Randomness analysis of A5/1 Stream Cipher for secure mobile communication

Prof. Darshana Upadhyay[1], Dr. Priyanka Sharma[2], Prof.Sharada Valiveti[3]
Department of Computer Science and Engineering
Institute Of Technology,Nirma University
Ahmedabad,Gujarat,India
darshana.upadhyay@nirmauni.ac.in, priyanka.sharma@nirmauni.ac.in, sharada.valiveti@nirmauni.ac.in

Abstract- Information Security over mobile communication networks is vital for secure communication. The GSM voice calls are encrypted using a family of algorithms cooperatively called A5. Global System for Mobile communication (GSM) uses A5/1 stream cipher in order to provide privacy on air communication. A5/1 algorithm uses LFSR to generate key stream. Longer shift registers with the help of feedback, generate patterns so long that they look like pseudo random pattern.A5/1 stream cipher generates key which encrypt the information transmitted between subscribers mobile and the base station. It is strong encryption algorithm among all cryptographic algorithms used in GSM but recent research studies show that A5/1 cipher is cryptanalized by a number of attacks..It has feeble clocking mechanism and output bit sequence of A5/1 has low rate of linear complexity. To overcome these problems we convert LFSR based stream cipher into NLFSR based stream cipher using nonlinear combinational generator. It has been observed that the enhanced scheme has much better and more strengthen. NIST Statistical test package approximate the randomness performance of output bit streams of two ciphers. The randomness results confirm that the output bit-stream generated by the proposed stream cipher has improved the randomness performance.

Keywords- GSM,A5/1 stream cipher, cryptography attacks, linear feedback shift register-LFSR ,Non-linear feedback shift register-NLFSR

I. INTRODUCTION

Mobile communication present wireless connectivity that facilitate the people to communicate with each other at anywhere and at any time. However, the openness of mobile communication poses severe security threats to the sensitive information. This makes security very crucial in mobile services and this is achieved by the use of stream ciphering techniques. Stream ciphers are symmetric-key ciphers that generate pseudo-random binary patterns which are used to encrypt the message signals on bit-by-bit basis. The encryption and decryption in stream ciphers is based on XOR operation.A5/1 algorithm uses LFSR where feedback mechanism is achieve by XOR gates. The strength and security of these ciphers depends upon the characteristics of bit sequences produced by them [1]. Recent research studies and analysis show that it has some limitations due to which it is cryptanalized by a number of cryptographic attacks. A5/1 was initially crypt analyzed by Golic [2] when only a rough outline of A5/1 was leaked. After A5/1 was reverse engineered, it was analyzed by Biryukov, Shamir, and Wagner [3]; Biham and Dunkelman [4]; Ekdahl and Johansson [5]; Maximov, Johansson and Babbage [6]; and recently by Barkan and Biham [7]. Due to the security imperfection in the architecture of A5/1, it is susceptible to several attacks. Most of the attacks against A5/1 stream cipher use the security failing in clocking mechanism [8].A proper choice of combining function greatly improves the performance of the cipher from the cryptographic point of view. A combining function should be balanced and nonlinear; it should have high algebraic degree and correlation immunity [3, 6].

The proposed scheme is simulated using Logisim simulator and analyzed by NIST toolkit. The rest of the paper is organized as follows. In section II, A5/1 stream cipher is described. In section III, the enhanced scheme of A5/1 is discussed. In section IV, the result obtained by NIST's randomness test suit and other analysis is discussed. Finally conclude in section V.

II. A5/1 STREAM CIPHER

GSM uses A5/1 stream cipher to encrypt the information of the mobile user [10]. GSM mobile information is transmitted as series of frames with the frame rate of 217 (frames per seconds) roughly. The frame length is 228 bits, 114 bits for the communication in each direction. A5/1 is used as a key stream generator and produces 228 bits for each frame which are XORed with the frame bits. A5/1 is initialized using a 64-bit secret key together with a publicly-known 22-bit frame number. The A5/1 stream cipher is based on three linear feedback shift registers (LFSRs), R1, R2 and R3 of lengths 19, 22 and 23 bits respectively. The circuit of A5/1 algorithm is implemented it logisim simulator which is shown in Figure 2. Three feedback polynomials used for LFSR R1, R2 and R3 are: x^{19}Å x^{18} Åx^{17} Å x^{14} Å 1, x^{22}Å x^{21} Å1 and x^{23} Å x^{22} Å x^{21} Å x^{8} Å1 respectively. Each LFSR is clocked cycles that depend upon majority rule which represented in Table 1. Majority rule uses three clocking bits x1,x2 and x3 of LFSR R1, R2 and R3 respectively and determines the value of majority m using m = maj(x1,x2,x3). The majority rule is simply the majority among these bits, if two or more are 1 then the value of majority m is 1. Similarly, if two or more are 0 then majority m is 0. Now if bi = m then Ci will be 1 else Ci will be 0, and if Ci is 1 then register Ri will be clocked (shifted), where i=1, 2, 3.This means that if clocked bit of any LFSR is in majority then that LFSR will clocked. Thus the probability of an individual LFSR being clocked is 3/4.combinational circuit for clocking mechanism is represented in Figure 1. At each clocking, each LFSR generates one bit xi(t). All three bits are than XORed together to generate the final output bit z(t).

Algorithm of A5/1 algorithm:

1. Reset all 3 registers.
2. Initialization : Load 64 bits of key K + 22 bits of frame number FN into 3 registers
   K and FN XORed bit-by-bit to the least
   significant bits, registers clocked regularly.
3. Warm-up: Clock for 100 cycles and discard the output, registers clocked irregularly.
4. Execution: Clock for 228 cycles, generate 114+114 bits, registers clocked irregularly.
5. Repeat for the next frame.

Polynomial Equation used in A5/1:

LFSR: 1 $v1 = x^{19} \oplus x^{18} \oplus x^{17} \oplus x^{14} \oplus 1$
LFSR: 2 $v2 = x^{22} \oplus x^{21} \oplus 1$
LFSR: 3 $v3 = x^{23} \oplus x^{22} \oplus x^{21} \oplus x^{8} \oplus 1$

Table 1: Majority Rule Evaluation

Middle Bit			Majority	Clock		
R1	R2	R3		R1	R2	R3
0	0	0	0	1	1	1
0	0	1	0	1	1	0
0	1	0	0	1	0	1
0	1	1	1	0	1	1
1	0	0	0	0	1	1
1	0	1	1	1	0	1
1	1	0	1	1	1	0
1	1	1	1	1	1	1

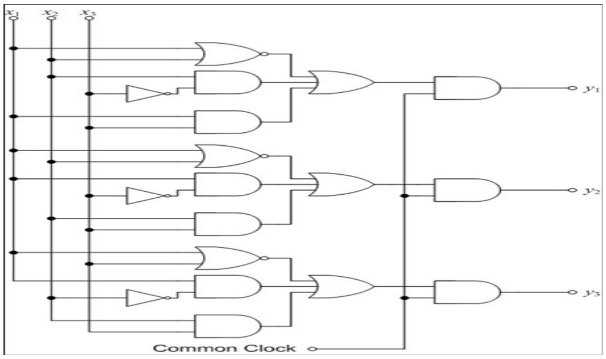


Figure 1: Combinational Circuit for clocking mechanism

Following equation represent Boolean expression for clocking mechanism:

$y_1 = m_0 + m_1 + m_2 + m_5 + m_6 + m_7$

$y_2 = m_0 + m_1 + m_3 + m_4 + m_6 + m_7$

y3 = m0 + m2 + m3 + m4 + m5 + m7

y1 = x1’ x2’ + x2x3’ + x1x3

y2 = x1’x2’ + x1x3’ + x2x3

y3 = x1’ x3’ + x1x2’ + x2x3

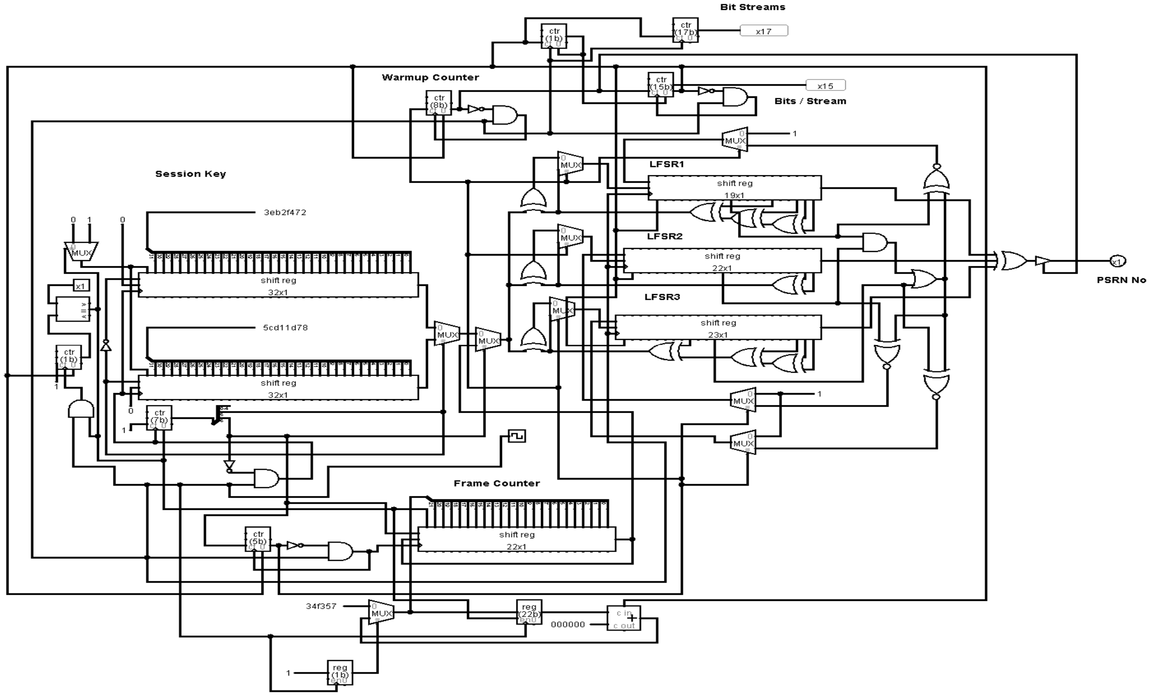


Figure 2: Hardware Simulation of A5/1 Algorithm

III. Proposed Stream Cipher

The architecture of the proposed stream cipher is shown in Figure 2 above.The major modification are made in the feedback tapping units of conventional A5/1.

A. Feedback and State selecting unit

In the modified A5/1, the feedback unit is modified in adding universal gates to convert LFSR into NLFSR.The modification that can be seen in figure 2 is that each feedback of LFSR is combined with universal gate to produce more randomness in bit pattern. As there are three states for each LFSR Feedback polynomial unit in the proposed A5/1 is v1= (v1 + ($x^{19} \oplus x^{18}$))',v2 = (v2 * x^{22})'and v3 = (v3 + ($x^{23} \oplus x^{22} \oplus x^{21}$))'. In our proposal feedback polynomial designed by universal gates are used for an LFSR have been selected that are shown in figure. The feedback polynomials are selected such that the output generated by polynomial primitive for each LFSR is combined with universal gate. This will help to realize the circuit easily.

Polynomial Equation used in Proposed A5/1:

LFSR: 1 v1= (v1 + ($x^{19} \oplus x^{18}$))'
LFSR: 2 v2 = (v2 * x^{22})'
LFSR: 3 v3 = (v3 + ($x^{23} \oplus x^{22} \oplus x^{21}$))'

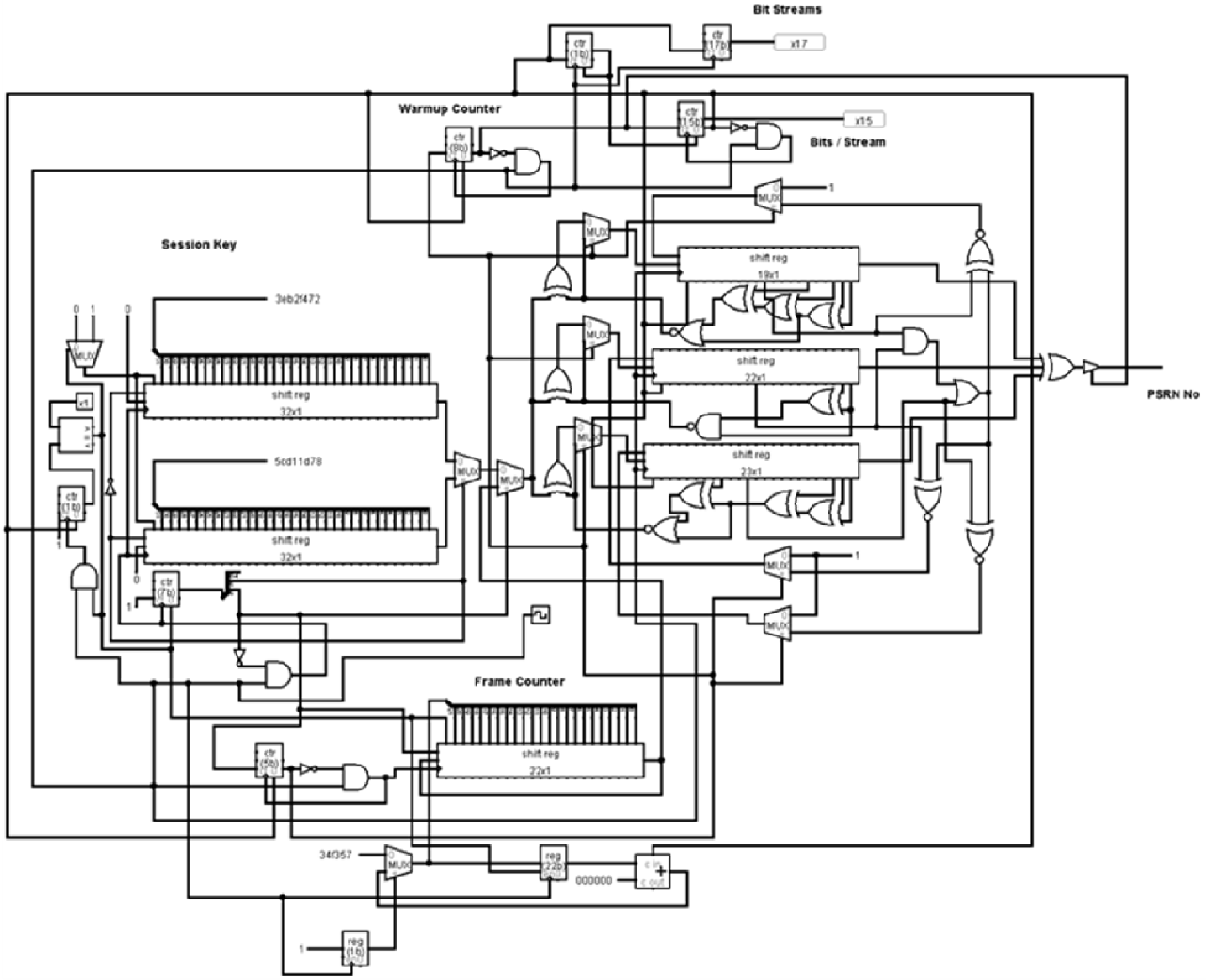


Figure 3: Hardware Simulation on proposed A5/1 Algorithm

IV. Randomness Evaluation

To estimate the randomness performance of the anticipated scheme, it is essential to statistically test the output sequence to decide the randomness attributes. To perform the randomness and statistical analysis of the proposed scheme, we used the statistical test package by the National Institute of Standards and Technology (NIST) [11]. This test package conducts a comprehensive battery of statistical tests, to check the randomness quality of the bit sequence generated. The performance of the scheme in these tests is no guarantee to secure communications, but only an indicator of what can be expected in practice. The statistical testing of binary sequence generators is an absolute necessity for cryptographic applications. The statistical tests are performed to calculate a p-value. Each p-value corresponds to the probability that the sequence under test is random. If p-value is 1 then it indicates that the sequence appears to have perfect randomness, so a high p-value is desirable. A test passes if evaluated p-value is larger than 0.01 indicates that one would expect 1 sequence in 100 sequences to be rejected. If p-value 0.01 indicates that the sequence is considered to be random with a confidence of 99%. A p-value < 0.01 indicates that the sequence is non-random with a confidence of 99%.bellow stastical tests are performed.

Frequency (Monobit) Test and (Test for Frequency within a Block: M Blocks)

Description: The focus of the test is the proportion of zeroes and ones for the entire sequence[11].

Purpose: To determine whether that number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence.

Runs Test and (Test for the Longest Run of Ones in a Block: M Blocks)

Description: The focus of this test is the total number of zero and one runs in the entire sequence, where a run is an uninterrupted sequence of identical bits. A run of length k means that a run consists of exactly k identical bits and is bounded before and after with a bit of the opposite value[11].

Purpose: To determine whether the number of runs of ones and zeros of various lengths is as expected for a random sequence. In particular, this test determines whether the oscillation between such substrings is too fast or too slow.

Discrete Fourier Transform (Spectral) Test

Description: The focus of this test is the peak heights in the discrete Fast Fourier Transform. The purpose of this test is to detect periodic features (i.e., repetitive patterns that are near each other) in the tested sequence that would indicate a deviation from the assumption of randomness[11].

Maurer's Universal Statistical Test

Description: The focus of this test is the number of bits between matching patterns. The purpose of the test is to detect whether or not the sequence can be significantly compressed without loss of information. An overly compressible sequence is considered to be non-random.

Linear Complexity Test

Description: The focus of this test is the length of a generating feedback register. The purpose of this test is to determine whether or not the sequence is complex enough to be considered random. Random sequences are characterized by a longer feedback register. A short feedback register implies non-randomness [11].

Serial Test

Description: The focus of this test is the frequency of each and every overlapping m-bit pattern across the entire sequence. The purpose of this test is to determine whether the number of occurrences of the 2m m-bit overlapping patterns is approximately the same as would be expected for a random sequence. The pattern can overlap.

Approximate Entropy Test

Description: The focus of this test is the frequency of each and every overlapping m-bit pattern. The purpose of the test is to compare the frequency of overlapping blocks of two consecutive/adjacent lengths (m and m+1) against the expected result for a random sequence.

Statistical tests are applied on sequence containing 114*10,000 =1, 00,00,000 consecutive bits of output key stream of two schemes. It is clear from Table 1 & Table 2 that proposed a5/1 cipher generates more random pattern then original a5/1 algorithm. The results of the statistical testing are shown in below graph. Moreover, the p-values corresponding to randomness tests in the case of proposed scheme are considerably higher than the p-values in the case of A5/1 scheme. This shows that the proposed scheme generates more random bit sequence than the sequence generated by the original A5/1 scheme. It can be said that the proposed scheme has better statistical and randomness performance than the original A5/1 cipher. Hence, bit sequence produced by the proposed scheme can be employed as random keys to encrypt the message signals in order to have more secure communication.

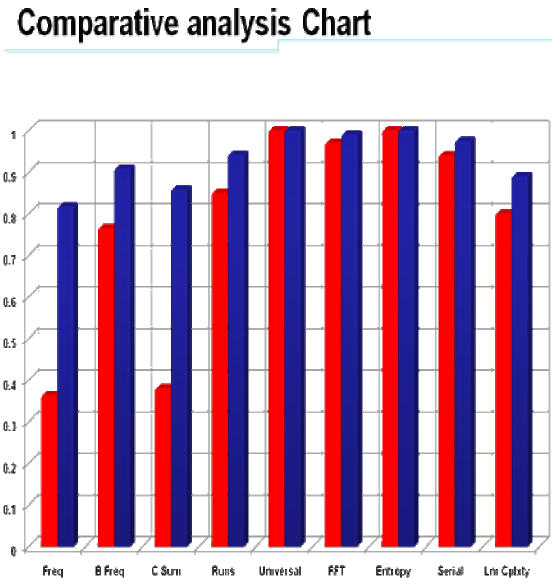
Table 2: Statistical test analysis for A51 using LFSR

Bit Streams	No. of Bits	Freq	B Freq	C Sum	Runs	FFT	Serial	Linear Complexity
100	114	0.34	0.78	0.33	0.87	0.98	0.94	0.81
500	114	0.33	0.75	0.36	0.85	0.98	0.94	0.78
1000	114	0.36	0.76	0.39	0.86	0.97	0.94	0.79
5000	114	0.38	0.75	0.40	0.85	0.97	0.94	0.78
8000	114	0.39	0.80	0.41	0.85	0.97	0.93	0.78
10000	114	0.38	0.75	0.40	0.85	0.97	0.94	0.88
Average		0.36	0.765	0.38	0.85	0.97	0.94	0.80

Table 3: Statistical test analysis for A51 using NLFSR

Bit Streams	No. of Bits	Freq	B Freq	C Sum	Runs	FFT	Serial	Linear Complexity
100	114	0.79	0.90	0.81	0.91	0.99	0.97	0.92
500	114	0.83	0.92	0.89	0.95	0.99	0.97	0.82
1000	114	0.82	0.92	0.87	0.95	0.99	0.97	0.92
5000	114	0.82	0.90	0.86	0.94	0.99	0.98	0.90

8000	114	0.82	0.91	0.86	0.95	0.99	0.98	0.87
10000	114	0.82	0.90	0.86	0.95	0.99	0.97	0.91
Average		0.81666	0.90833	0.85833	0.9417	0.99	0.975	0.89



V. CONCLUSIONS

In this paper, the modifications in A5/1 stream cipher are proposed. Modifications are done to improve the randomization property of A5/1 algorithm to make it robust to attacks. It is observed that the changing of feedback taps is an effective to make the generator stronger. Now, cryptanalyst has to identify NLFSR based feedback polynomials instead of polynomial primitive which is associate with LFSR. It is also observed that the modified A5/1 have larger p-value for frequency test & cumulative sum test which identify that proposed algorithm determine that number of ones and zeros in a sequence are approximately the same as would be expected for a truly random sequence. Based on the observations and results, it can be concluded that the proposed scheme is robust to the cryptographic attacks compare to the conventional A5/1 stream cipher. Hence the proposed scheme generates cryptographically better binary pattern than the A5/1 stream cipher of GSM with minor increase in the hardware.

VI. REFERENCES

[1] R. Mita, G. Palumbo and M. Poli, Pseudo-random sequence generators with improved inviolability performance, IEE Proceedings of Circuits, Devices and Systems, vol. 153, pp 375-382, 2006.

[2] J. Golic, Cryptanalysis of alleged A5 stream cipher, Advances in Cryptology, proceedings of EUROCRYPT'97, LNCS, vol. 1233, pp.239–255, Springer-Verlag, 1997.

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8]S.E.AlAschkar and M.T.El-Hadidi, Known attacks for the A5/1 algorithm: A Tutorial, International Conference on Information and Communications Technology (ICICT03), pp. 229-251, 2003.

[9]Patrik Ekdahl,On LFSR based Stream Ciphers:Analysis and Design, Lund University, Ph.D. Thesis,November 21, 2003.

[10]Recommendation GSM 02.09,European Telecommunications Standards Institute(ETSI), Security aspects.

[11] Andrew Rukhin et all, 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.