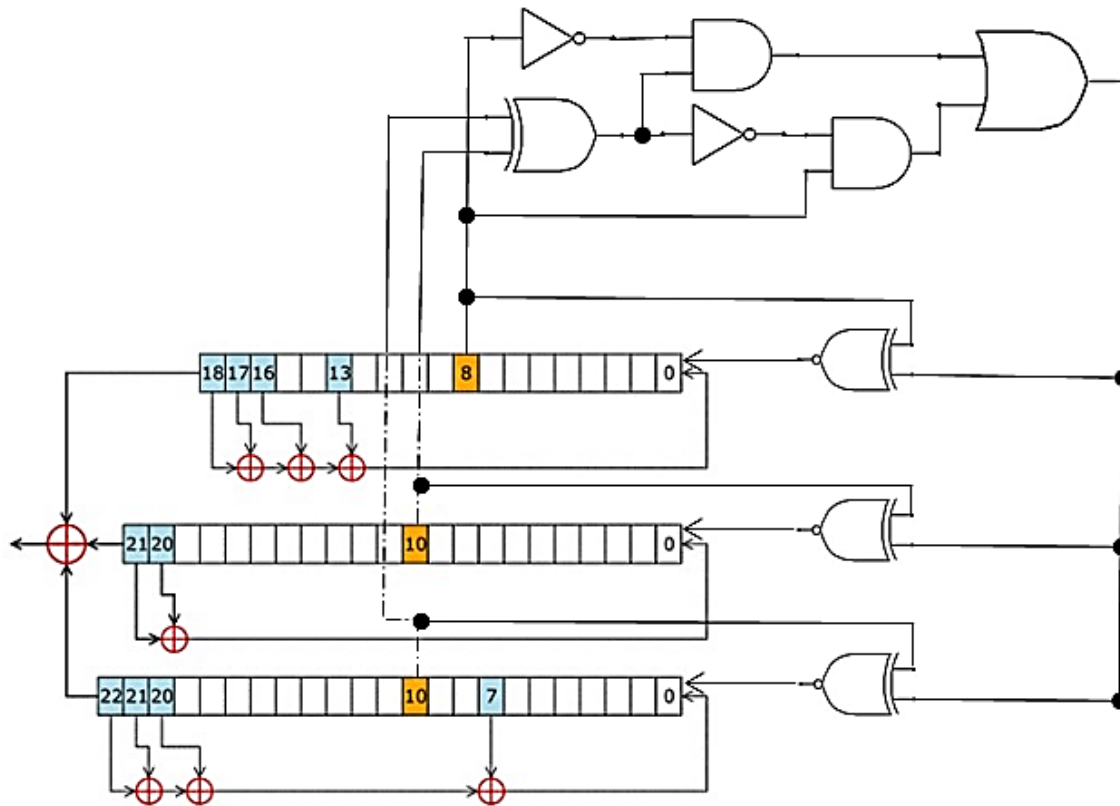


Figure 4: Structure of Modified A5/1 stream cipher

A. Clocking controlling unit

In the clock controlling scheme in figure 2, the register will clock according to the tap position calculate output. The clocking bit is calculated with the given Boolean algebra for expression in equation 2. The is equation given as below:

$$Y = \bar{A} \cdot (B \oplus C) + A \cdot (\bar{B} \oplus \bar{C}) \quad (2)$$

TABLE 1: POSSIBLE CASES OF A5/1 AND A5/1 MODIFIED STREAM CIPHER REGISTER TO CLOCK

Clocking bit			A5/1				Modified A5/1			
A	B	C	X	Register Clocked 1: Yes, 0: No			Y	Register Clocked 1: Yes, 0: No		
				R1	R2	R3		R1	R2	R3
0	0	0	0	1	1	1	0	1	1	1
0	0	1	0	1	1	0	1	0	0	1
0	1	0	0	1	0	1	1	0	1	0
0	1	1	1	0	1	1	0	1	0	0
1	0	0	0	0	1	1	1	1	0	0

1	0	1	1	1	0	1	0	0	1	0
1	1	0	1	1	1	0	0	0	0	1
1	1	1	1	1	1	1	1	1	1	1

TABLE 2: AVERAGE OF 100 KEY STREAMS EXISTING AND MODIFIED A5/1

Tests	P-value (A5/1)	P-value (Modified A5/1)
Approximate Entropy	0.11294192	0.11356817
Block Frequency	0.50925444	0.51980295
Cum Sum Forward	0.474555	0.5436332
Cum Sum Reverse	0.4565333	0.53749007
DFT	0.61447459	0.63303992
Frequency	0.47850504	0.52737295
Lempel Ziv	1	1
Linear Complexity	0.49111928	0.53545316
Longest Run	0.4610171	0.51616916
Overlapping Template	0.45930098	0.49203098
Rank	0.43123195	0.47496719
Runs	0.57857773	0.46296932
Serial Test 1	0.46556593	0.55040955
Serial Test 2	0.47076616	0.51397941

The expression of output ‘Y’ is formed by concept that of probability will become 0.5. For each cycle of shift register whose clocking tap is agree with ‘Y’ that register will clock. In Table 1, earlier every cycle the registers are clocked with 75% of probability. This probability has been reduced to 50% where at least one LFSR will clock at one time.

V. STATISTICAL TESTING

Generators are unpredictable, it is an important to analysis with statistics that the output came by key stream generator is random or not. For this, NIST provided different tests is used to check the pattern of randomness. The cryptographic applications are requiring the generation of the random bit sequences. It tests deviation from randomness with respect calculate proportion-values (p-values) correspondence to tests. Once a generator to be selected, a series of binary sequences are to be generated and saved file for analysis [10].

A. NIST Test Tool

The NIST test tool is requires to test the significance level of the random bit sequences. Each test result in the p-value which lies between 0 and 1. Higher the p-value, the result is more significance. The given random sequence passes the test if resultant value is greater than 0.01 as per standard for cryptographic applications. The significance value shows the probability of expectation of coming particular sequence in hundred sequences to be rejected. If the resultant p-value is greater than or equal to 0.01 then it indicates

as the bit sequence is random with 99% confidence level else the sequence will not suitable for cryptographic application[10].

B. Test Summary

Here consider following test their description as follows:

- 1) *Frequency Test*
 - a) *Input*- Bitstream, sequence length (n)
 - b) *Procedure* - Compute the frequency of one's (or zeros).
 - c) *Defect Detected*- Either there are too many ones or there are too many zeros.
- 2) *Cumulative Sum Test*
 - a) *Input*- Bitstream, sequence length (n)
 - b) *Procedure*- Computes the maximum of the partial sums of the shifted bit stream values.
 - c) *Defect Detected* – In the initial stages, either more numbers of ones or zeros.
- 3) *Runs test*
 - a) *Input* –Bitstream, sequence length (n)
 - b) *Procedure* - Compute the total number of runs of zeros and ones in the bit stream.
 - c) *Defect Detected* – The large value indicates more runs and small values indicates less runs in the bit stream.
- 4) *Rank test*
 - a) *Input*- Bitstream, sequence length (n), block length (m)
 - b) *Procedure* - Construct n matrices (m x m) from the bit stream. For each matrix, determine its rank & compute a chi-square statistic based on the theoretical distribution of rank.
 - c) *Defect Detected* – Shows the deviation from random sequence in rank distribution.
- 5) *Spectral test*
 - a) *Input*- Shifted sequence, sequence length (n)
 - b) *Procedure* - Apply the DFT on the shifted sequence and then determine its modulus.
 - c) *Defect Detected*- Detects the periodicity in the bit stream.
- 6) *Template matching test*
 - a) *Input* –Bitstream, sequence length (n), block length (m), template
 - b) *Procedure* - Compute the # of times b appears in the bit stream.
 - c) *Defect Detected*- More occurrences of un-periodic templates and more occurrences of m-runs of ones.
- 7) *Approximate Entropy test*
 - a) *Input* – Bitstream, block length (m)
 - b) *Procedure* - Compute the bit stream block frequencies. And then compute APEN (Approximate entropy).
 - c) *Defect Detected* – Strong regularity results when values of APEN (m) is small.
- 8) *Linear complexity test*
 - a) *Input* - Bitstream
 - b) *Procedure* - Compute the connection polynomial for the bit stream.
 - c) *Defect Detected*- The complexity of sequence is less so, cannot consider as random.
- 9) *Lempel-Ziv compression test*
 - a) *Input*- bit stream

b) *Procedure*- Measures the rate at which new patterns appear in a sequence. Construct a dictionary from the bit stream. Add a new word to the dictionary that has never appeared there before. Count the number of words in the dictionary.

c) *Defect Detected*- More compressed than a truly random sequence.

10) Serial test

a) *Input*- Bitstream, sequence length (n), block length (m)

b) *Procedure*- Determine possible overlapping frequency of all m -bit blocks

c) *Defect Detected* – Non-uniform distribution of specific length words

VI. NIST TEST RESULT

This section shows the significant improvement of modified keystream generator over existing A5/1. The implementation of proposed and the existing A5/1 algorithm has been tested through NIST Test tool. The test has been conducted for 100 different key streams of **10000** bits each. Average p-value of 100 key streams shown in the Table 2, which shows the improvement of the proposed method [10].

A. Existing A5/1 Key Stream Generator results

The average of 100 different key stream result of existing A5/1 collected as shown in Table 2. All result came above significance level i.e. $p\text{-value} \geq \alpha$ which is 0.01 with the status of test success illustrated in figure 5.

B. Modified A5/1 Keystream generator results

In order to test characteristic of the modified A5/1 key stream generator, that simulation program based on clocking cases mentioned in Table 1. This configuration was used to generate the test files necessary for carrying out the NIST test. All result taken from a sample size 1000000 bits. In Table 2, the result came from NIST test suite for modified A5/1 key stream generator p-values more than p-values of existing A5/1 except one that ran the test. However, that test also not exhibits that much difference. Figure 6, a graph of the p-value with respect to correspondence tests. The p-value came above significance level shows that all test is pass as a consideration that p-value should be greater than equal to alpha.

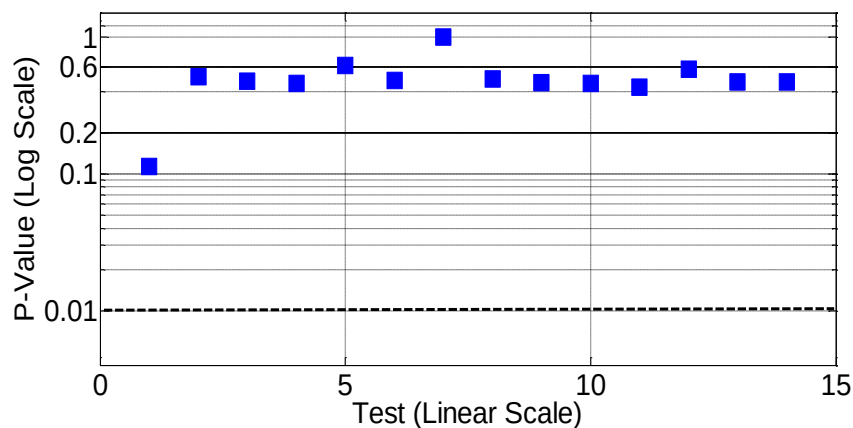


Figure 5: NIST Test result for 100 key streams ($P\text{-Value} \geq \alpha$)

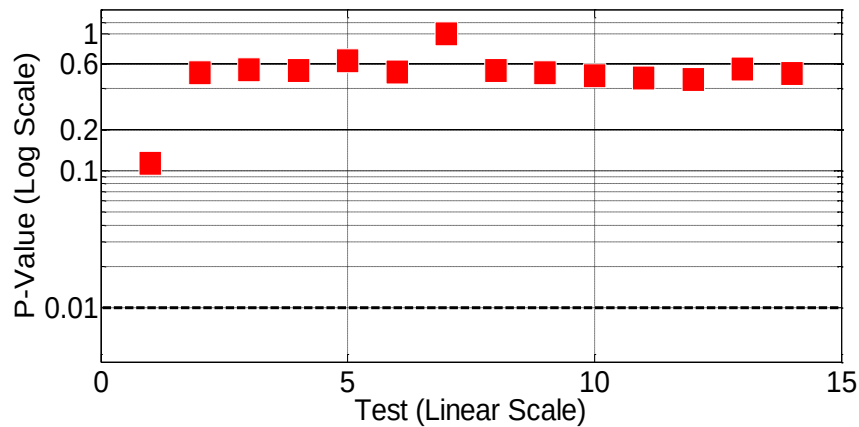


Figure 6: Test result for 100 key streams ($P\text{-Value} \geq \alpha$)

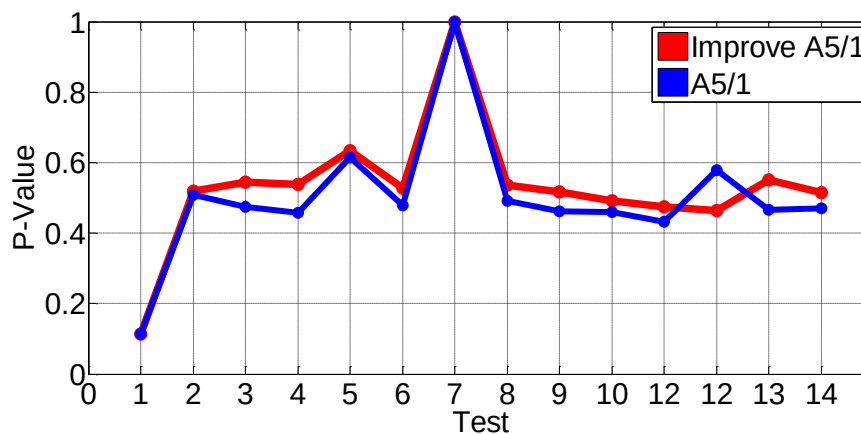


Figure 7: Result using Test for 100 key streams for proposed A5/1

C. Comparison of proposed A5/1 with A5/1

From the experiment, it can be seen that modified A5/1 design provides a good source of a random number for cryptographic purposes. In figure 7, average result of 100 key streams of length 10000 came with the NIST test tool.

VII. REDUCTION OF AUTO-CORRELATION FACTOR

The Modified mechanism for clocking an LFSR in A5/1 the correlation attack is reduced. If determine autocorrelation factor value for both existing and modified A5/1 by eliminating the maximum value of autocorrelation factor. However, value came for existing A5/1 was 0.0379 and similarly, for modified A5/1 was 0.0288. If consider the difference between two values comes 0.0091. From this result, we can say that correlation reduces.

VIII. CONCLUSION

The key stream generator can efficient to implement and it is effective algorithm for encryption using for communication as an application of GSM [12]. Therefore, it exhibits drawback as if the length of LFSRs is short and attack by intruder i.e. correlation. With analysis, this way of using will decrease the possibility

of correlation attack. The previous clocking mechanism has been improved for enhancing the security. With this the possibility of attacks have been reduce and security will increase. The clocking probability has been reduced to 0.5. Therefore, it enhances security and help to not predict output sequence bits which uncorrelated with output sequence up to 6 cycles. Hence, the A5/1 stream cipher is shown in the section 3. The randomness of key stream has been proving by various tests. This proposed strategy will have a speed and less cost for A5/1 key stream algorithm.

REFERENCES

- [1] E. Barkan, E. Biham, and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted communication," *Journal of Cryptology*, vol. 21, no. 3, pp. 392–429, Sep. 2007. David Margrave, George Mason University, "GSM Security and Encryption".
- [2] O. Dunkelman, N. Keller, and A. Shamir, "A practical-time attack on the A5/3 Cryptosystem used in Third generation GSM Telephony," 2010.
- [3] Greg Rose, "A précis of the new attacks on GSM encryption, " 2003 ,QUALCOMM Australia.
- [4] "Communication security in GSM networks," 2008.
- [5] Musheer Ahmad and Izharuddin, "Enhanced A5/1 cipher with improved linear complexity," 2009
- [6] M. Tkl and Peuhkuri, "Mobile networks security history of mobile phones," 2008.
- [7] N. Komninos, B. Honary, and M. Darnell, "Security enhancements for A5/1 without loosing hardware efficiency in future mobile systems," 2002
- [8] Chi-Chun La and Yu-Jen Chen, "Stream Ciphers for GSM Networks, " 2000, Institute of Information Management, National Chiao-Tung University.
- [9] http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html.
- [10] Bruce Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C," Second Edition. Jon Wiley & Cons, Inc. 1996. ISBN 0-471-12845-7. Page 382 of section 16.4: Stream Ciphers Using LFSRs.
- [11] Patrik Ekdahl, "On LFSR based stream cipher, " *Analysis and Design*, 2003, Lund University.
- [12] Aoran Sun, Qun Ding, "The design of the mobile phone module information encryption system based on FPGA, " 2016.