Information Security Enhancement by Increasing Randomness of Stream Ciphers in GSM

Ram Prakash Prajapat[1]
SDE, BSNL
Jodhpur, Rajasthan
India

Dr. Rajesh Bhadada[2]
Professor and Head
MBM Engg. College
Jodhpur, Rajasthan, India

Arjun Choudhary[3]
Centre for Cyber Security
Sardar Patel University of Police
Jodhpur, India

Abstract—**Information security is a crucial issue and needs to be addressed efficiently. Encryption of the original information is used to ensure privacy during exchange of information. In GSM (Global System for Mobile) standard, once the voice traffic initiates after signaling, encryption comes into the picture to ensure privacy during the call, after authentication. Here in this process, the plaintext is encrypted in to cipher-text using stream ciphers. For stronger security, strong ciphers with strong randomness are required. Linear Feedback Shift Registers (LFSRs) based A5 algorithm family is used for encryption in GSM. There are many shortcomings of this cipher and with these, privacy can't be assured. Some ways are proposed in this paper to ensure better security by enhancing the randomness of the generated bit stream being used for encryption. These are incorporation of user's current location, reuse of already generated 32 bit SRES during authentication process and conversion of linear FSRs into nonlinear FSRs. Statistical Test Suite NIST is used to test the various properties of random bit stream and an attempt has been made to achieve better randomness, hence more security.**

Keywords—Security; encryption; A5/1 stream cipher; randomness; NIST test suite

I. Introduction

Although with the advancement of technology, many vulnerabilities of security threats of GSM have been addressed in EDGE, 3G (HPA/HSDPA) & 4G (LTE) but this is still relevant as large number of people use GSM specially in rural areas. In addition to this, stream ciphers are used in many other wireless applications like modems / routers, smart appliances & security devices. Few algorithms like A3, A8 & A5 are used in GSM for authentication & encryption process over A_{bis} air interface between user mobile (MS) and base station (BS). The details of inputs, outputs & use of these algorithms are described in Table I. Here the SRES is Signed Response of 32 bits, K_c is a 64 bits Cipher Key and RAND is a 128 bits random number. Fig. 1 shows that the combination of K_c, RAND and SRES is called "Triplet".

A5 is mainly responsible for encryption as shown in Fig. 2. Here by using Cipher Key K_c of 64 bits along with TDMA Frame number F_n, a 228 bits pseudo random number PRAN is generated which is XORed with 228 bits plain-text in bit-by-bit manner to get cipher-text. This cipher form of information after encryption is finally transmitted over the air interface between the user mobile station & base station.

Two stage security, i.e. "Authentication" & "Encryption" is implemented in GSM. Initially, the access of the network resources is granted to any new or existing subscriber on its request after authentication process on every location update.

During this "Authentication Process", the core network challenges MS and in response to this, MS sends SRES. This is matched with the SRES available with itself and grants the access on matching only as described in Fig. 3. After getting the access of the network, the encryption process takes place to ensure the privacy during the call. Here in this process, the plaintext is encrypted in to cipher-text using stream ciphers of A5/1 algorithm. In the same way, decryption occurs at the other end to reconstruct the original information.

As the transmission of information is bursty in nature in GSM, the 114 bit frame sequence in downlink (BS to MS) & the same way a 114 bit frame sequence in uplink (MS to BS) is transmitted every 4.6 milliseconds. K_c is produced and mixed with a publically known TDMA frame number Fn for each frame for every new voice call.

The configuration of A5 was never shared by the ETSI [1]. Although, it got reverse engineered & became available to all. Many crypto attacks occurred by cryptanalysts to reveal the internal structure of this algorithm and hackers & intruders managed to decrypt the transmitted information by users. Golic [2, 3] presented the functional design in the year 1994 and later Marc Briceno [4] revealed the entire design by reverse engineering in the year 1999 [15,16,17,19,20].

TABLE I. ALGORITHMS USED FOR INFORMATION SECURITY IN GSM

Algorithm	Inputs	Output	Purpose
A3	K_i (128 Bits)	SRES (32 Bits)	Authentication Process
	RAND (128 Bits)		
A8	K_i (128 Bits)	K_c (64 Bits)	Cipher Key Generation (K_c)
	RAND (128 Bits)		
A5	K_c (64 Bits)	Cipher Text (228 Bits)	Encryption Process (Voice & Data)
	TDMA Frame No. (22 Bits)		
	Plain Text (228 Bits)		

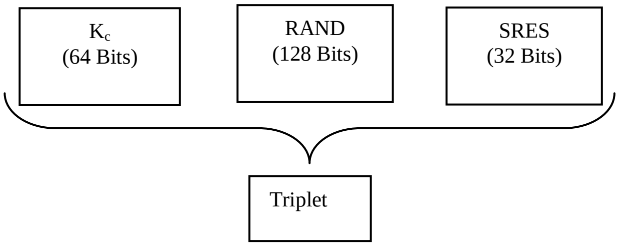

Fig. 1. Triplet Details.

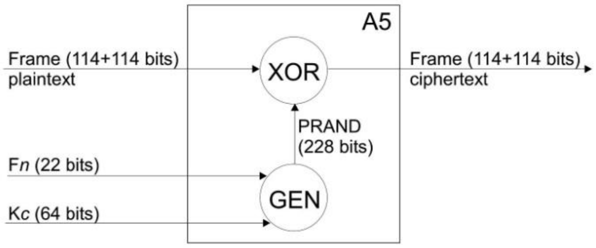

Fig. 2. Encryption by A5/1 in GSM.

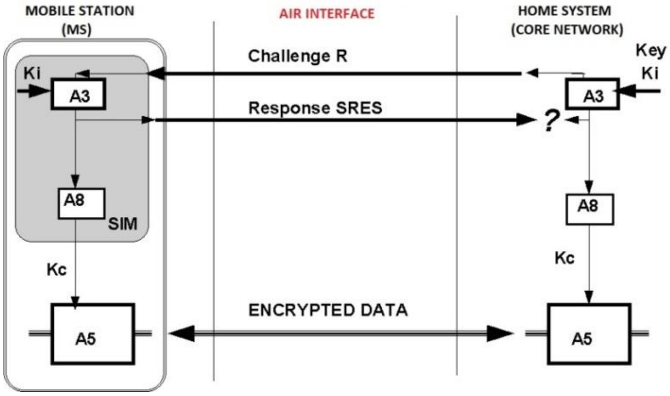

Fig. 3. Authentication and Encryption Process.

Biryukov, Wagner and Shamir [6], Ekdahl and Johansson [10], Dunkelman and Biham [5], Maximov & team [11] and Barkan [14] contributed lot. Contribution of Andrew Rukhin et al [8], N. Komninos [9], Basar Kasim [12, 13] is also remarkable. Very recently, Darshana Upadhyay, Priyanka Sharma & Sharada Valiveti [18], Sattar B. Sadkhan [21,24,26] & Nagendar Yerukala [27] made some modifications by changing of feedback taps in A5/1 stream cipher to improve the randomization property to make it robust to attacks [22,23].

Many cryptanalysts proved that due to weaknesses of this stream cipher, information security can be compromised in GSM [25, 28, 29]. These weaknesses are:

1) Weak Linear Complexity (LC).
2) Poor clocking system (Majority Function Rule).
3) Clocking period is too short.
4) Poor clocking taps selection.
5) Collision issue.

Using an improved clocking system with a combinational function of high correlation immunity and high algebraic degree, the security can be increased [6, 11].

Logisim simulator (primarily developed by Dr. Carl Burch) is used to realize the structure of the proposed A5/1 algorithm and its randomness parameters are analyzed by NIST Suite [7]. Brief description about the internal structure of A5/1 is given in Section II, modifications are proposed in Section III, observations and randomness analysis is given in Section IV and Section V concludes the results.

II. Internal Structure of A5/1

It has three Linear Feedback Shift Registers (LFSRs) of different bit lengths to generate a pseudo random binary stream. The total bit length of this cipher is 64 bits in which LFSR-1 (R1) has 19 bits, LFSR-2 (R2) has 22 bits, and LFSR-3 (R3) has 23 bitsas depicted in Fig. 4.

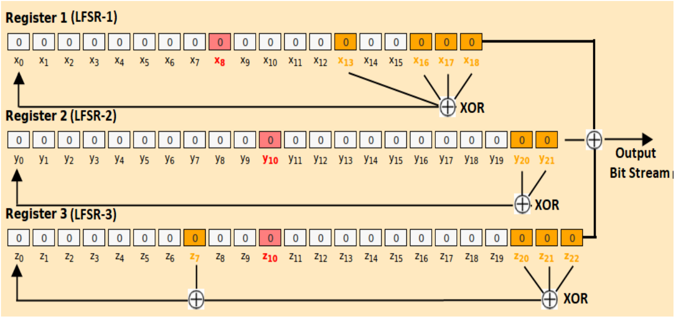

Fig. 4. Internal Design of A5/1.

Following its own feedback polynomial, periodic bit sequence is generated by these registers. The feedback bit positions are predefined at 13, 16, 17, 18 and 20, 21 and 7, 20, 21, 22 for R1, R2 and R3, respectively.

Similarly, the single clocking taps of these registers are also predefined at tap 8, 10, and 10 for R1, R2 and R3, respectively. Bit length, clocking bit, tap bits and primitive polynomial are shown in Table II.

TABLE II. Information Table for LFSRs

LFSR	Length (in bits)	Clocking Bit	Tap Bits	Primitive Feedback Polynomials
R1	19	8	13, 16, 17, 18	$x^{19}+x^{18}+x^{17}+x^{14}+1$
R2	22	10	20, 21	$x^{22}+x^{21}+1$
R3	23	10	7, 20, 21, 22	$x^{23}+x^{22}+x^{21}+x^{8}+1$

TABLE III. Majority Rule Truth Table

Clocking Bit			Majority Function	Clocked LFSR		
R1	R2	R3		R1	R2	R3
0	0	0	0	Yes	Yes	Yes
0	0	1	0	Yes	Yes	No
0	1	0	0	Yes	No	Yes
0	1	1	1	No	Yes	Yes
1	0	0	0	No	Yes	Yes
1	0	1	1	Yes	No	Yes
1	1	0	1	Yes	Yes	No
1	1	1	1	Yes	Yes	Yes

The clocking mechanism of each register is decided by Majority Rule as shown in the truth table Table III below. For each cycle, only those registers will be clocked and updated whose clocking bit values have majority. The majority value m is decided by m = *maj* (C1,C2,C3), here C1, C2 and C3 are the clocking bits of all three registers.

In simple words, “at least two out of three” is the majority rule i.e. the majority among these bits. If two or more clocking bits are 1, the majority value m will be 1, and similarly if two or more are 0, the majority value m will be 0.

Thus, in this mechanism, two or more, whose clocking bit is the equal to m, will be clocked at each clock cycle. Every register has the clocking probability of 0.75 and non-clocking probability of 0.25. The majority rule function can be realized using logic gates as shown below in Fig. 5 (Logisim simulator).

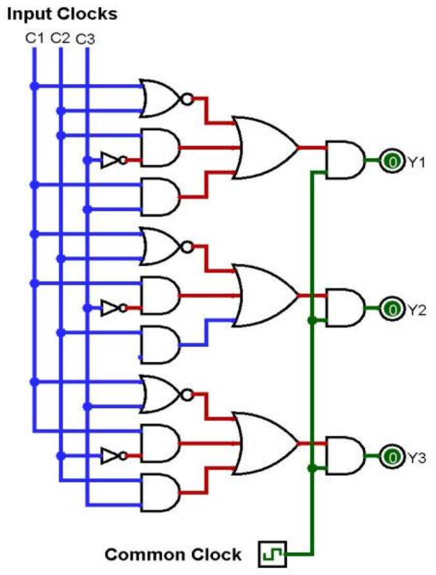

Fig. 5. Realization Majority Function in Logisim.

All three registers are reset by setting a zero value. In next 86 cycles, K_c and Fn are loaded bit by bit with regular clocking. The output ignored during initial stage of the first 100 clock cycles and during this period the irregular clocking continues for all three LFSRs as per the majority rule. Now the required random bit stream of 228 bits is obtained for 228 clock cycles [28]. The same steps are repeated for the next frame.

III. Proposed Cipher

To overcome some of the problems mentioned above in previous section, the following schemes / modifications are proposed to increase the randomness:

1) MOD-I: Here in this scheme as shown in Fig. 6, the nonlinearity is introduced in the feedback path of the shift registers by adding universal gates. Thus, the LFSRs have been converted into NLFSRs. By this, the randomness of the generated bit stream will be improved.

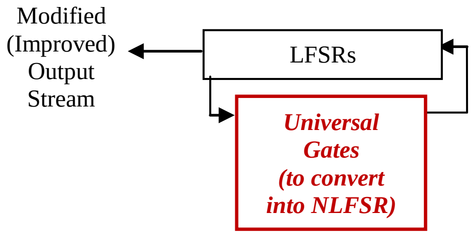

Fig. 6. Proposed MOD-I Scheme.

Polynomial equations of this MOD-I scheme will have the impact of NAND and NOR logic gates in it.

2) MOD-II: Here in this scheme, the 32 bit SRES is reused in the feedback path of the shift registers, which is already generated during the authentication process by A3 algorithm, as shown in Fig. 7. The SRES is XOR’ed in the feedback unit of LFSR through a NAND gate on bit by bit basis. This scheme reuses the output of another algorithm, hence increases the randomness of the cipher key.

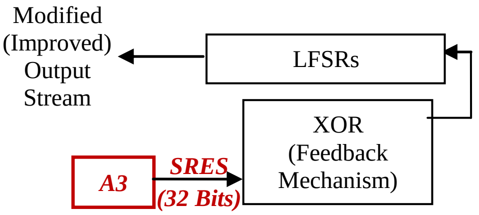

Fig. 7. Proposed MOD-II Scheme.

3) MOD-III: The user location is mixed with the bit stream generated using XOR (only last 32 bits). This works as a key feature as generally users have different locations and intruders cannot crack it easily. This is very important proposal, because the location of each individual user is not known to intruders and many times dynamic in nature. The CGI changes with the movement of the user and this makes the bit stream more complex. The idea is shown in Fig. 8.

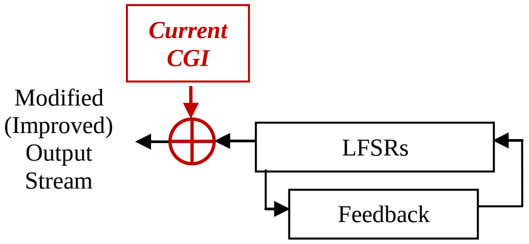

Fig. 8. Proposed MOD-III Scheme.

4) MOD-C: In this, all the above three modifications are combined to get the simultaneous impact of all above modifications.

The idea of combining all three modifications is shown in Fig. 9.

The proposed A5/1 cipher is realized and simulated in Logisim as shown in Fig. 10.

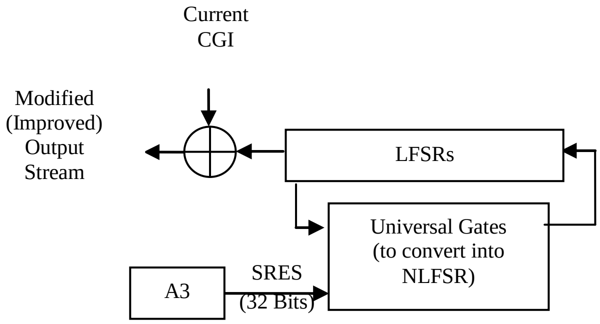

Fig. 9. Proposed Scheme of MOD-C.

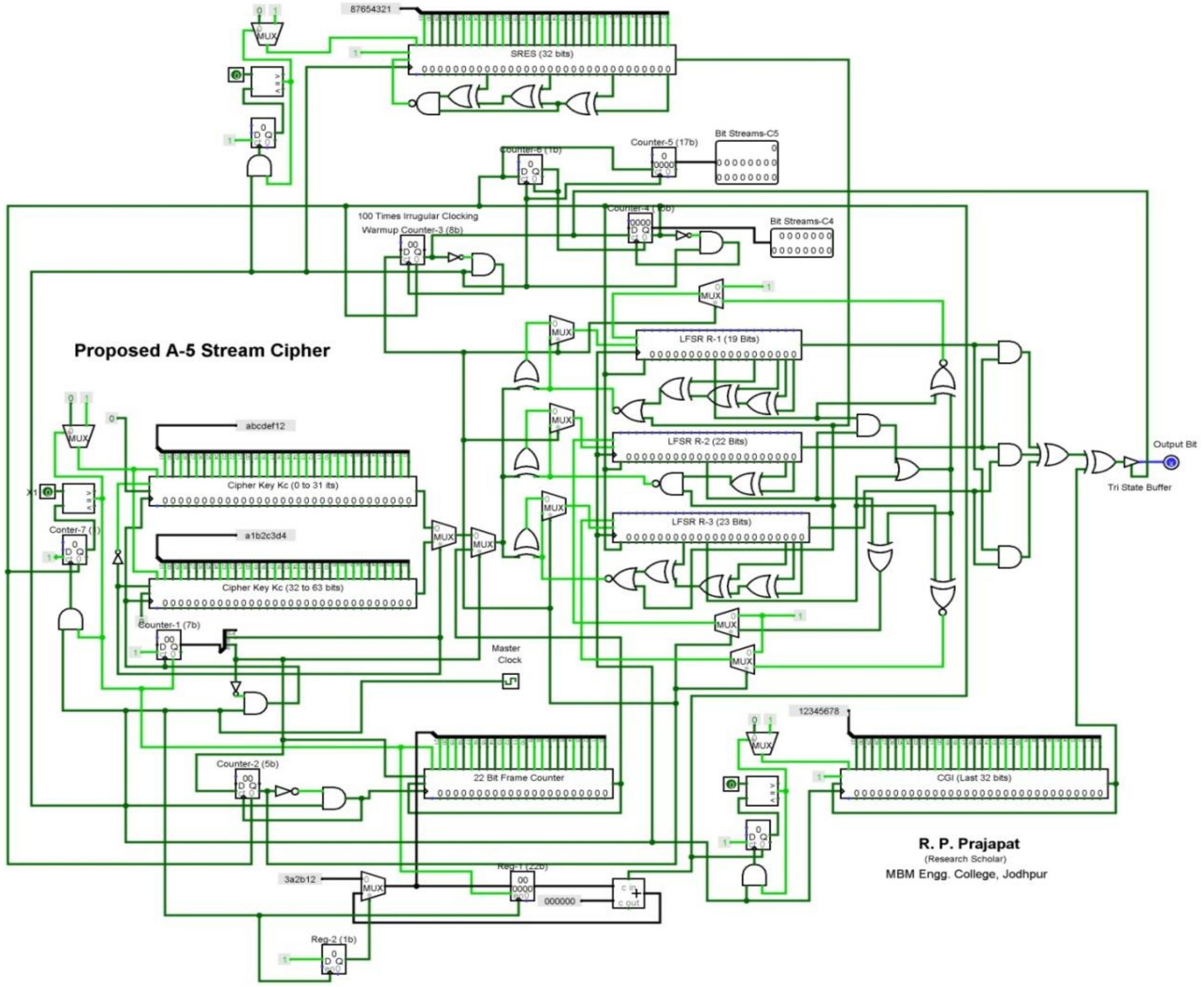

Fig. 10. Proposed Scheme of MOD-C in Logisim.

IV. Observations and Randomness Analysis

In a broader sense, the randomness of a data set is the lack of predictability, i.e. more uncertainty or more entropy. If a data set has more randomness means it has more encryption capability, hence more security. Such tests are carried out to check recognizable or repetitive patterns in any data set under test. Randomness is related to the theory of information entropy, probability, and chance. Entropy is a measuring tool for randomness.

NIST Suite is a statistical test suite based on Linux operating system and is used for statistical parameters testing of the output bit stream of both the actual and proposed scheme of A5/1 cipher. This test suite is also used in various cryptographic applications [7]. Performance comparison has also been done between these two with respect to various parameters. Following are the main tests which were carried out for the randomness test:

1) The frequency test (monobit & within a block): It tests the balance of 0's and 1's in the bit stream. The equilibrium between 0's and 1's should be maintained for a perfectly random data set. Therefore, the probability of availability of 0's and 1's should be close to 0.5 [7].

2) The cumulative sums test (cusums): It tests the randomness of a sequence of 0's and 1's which are called "random walks" or "partial sequences". It tells that the sum of the partial sequences is too large or too small [7].

3) The runs test: It analyzes the occurrence of similar patterns that are separated by different patterns [7].

4) The DFT (spectral) test: It finds out the patterns which are periodic in nature in a random bit sequence. The repetitive or periodic patterns close to each other are detected in this test [7].

5) The serial test: It detects the pair or patterns like 00, 01, 10, 11, 100 & 101 etc and checks the balances with its complimentary pair/pattern [7].

6) The linear complexity test: It is directly related to the bit length of the LFSRs used to generate the random bit stream [7].

The P-value parameter is defined for all these tests in NIST suite. It shows the probability of a bit stream of being random in nature. For an ideal random bit set, this P-value is 1 and if it is 0, then the bit stream is completely nonrandom. Thus, a higher value or close to 1 is desirable.

Different sizes of data (up to 10,000 blocks of 114 bit i.e. 10,000 x 114 =10, 00,000 consecutive bits) are used during the statistical tests both for the actual and proposed cipher [28]. The observations of different tests conducted upon the generated bit stream are as follows:

As the LFSRs of the actual cipher have been converted into NLFSRs in MOD-I scheme, we see a slight increase in the P-values of various tests. The 32 bit SRES is reused in feedback path of the shift registers in MOD-II and again slight increment in the P-values of various tests. As the last 32 bits of current location (CGI) of the user incorporated in output bit stream the slight increment in the P-values of various tests can be observed I MOD-III. Because all proposed modifications are implemented here simultaneously in MOD-C, a huge increase in the P-values of various tests can be observed.

The details of observations of different sizes of the data set are also provided in Table V for this MOD-C scheme.

TABLE IV. OBSERVATIONS OF THE PROPOSED SCHEMES

Test Parameter	**Actual A5/1** ***(P-Value)***	**Proposed MOD-I Scheme** ***(P-Value)***	**Proposed MOD-II Scheme** ***(P-Value)***	**Proposed MOD-III Scheme** ***(P-Value)***	**Proposed MOD-C Scheme** ***(P-Value)***
Frequency	0.46	0.55	0.58	0.57	0.77
Block Frequency	0.82	0.87	0.87	0.86	0.92
Cumulative Sum	0.44	0.61	0.62	0.64	0.80
Runs	0.90	0.91	0.92	0.91	0.94
Spectral DFT	0.95	0.96	0.95	0.96	0.98
Serial	0.96	0.97	0.96	0.97	0.98
Linear Complexity	0.79	0.82	0.81	0.82	0.88

TABLE V. STATISTICAL TEST RESULTS BY NIST TEST SUITE (A : ACTUAL A5/1 & P : PROPOSED A5/1)

MOD-C Scheme															
Bit Stream	Bits	**Frequency**		**Block Frequency**		**Cumulative Sum**		**Runs**		**DFT**		**Serial**		**Linear Complexity**	
		A	**P**	**A**	**P**	**A**	**P**	**A**	**P**	**A**	**P**	**A**	**P**	**A**	**P**
100	114	0.43	0.76	0.80	0.89	0.42	0.77	0.83	0.89	0.92	0.96	0.91	0.95	0.73	0.84
500	114	0.47	0.79	0.79	0.86	0.41	0.76	0.82	0.88	0.93	0.96	0.92	0.96	0.74	0.85
1000	114	0.49	0.81	0.82	0.91	0.43	0.78	0.83	0.89	0.92	0.97	0.95	0.98	0.75	0.86
5000	114	0.48	0.80	0.80	0.90	0.43	0.79	0.85	0.91	0.93	0.98	0.93	0.96	0.76	0.87
8000	114	0.43	0.78	0.81	0.90	0.41	0.77	0.89	0.93	0.94	0.98	0.96	0.98	0.76	0.88
10000	114	0.46	0.77	0.82	0.92	0.44	0.80	0.90	0.94	0.95	0.98	0.96	0.98	0.79	0.88
Average		0.46	0.79	0.81	0.90	0.42	0.78	0.85	0.91	0.93	0.97	0.94	0.97	0.76	0.86

V. Conclusion

The improvements in P-values of various tests of all four modifications (MOD-I, MOD-II, MOD-III & MOD-C) have been described in different tables of previous section. Based on these test results, it is stated that there is slight improvement in the randomness of generated bit stream of all three MODs but when all MODs are combined simultaneously in MOD-C a huge improvement can be observed in the P-values of Cumulative Sum test, Frequency test and most importantly in Linear Complexity test. There is a good balance between 0’s and 1’s (results of Frequency test), better random walks (results of Cumulative test), less occurrence of similar patterns and that too are well separated by different patterns (results of Run tests), low periodic patterns (results of DFT test) and enhanced entropy (results of Linear Complexity test) in random bit stream generated by proposed cipher.

An effort is made in this paper to improve the randomness by making three modifications MOD-I, II, & III and then comparing the NIST test results. These modifications are the incorporation of nonlinearity I feedback path of LFSRs, reusing the SRES of A3, and inclusion of current CGI of the user, respectively to improve the entropy. After that, all three modifications are implemented simultaneously in a combined manner to achieve better results. These are the major improvements and contributions in the proposed cipher scheme.

The weakness issues mentioned in early part of this paper are addressed significantly by these proposed schemes. Simulation & testing results confirmed it.

The test results of MOD-C scheme for different data sizes as shown in Table V and depicted in graphical form in Fig. 11 above. The P-values of all the tests of proposed A5/1 have been increased by a significant value in comparison with the original A5/1 cipher. For better randomness, higher P-values are desired and better randomness means stronger encryption and enhanced security. Therefore, as per the observations and test results, it is concluded that the proposed scheme of cipher is having better security against the cryptographic attacks with respect to the actual A5/1 cipher due to increased randomness (at the cost of slight increment in hardware).

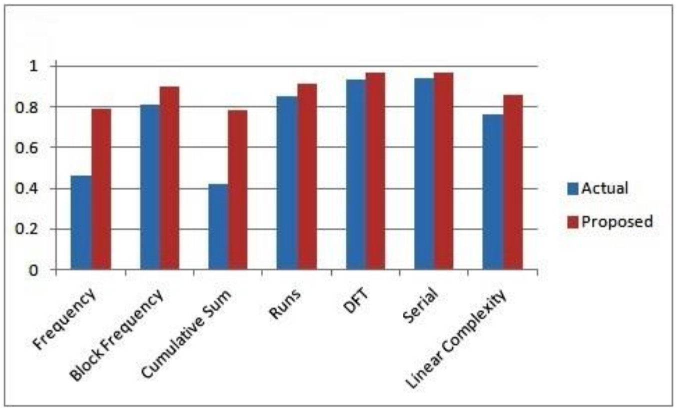

Fig. 11. Comparative Analysis of Test results of MOD-C Scheme.

References

[1] GSM Recommendations 02.09, Security Aspects by European Telecommunications Standards Institute (ETSI), June 1993.

[2] Jovan Dj. Golić, “On the security of shift register based key stream generators,” Fast Software Encryption-Cambridge’ 93, Lecture Notes in Computer Science, vol. 809, R. J. Anderson ed., Springer-Verlag, pp. 90–100, 1994.

[3] Jovan Dj. Golić, “Cryptanalysis of alleged A5 stream cipher,” Advances in Cryptology, proceedings of EUROCRYPT’97, LNCS, vol. 1233, pp.239–255, Springer-Verlag, 1997.

[4] M. Briceno, I. Goldberg, D. Wagner, A pedagogical implementation of the GSM A5/1 and A5/2 voice privacy encryption algorithms, (1999), http://cryptome.org/gsm-a512.htm, originally on www.scard.org.

[5] E. Biham, and O. Dunkelman, Cryptanalysis of the A5/1 GSM stream cipher, Progress in Cryptology, proceedings of INDOCRYPT’00, LNCS, pp. 43–51, Springer-Verlag, 2000.

[6] A. Biryukov, A. Shamir, and D. Wagner, Real time cryptanalysis of A5/1 on a PC, Advances in Cryptology, proceedings of Fast Software Encryption’00, LNCS, pp.1–18, Springer-Verlag, 2001.

[7] C. Burch, “Logisim : A Graphical System for Logic Circuit Design and Simulation,” J. Educational Resources in Comput., vol. 2(1), pp. 5-16, 2002.

[8] Andrew Rukhin et al, NIST, A Statistical Test Suit for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22, with revisions dated May 15, 2001.

[9] N. Komninos, B. Honary & M. Darnel1, “Security enhancements for A5/1 without loosing hardware efficiency in future”, 3G Mobile Communication Technologies Conference, 2002, Page No. 324-328.

[10] P. Ekdahl, and T. Johansson, Another attack on A5/1, IEEE Transactions on Information Theory, vol. 49, pp. 284-289, 2003.

[11] A. Maximov, T. Johansson, and S. Babbage, An improved correlation attack on A5/1, proceedings of SAC 2004, LNCS, vol.3357, pp.1–18, Springer-Verlag, 2005.

[12] Basar Kasim & Levent Ertaul, “GSM Security”, International Conference on Wireless Networks (ICWN), 2005, pp. 555-561.

[13] I. Erguler and E. Anarim, A modified stream generator for the GSM encryption algorithms A5/1 and A5/2, 13th European Signal Processing Conference (EUSIPCO’05), September, 2005.

[14] E. Barkan, and E. Biham, Conditional estimators: an effective attack on A5/1, proceedings of SAC 2005, LNCS, vol. 3897, pp. 1-19, Springer-Verlag, 2006.

[15] Elad Barkan, Eli Biham & Nathan Keller, “Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication”, Technion - Computer Science Department - Technical Report CS-2006-07 - 2006.

[16] Sukalyan Goswami, Subarna Laha, Satarupa Chakraborty & Ankana Dhar, “Enhancement of GSM Security Using Elliptic Curve Cryptography Algorithm” 3rd Int. Conference on Intelligent Systems Modelling and Simulation, IEEE, 2012 Page No. : 639-644.

[17] Mahdi Daghmechi Firoozjaei & Javad Vahidi, “Implementing Geo-encryption in GSM Cellular Network”, IEEE, 2012, Page No. 299-302.

[18] Prof. Darshana Upadhyay et al, Randomness analysis of A5/1 Stream Cipher for secure mobile communication, IJCSC Vol. 5, pp. 95-100, Sept. 2014.

[19] Pankaj et el., “Design of Enhanced Pseudo-Random Sequence Generator usable in GSM Communication”, IEEE WiSPNET 2016 conference.

[20] Nibras Hadi Jawad, "Simulation and Developed A5/3", International Conference on Current Research in Computer Science and Information Technology (ICCIT), Slemani - Iraq, 2017.

[21] Sattar B. Sadkhan et al., "A DNA-Sticker Algorithm for Cryptanalysis LFSRs and NLFSRs Based Stream Cipher" International Conference on Advanced Science and Engineering (ICOASE), Iraq, 2018.

[22] Martin Jurecek, Jirí Bucek, and Róbert Lórencz, "Side-Channel Attack on the A5/1 Stream Cipher" 2019 22nd IEEE Euromicro Conference on Digital System Design (DSD), 2019.

[23] Sattar B. Sadkhan et al., " Proposed enhancement of A5/1 stream cipher" 2nd International Conference on Engineering Technology and their Applications 2019-IICET2019-IRAQ, 2019.

[24] Sattar B. Sadkhan & Zainab Hamza, Proposed Enhancement of A5/1 stream cipher, 2019 2nd International Conference on Engineering Technology and its Applications (IICETA).

[25] Martin Jurecek, Jirí Bucek and Róbert Lórencz, Side-Channel Attack on the A5/1 Stream Cipher, 2019 22nd Euromicro Conference on Digital System Design (DSD), 2019.

[26] Sattar B. Sadkhan, "A proposed Development of Clock Control Stream Cipher based on Suitable Attack" 2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA, 2020.

[27] Nagendar Yerukala, V Kamakshi Prasad, and Allam Apparao, "Performance and Statistical Analysis of Stream Ciphers in GSM Communications" Journal of Communications Software and Systems, Vol. 16, No. 1, March 2020.

[28] Ram Prakash Prajapat, Rajesh Bhadada and Giriraj Sharma, Security Enhancement of A5/1 Stream Cipher in GSM Communication & its Randomness Analysis" 2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI), 6-9 Sept. 2021.

[29] Yi Qian, Feng Ye and Hsiao-Hwa Chen, Cryptographic Techniques, Security in Wireless Communication Networks (SWCN), 2022.