Enhancement of A5/1 Stream Cipher with Non-Linear Function using MOSFET

Farhan Rahman, Siddharth Singh

***Abstract:** Living in this modern era – the epitome of communication GSM networks is one of the mainly used architectures. But GSM architecture has its own shortcomings; the GSM network is vulnerable to various security threats. For any network to provide security to the user, the algorithms should be planned and designed in such a way that it provides cellular secrecy, data and signaling confidentiality to the concerned user. Keeping in mind the above features, the A5/1 algorithm provides network security. Initially, the A5/1 algorithm dealt with a pre-defined secret key but they still possess the threat of being decrypted by cryptanalytic attacks. Although decrypting this algorithm is not easy and requires high computational power. Such attacks lead to the necessity to modify the A5/1 algorithm; in our paper, we have proposed a better method to enhance the already existing algorithm.*

***Keywords:** A5/1 algorithm, GSM Networks, non-linear, session key, stream cipher.*

I. INTRODUCTION

The Global System for Mobile Communication (GSM) is extensively used but there is various advanced communication architecture. GSM architecture deals with various network sublevels consisting of the Network and Switching Subsystem (NSS), Base-Station Subsystem (BSS), Mobile Station (MS) and the Operation and Support Subsystem (OSS). The figure below shows the proposed networking system.

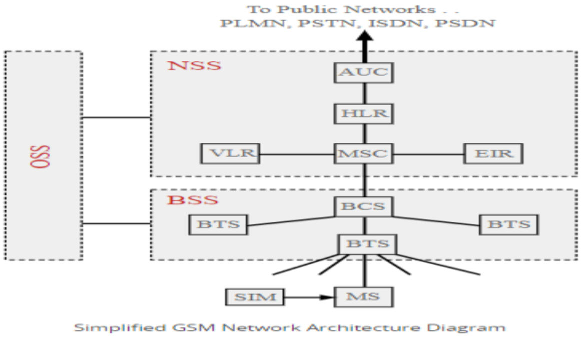


Fig. 1. GSM Architecture Diagram

Manuscript published on 30 December 2019.
* Correspondence Author (s)

Farhan Rahman*, Electronics and Communication Engineering, Vellore Institute of Technology, Chennai, India . Email: farhanrahman02@gmail.com
Siddharth Singh, Electronics and Communication Engineering, Vellore Institute of Technology, Chennai, India . Email: sidssr2012@gmail.com

The existing A5/1 algorithm ensures mobile security by generating a 64-bit secret key which is randomly generated and with the repeated XOR-ing operation of the tapped bits of the Linear Feedback Shift Register (LFSR). The existing A5/1 uses a linear operation like XOR-ing the bit values but our proposed idea uses a non-linear function implemented by MOSFET. The existing A5/1 algorithm has less complexity because of the use of XOR-ing operation with the randomly generated session key.

II. RELATED WORK

The already existing research and work show that there are various vulnerabilities to the A5/1 Algorithm, such as authentication of a call, maintaining the call, integrity and monitoring the authorization and accessibility. Threats like eavesdropping, impersonation of the user, impersonation of the network, Man-in-the-Middle (MITM), Network authentication compromise possess leakage of user data. The A5/1 algorithm is weak because of the use of linear function; our proposed work increases the complexity by using non-linear function and by increasing the data size of the session key to 128, increasing the size of the LSFR and by altering the tapped bits. In general, the A5/1 algorithm uses a randomly generated 64-bit session with a frame counter. Initially, the register value is set to zero; the ith key gets added to the LSB (least significant bit) and using XOR, for every cycle. Every register is clocked afterward; the same method is used for the 22-bit frame counter.

III. EXISTING A5/1 ALGORITHM

Following are the steps of the original A5/1 algorithm from the generation of 228-bits of the key sequence [1]:

Step 1. All three registers are set to 0. V1 = V2 = V3 = 0 and set the corresponding clocking and tapped bit values set.

Step 2. The registers with a size of 64 bits are passed into all registers at the same time. This key is generated during the authentication of a mobile device to the network. Then, the key is consecutively XOR-ed in parallel to the feedback of the registers, for the following next 64 cycles using the algorithm: For i = 0 to 63 do V1[0] = V1[0] ⊕ Jc[i] ,V2[0] = V2[0] ⊕ Jc[i] ,V3[0] = V3[0] ⊕ Jc[i] all the registers are clocked ignoring the stop/go clocking unit. The end for the loop.

Step 3. In this step, the clocking of the register takes place 22 times ignoring the irregular clocking. Key bits of a 22bit frame counter of the GSM frame is inserted and XORed with the feedback of each register.

Frame counter indicates the number of the actual frame that is being ciphered. The length of a frame is 228bits long. The algorithm for this step is as follows that is: For i = 0 to 21 do V1 [0] = R1 [0] ⊕ CFRAM[i], V2 [0] = V2 [0] ⊕ CFRAM[i], V3 [0] = V3 [0] ⊕ CFRAM[i], again we will clock all three registers ignoring the stop/go clocking unit, End for loop.

Step 4. Registers are clocked 100 times with irregular clocking. For i= 0 to 99 do z = V1[clb8] ⊕ V2[clb10] ⊕ V3[clb10];If V1[cb8] = z then Clk1=1 ; Else Clk1 =0 ; If V2[clb10] = z then Clk2=1;Else Clk2 =0;If V3[clb10] = z then Clk3=1; Else Clk3 =0 .Irregular clocking follows majority rule .majority bit is determined based on clocking bits of the (LFSR1 clocking bit :8,LSFR2 clocking bit:10,LSFR3 clocking bit:10).If the clocking bit of the register is same as the majority bit , the register is clocked. The result value of the registers after this step is considered as the initial state of A5/1.

Step5. After the initialization of registers is complete, we clock the registers 228 times (clocks) with irregular clocking and the output of each register is XORed to produce 228bits long keystream. The generated 228 keystreams are XORed with 228 bits of a plain text to create ciphertext .this creates one 228 bits long frame of communication. To Cipher another frame of data the registers are initialized again using the same session key and the frame counter increased by one. Session key changes when the network carrier decides to re-authenticate the mobile device.

IV. PROPOSED A5/1 ALGORITHM

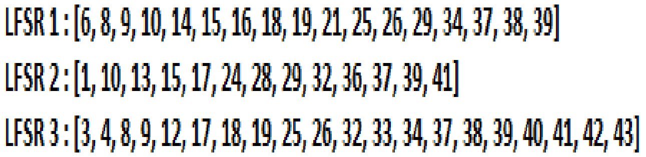
Use of MOSFET logic for non-linear function generation:

MOSFET is the most frequently used transistor that can be found in both analog and digital circuits. The use of MOSFET increases the randomness of the generated key. The selection of complementary MOSFET can help to implement digital non-linear logic, with proper parameter selection of width ratio of the CMOS.

The method we opted for ensures more security and complexity to the computation by maintaining the same time complexity and increasing the randomness of the ciphertext and the session key. In our case, we generated a 128-bit session key which minimizes the chances of MITM attack, as decrypting the 128-bit key is much more complex than 64 bit. By increasing the LFSR value to 40bits, 43bits and 45 bits it increases the computational time and with the help of non-linear function generated using MOSFET, it enhances the previous A5/1 algorithm.

The use of an increased size of LFSR leads to the highest period of the first register as:

2^{40}-1= 1.0995x10^{12}, for the second we have 2^{43}-1=8.796x10^{12} and third as 2^{45}-1=3.518x10^{13} with this it is very hard to follow the calculations and approximation for the new A5/1 algorithm. This makes attacks highly unlikely and difficult to crack.

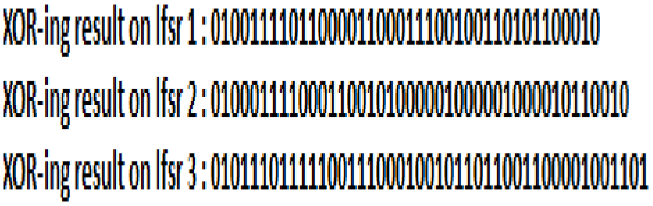


LFSR 1 : [6, 8, 9, 10, 14, 15, 16, 18, 19, 21, 25, 26, 29, 34, 37, 38, 39]

LFSR 2 : [1, 10, 13, 15, 17, 24, 28, 29, 32, 36, 37, 39, 41]

LFSR 3 : [3, 4, 8, 9, 12, 17, 18, 19, 25, 26, 32, 33, 34, 37, 38, 39, 40, 41, 42, 43]

Fig. 2. Shows the tapped bits of the three LFSR



XOR-ing result on lfsr 1 : 0100111101100001100011100100110101100010

XOR-ing result on lfsr 2 : 0100011110001100101000001000001000010110010

XOR-ing result on lfsr 3 : 010111011111001110001001011011001100001001101

Fig. 3. XOR operation between the LFSR and session key

V. NON – LINEAR FUNCTION

Studies have shown that the linear XOR operations have less complexity and comparatively easily attacked but with nonlinear function, like in our case **f(x) = ((x1⊕ x2).(x2 ⊕x3). x1) ⊕ x3**

The use of the nonlinear function increases the difficulty level for the attackers and thereby increasing the computational time. Initially, the linear operation was simple with the use of less critical hardware and the logical function **f(x) = x1 ⊕ x2 ⊕ x3.**

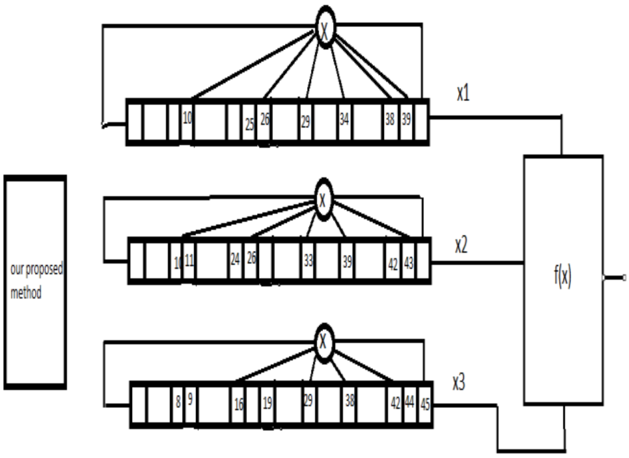


Fig. 4. Stream Key Generator

With the increase of tapped bits and session key bits, the improved algorithm has solved the purpose of security and increases the randomness in the sequence. The original A5/1 algorithm uses simple XOR operation of the output of the LFSR but we use our own logic which has significance in terms of analog circuits as well.

The clocked bits are similar to the original A5/1 algorithm, that is, tapping the 8th, 10th and 10th bit of the first, second and third LFSR respectively. But our method has increased data bit size and also the values of the bits getting XOR-ed increasing the complexity.

Our proposed work prevents attacks by increasing the randomness of the session key and cipher text so thereby increasing the complexity for the attackers trying to decipher the text. For proving the complexity of our method we have used certain calculations and tests.

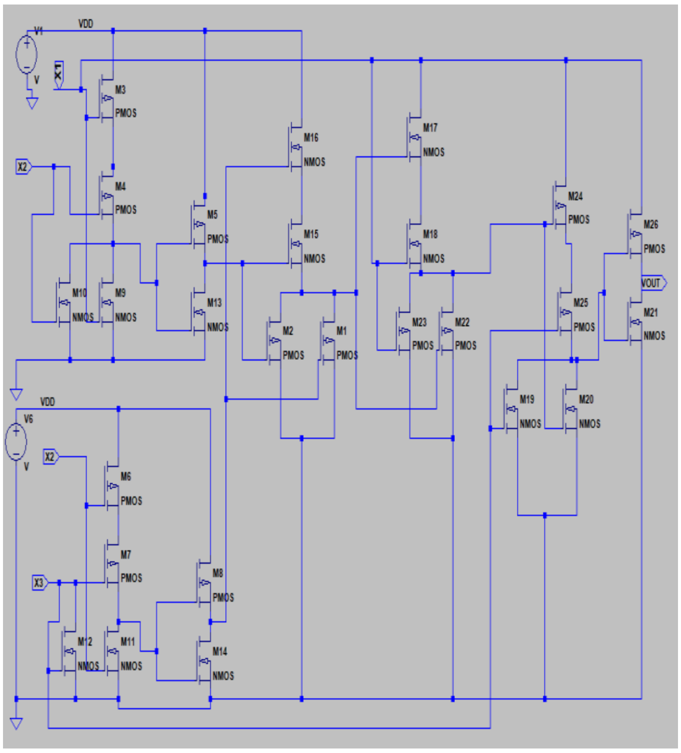


Fig. 5. MOSFET Circuit Diagram

VI. TESTS

So for predicting the randomness we have used frequency test, runs test and entropy test. The method for the tests is listed below, suggested by the authors of [11].

a) Frequency test:

- The first step deals with the conversion of bit values of signal to +-1. The lower value of the input sequence (0's) and the higher values (1's) of the input sequence are converted to values of -1 and +1 and are aggregated together to generate a summation $\mathbf{S_n=X_1+X_2+........+X_n}$ **where** $\mathbf{X_i=2\varepsilon_i-1}$
- Analyze the observed value $\mathbf{S_{obs}=|S_n|/\sqrt{n}}$
- Evaluate the ***P-value*****=erfc(**$\mathbf{S_{obs}/\sqrt{2}}$**)**
- This test depends on P-value, if the P-value is <0.01, then it can be inferred that the sequence is non-random. Or else we infer that the input key is random.
- So more the value of $\mathbf{S_n}$ the more random is the text.

b) Runs test:

- For this test evaluate the pre-test proportion π of the higher data values(1's) in the key input sequence: $\boldsymbol{\pi=\sum_j\varepsilon_j/n}$
- Regulate if the pre-test Frequency test is successful: If $\boldsymbol{|\pi-0.5|\geq\tau}$ holds true, then the Runs test need not be carried out.
- Compute the test statistics by the formula

$$V_n(obs)=\sum_{k=1}^{n-1}r(k)+1\text{, where } r(k)=0 \text{ if } \varepsilon_k=\varepsilon_{k+1}$$

- Compute ***P-value*****=**

$$= erfc\left(\frac{|V_n(obs)-2n\pi(1-\pi)|}{2\sqrt{2n}\pi(1-\pi)}\right)$$

c) Entropy test:

- Sum up the n- bit key sequence to generate n coincidental m-bit sequences by adding m-1 bits from the start to the end of the input key.
- A track of the number of 0's and 1's is made of the n coincidental blocks. Let the number of the accepted m-bit ((m+1)-bit) values be represented as $\mathbf{C^m_j}$ where I is the m-bit value.
- Evaluate $\mathbf{C^m_j=\#i/n}$ for each corresponding i
- Analyze

$$\varphi^{(m)}=\sum_{i=0}^{2^m-1}\pi_i\log\pi_i\text{, where }\pi_i=C_j^3\text{, and } j=\log_2 i$$

- Rerun the process from steps 1-4, replacing m by m+1.
- Compute the test statistic

$$\chi^2=2n[\log 2-ApEn(m)]\text{, where } ApEn(m)=\varphi^{(m)}-\varphi^{(m+1)}$$

- Compute

$$P-value=igamc(2^{m-1},\frac{\chi^2}{2})$$

VII. RESULT AND ANALYSIS

The below table is an outcome of various tests for randomness listed by authors in [11], proposing tests to measure the extent of randomness using the following tests:

- **Frequency test (mono bit test)** for this randomness check; we consider the count of zeros and ones in the generated random key streams**.**
- **Runs Test** in this test, we evaluate whether the count of runs of different lengths in the key streams S is conventional to the random key streams.
- **Entropy test** is used to measure the randomness more the entropy value more is the randomness of the generated key.

Retrieval Number: A10211291S319/2019©BEIESP
DOI:10.35940/ijeat.A1021.1291S319
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

Table- I: Tabulation of Different Tests Used

Test Used (Randomness)	Original A5/1 for Session Key	Modified A5/1 for Session Key	Original A5/1 for Chipper text	Modified A5/1 for Chipper text	Remark (conclusion)
Frequency Test	0.01242	0.72367	0.11269	0.85967	Success
Runs Test	0.75528	0.77206	0.07943	0.47713	Success
Entropy Test	0.12041	0.12079	0.01745	0.14316	Success

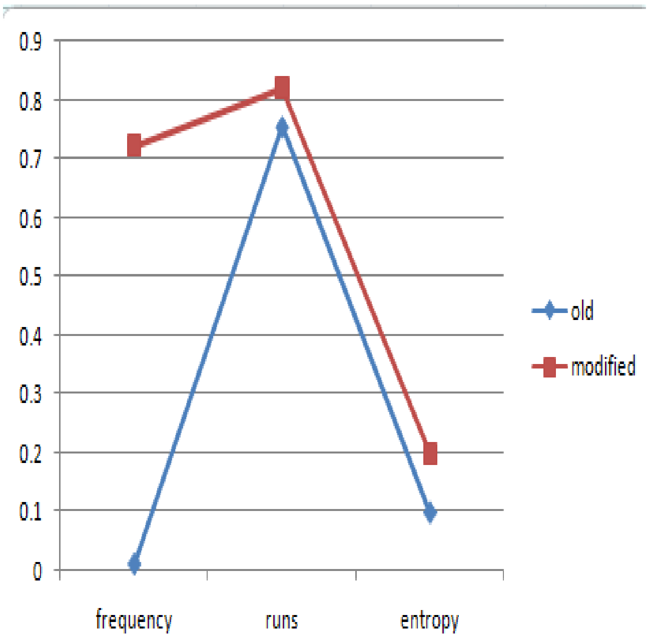


Fig. 6. Graph for Old vs. Modified Session Key

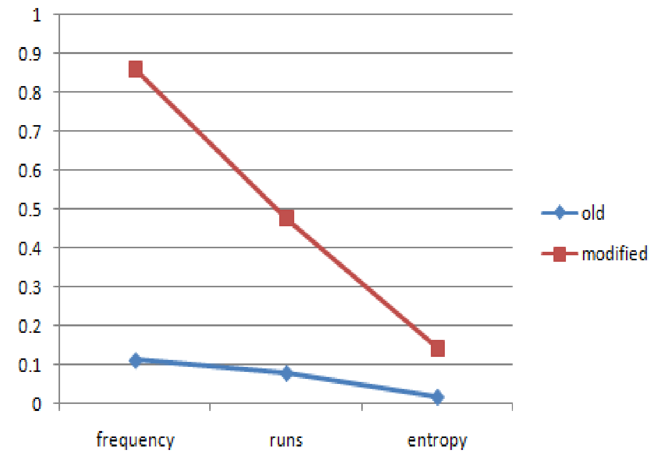


Fig. 7. Graph for Old vs. Modified Cipher Text

VIII. CONCLUSION

In this paper, the modifications to the existing A5/1 stream cipher are proposed. Modifications are done to improve the complexity of the A5/1 algorithm to make it robust to attacks, mainly focusing on MITM attacks. Our proposed work increases the complexity by using nonlinear function and by increasing the data size of the session key to 128 and by also increasing the size of the LSFR and by altering the tapped bits. According to the observations and results obtained from different tests, it can be concluded that the proposed scheme is robust enough from cryptographic attacks in comparison to the A5/1 stream cipher which already exists. As it is clear from figure [6 and 7], both the session key and the ciphertexts for our proposed A5/1 algorithm results in greater randomness and complexity to attacks. From the figures, we can conclude that for frequency test there is a huge difference between the old and the modified algorithm and there is also a considerable amount of change in the entropy of the two algorithms, where the modified algorithm shows a gradual increase from the original A5/1 algorithm. Hence it can be seen that the anticipated scheme generates a cryptographically improved binary sequence than the active A5/1 stream cipher of GSM with a minor increase in the hardware.

REFERENCES

1. JOURNAL OF NETWORKS, VOL. 1, NO. 6, NOVEMBER/DECEMBER (2006) Threats and Countermeasures in GSM Networks Valer BOCAN Department of Computer Science and Engineering, Politehnica University of Timişoara, Romania Alcatel Romania
2. https://asecuritysite.com/encryption/a5
3. IOP Conf. Series: Materials Science and Engineering 263 (2017) 042084 doi:10.1088/1757-899X/263/4/042084 Enhancement of A5/1 encryption algorithm Ria Elin Thomas, Chandhiny G, Katyayani Sharma, H Santhi and P Gayathri School of Computer Science and Engineering, VIT University, Vellore- 632014, India
4. Marappan D 2017 Securing Mobile Technology of GSM using A5 / 1 Algorithm, 111-113
5. https://www.electronics-notes.com/articles/connectivity/2g-gsm/network-architecture.php

6. A Modified Stream Generator For The Gsm Encryption Algorithms A5/1 And A5/2 Imran Erguler1,2, And Emin Anarim2
7. Enhancement of A5/1 Stream Cipher Overcoming its Weakneses, Mahdi Madani, Salim Chitroub Signal and Image Processing Laboratory Electronics and Computer Science Faculty, USTHB Algiers, Algeria
8. Randomness analysis of A5/1 Stream Cipher for secure mobile communication, Prof. Darshana Upadhyay1, Dr. Priyanka Sharma2, Prof.Sharada Valiveti3 Department of Computer Science and Engineering Institute Of Technology, Nirma University Ahmedabad, Gujarat, India
9. Randomness analysis of A5/1 Stream Cipher for secure mobile communication, Prof. Darshana Upadhyay1, Dr. Priyanka Sharma2, Prof.Sharada Valiveti3 Department of Computer Science and Engineering Institute Of Technology,Nirma University Ahmedabad, Gujarat, India
10. INFORMATICA, 2013, Vol. 24, No. 3, 339–356 339 □ 2013 Vilnius University, A New Randomness Test for Bit Sequences. Pedro María ALCOVER1∗, Antonio GUILLAMÓN2, María del Carmen RUIZ3.
11. TRINITY COLLEGE DUBLIN Management Science and Information Systems Studies Project Report. THE DISTRIBUTED SYSTEMS GROUP, Computer Science Department, TCD. Random Number Generators: An Evaluation and Comparison of Random number sequence.
12. Christof Paar and Jan Pelzl, Understanding Cryptography, A Textbook for Students and Practitioners, Foreword by Bart Preneel.
13. Mavoungou S, Kaddoum G, Taha M and Matar G (2016) Survey on threats and attacks on mobile networks IEEE Access 4 4543–4572.
14. Naveen C (2016) Image Encryption Technique Using Improved A5 / 1 Cipher on Image Bitplanes for Wireless Data Security.
15. Bird R, Canada B C and Layers A G S M (2015) Investigating Vulnerabilities in GSM Security.

AUTHORS PROFILE

Farhan Rahman, currently pursuing Electronics and Communication Engineering from VIT Chennai. Research interest field consists of Internet of things, Digital Signal Processing .

Siddharth Singh, currently pursuing Electronics and Communication Engineering from VIT Chennai. Research interest field consists of Internet of things and Networking .