Advanced Research in Electrical and Electronic Engineering
Print ISSN: 2349-5804; Online ISSN: 2349-5812 Volume 2, Number 8 April-June (2015) pp. 98-100
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/areee.html

GSM A5/1 Modification for Improved Randomized Stream Output

Praveen Kumar Yadav[1] **and G.P. Biswas**[2]

[1,2]Department of Computer Science and Engineering Indian School Of Mines, Dhanbad, India
E-mail: [1]praveenyadav@cse.ism.ac.in

Abstract—*A5/1 encryption algorithm is used to provide privacy for conversation in GSM. A binary stream cipher, consisting of the 3 short LFSR of total length 64 bits is/are mutually clocked in the stop and go manner which is known as A5. In this study, the modified version of the A5/1 algorithm is presented that offers security improvement by changing the clocking mechanism.*

Keywords*: GSM, Encryption, LFSR, A5/1 stream cipher, Authentication*

1. INTRODUCTION

Encryption in mobile communication is very important because lots of sensitive data that are not to be disclosed to the third parties are transmitted through the air. GSM uses A5 algorithm for encryption in the Global system for mobile communication. In GSM, A5 stream generator is used to encrypt digital user data transmitted from the mobile station to the base station and vice-versa. A5 has two major variants - A5/1 and A5/2. In the western European country, stronger version is used which is A5/1 and in other countries, weaker version is used which is A5/2.

In this paper, we have proposed a modified version of the A5/1 algorithm that makes the basic attack impractical. The improvement that increases the security of the algorithm is mainly based on the clocking mechanism of the proposed algorithm.

2. LITERATURE REVIEW

2.1 GSM Architecture

GSM, which is the second generation cellular system is a standard developed by the European Telecommunication standards Institutes (ETSI). GSM network can be subdivided into three major parts as shown in Fig. 1:

1. The Base Station Subsystem (BSS) is mainly divided into two parts–
   i) BTS (Base Transceiver Station) used for encryption, encoding, decoding, modulation and feeding the RF signals to the antenna.
   ii) BSC (Base Station Controller) used for frequency hopping, traffic concentration, reallocation of frequencies among BTS and power management.
2) The Network Switching System (NSS) consisting of MSC which is its major component performs the switching of calls between the mobile and other parts of fixed or mobile networks. MSC also performs the authentication in GSM.
3) The Operation and maintenance centre (OMC) performs security management, maintenance task, network configuration, operation and maintenance task and commercial operation.

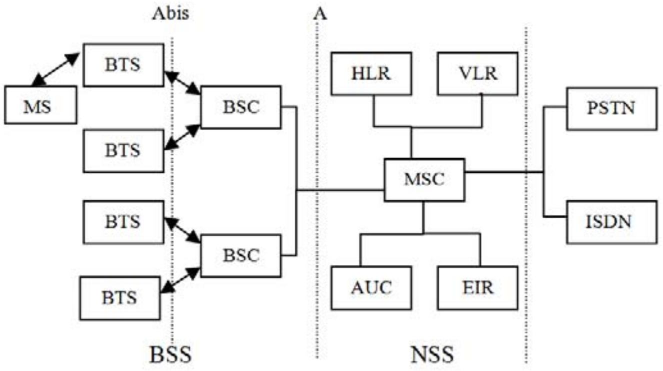


Fig. 1: GSM System architecture

3. GSM AUTHENTICATION PROTOCOL

The GSM authentication process is based on algorithm A3, A5 and A8. The GSM authentication protocol is carried out by a challenge/response mechanism which is based on asking questions that only the right user equipment might be able to answer. The returned answer computed internally in the user SIM card will be compared in the VLR. The following steps summarize the authentication protocol:

Step 1: Compare the received LAI from the visited network and the LAI of the home network. If the MS detects that it is in the new network area, it transmits a registration request to the visited network. The registration request consists of LAI and TMSI.

Step 2: Analyzing the TMSI, the VLR understands that the user is a roaming mobile station (RMS). The visited network doesn't have the ability to authenticate this roaming mobile station. So, the home domain has to be contacted for the authentication process.

Step 3: The visited network VLR through the MSC makes a request to the home domain requesting for the authentication triplet (RAND, SRES, and K_c) of this RMS.

Step 4: The Auc received the request from the VLR through the HLR.

Step 5: The Auc computes SRES and K_c by applying the MS's secret key K_i and a RAND to A3 and A8 algorithm. Home domain sends the authentication triplet to the visited network VLR through the MSC.

Step 6: After receiving the triplet, the VLR in the visited network sends the RAND to the MS through the MSC and asks the MS to compute the SRES and sends it back.

Step 7: MS computes the SRES and K_c and sends SRES back to the VLR and keeps K_c for later use.

Step 8: VLR once receives the SRES from the MS compares it with the SRES provided by the Auc of the home domain. If both are equal, the MS is authenticated by the network.

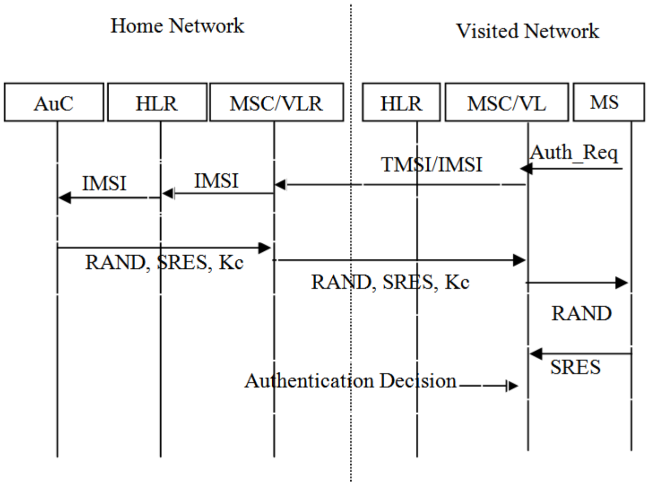


Fig. 2: GSM authentication signaling flow

4. DESCRIPTION OF A5/1

A5/1 uses 3 LFSR. We denote the LFSR as R1, R2 and R3. Registers R1, R2 and R3 are having a length of 19, 22 and 23 bits respectively. The XORing of the last bit of each LFSR gives the resultant output bit. According to their feedback polynomial, the registers are updated. Clocking decision of each LFSR is based on the clocking bit of the corresponding LFSRs. The three bits are considered (R1[8], R2[10] and R3[10]) and the majority bit is calculated by clock controlling unit. The output of the majority bit is then compared with the clock controlling bit of each register. If the clock controlling bit of the registers match with the majority bit, the respective register is clocked.

Table 1: A5/1 Registers Parameters

Register No.	Length in bits	Primitive Polynomial	Clock controlling bit	Bits that are Xored
1	19	x19+x18+x2+x+1	8	18,17,16,13
2	22	x22+x+1	10	20,21
3	23	x23+x15+x2+x+1	10	22,21,20,7

On initialization of the, the bits of the secret key is loaded, followed by the frame number and then discarding 100 output bits as follow:

```
1. Set all LFSR to 0.
2. For i: 0 to 63 do
    a) R1[0]=R1[0] Xor Key[i]
    b) R2[0]=R2[0] Xor Key[i]
    c) R3[0]=R3[0] Xor Key[i]
    d) Clock all 3 LFSR
3. For i: 0 to 21 do
    a) R1[0]=R1[0] Xor Key[i]
    b) R2[0]=R2[0] Xor Key[i]
    c) R3[0]=R3[0] Xor Key[i]
    d) Clock all 3 LFSR
4. For i: 0 to 99, Clock all 3 LFSR based on majority bit and discard the output.
```

After initialization, output stream of 228 bits is generated. To encrypt the data from the centre to the mobile station first 114 bits are used and the remaining 114 bits are used to encrypt data from the mobile phone to the centre.

5. PROPOSED A5/1 ALGORITHM

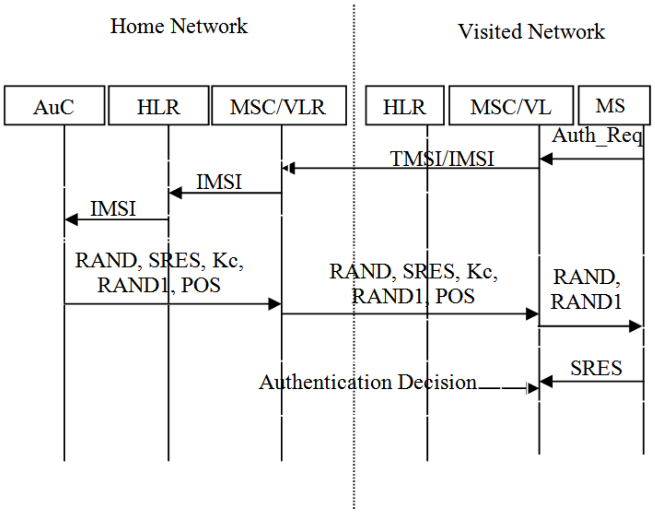
A5/1 is cryptanalyzed mainly because of the fixed clock controlling bit of each LFSR that is used as an input in the majority gate and then it is matched with the output of the majority gate. In this study, we have proposed a random clock controlling bit for each LFSR.

In the proposed A5/1, at the time of authentication process Auc centre generates another random variable RAND1 and calculates POS with the help of A3 algorithm and sends it along with the RAND, K_c and SRES. When values are received by the visitor network, it will forward RAND1 and RAND to the Mobile Station. Mobile Station calculates $K_{c,}$ SRES and Pos and transmits SRES to the VLR for authentication and keeps K_c and SRES variables for further use.

Calculation of random clock controlling bit position is done as follows:

- CCBR1= (POS) mod 19
- CCBR2= (POS) mod 22
- CCBR3= (POS) mod 23

Now these 3 randomly calculated bits are used for clock controlling and the rest of the algorithm works the same as in the original one.



6. CONCLUSION

Attackers can easily cryptanalyze the A5/1 stream cipher with basic attack just because of the fixed position of the clocking bit that is used in the original A5/1. In the proposed A5/1 algorithm the clocking bit is randomized which prevents the basic attack on this algorithm. When the original A5/1 algorithm comes under basic attack, it requires about 2^{47} running time and approximately 2^{20} bits of the output stream, whereas proposed A5/1 algorithm requires 2^{111} running time and 2^{20} bits of the output stream.

After analysis, it is seen that the proposed A5/1 decreases the possibility of Basic attack. A5/1 modified structure is easy to implement. In the proposed structure, there is randomization in the clocking bit of each LFSR.

In this paper, we have described a modified stream generator model for the GSM encryption algorithm A5/1. The new stream generator provides a cryptographically unthreatened stream cipher with respect to some popular attacks such as basic attack just by varying the clocking mechanism of A5.

REFERENCES

[1] C. C. Lee, M. S. Hwang, W. P. Yang, Extension of authentication protocol for GSM, 2003

[2] K. A. Tawil, A. Akrami, A new authentication protocol for roaming users in GSM networks

[3] I. Erguler, Emin Anarim, A modified stream generator for the GSM encryption algorithms A5/1 and A5/2

[4] Eli Biham, Orr Dunkelman, Cryptanalysis of the A5/1 GSM stream cipher NES/DOC/TEC/WP3/005

[5] Rosepreet Kaur, Nikesh Bajaj, Enhancement in feedback polynomial of LFSR used in A5/1 stream cipher

[6] Thomas F. Johnston, Security issues in a satellite global GSM network, 1999

[7] Zahra Ahmadian, Somayeh Salimi, Security enhancement against UMTS- GSM interworking attacks, 2010

[8] Majid Bakhtiari, Mohd. A. Maarof, An efficient stream cipher algorithm for data encryption

[9] Jovan D. Golic, Cryptanalysis of alleged A5 stream cipher

[10] C. C Lo, Yu-Jen Chen, Stream cipher for GSM networks

[11] M. S. Hwang, Y. L. Tang, C. C. Lee, An efficient authentication protocol for GSM networks

[12] Teletopix.org, How authentication centre works in GSM

[13] C. C. Chang, J. S. Lee, Y. F. Chang, Efficient authentication protocols of GSM

[14] B. Scheneir, Applied cryptography: protocols, algorithm and source code in c, Second Edition. Jon Wiley & Cons, Inc, 1996