Securing Mobile Technology of GSM using A5/1 Algorithm

Divyabharathi Marappan

*Department of Computer Science, Selvamm Arts and Science College(Autonomous),
Affiliated to Periyar University(Salem), Namakkal-637 003, Tamil Nadu, India*

Abstract - *The security and the authentication mechanism are very important in mobile networks since the GSM networks are susceptible to several attacks aiming to penetrate the conversation and access to data transmitted through the network. The mechanisms involved in security used to protect subscribers and service providers. The main aspects of the system that need protection are described, provided with the implementation of mechanisms used for the protection. The authentication mechanisms may even be attacked. Either by having physical access to the smart card or over the air interface, it is possible to clone a subscription. Base station functionality is required to clone a subscription over the air. Eavesdropping is the most evident threat against communication systems. The users on GSM network are provided with the GSM security and encryption algorithms for authentication and radio link privacy. One of the elements of the GSM network security is the encryption algorithm where it depends on the encryption algorithm A5/1 which is the strong encryption algorithm used for encryption of conversations on GSM mobile phones. The structure of this algorithm depends on the block cipher. The aim of this thesis is to improve GSM network security in order to overcome the weakness which appears in clocking mechanism that used in A5/1 stream cipher. New S-box generation is proposed to improve the efficiency of A5/1 majority function. The output bit-stream generated by the proposed stream cipher improves the performance.*

Key Words: **Mobile Networks, Stream cipher, Block cipher, A5/1 algorithm.**

1.INTRODUCTION

GSM is the widely used cellular standard in the world. Mobile network is the shared media and any user of the media may intercept the network. Any one can listen to or transmit on the media, when it is shared. Thus there is no longer private communication. When media are shared, authentication and privacy are lost unless some method is established to regain it. Cryptography provides the way to regain control over authentication and privacy. A5/x are the encryption algorithms used to ensure privacy of conversations on GSM mobile phones. A5/x algorithms used to secure the information sent over the air interface. In most countries, the strong version A5/1 is used. A5/1 based on stream ciphering that is very fast. A5/1 made up of linear feedback shift register. Initial value of LFSR is called seeds because values produced by LFSRs is completely determined by its current or previous state. However, LFRS can produce a sequence of bits which appears random and which has long cycle.

It is necessary to protect communications by securing them from the risk of theft and eavesdropping by GSM networks. One of the components of the security of the GSM network is the encryption algorithm used to encrypt communications is A5. The basic building block for many cryptographic primitive is the feedback shift registers. Because of the insecurities with LFSRs systems, the use of unit delays becomes very popular. The modification performed on LFSRs through adding (unit delay) to the shift register of LFSR used in original A5/1.

2.ATTACKS ON A5/1 STREAM CIPHER

The attacks on A5/1 stream cipher can be classified into two main attacks: They are known plaintext attacks and the time memory trade-off attacks. The second attack that is the, time memory trade-off can be avoided by using increment in length of registers. The plain text attacks happens by the guessing of the key bits while reset and it happens only when the intruder accesses both the plain text and the cipher text. Mostly by using XOR to implement final key stream at the end part of algorithm, the A5/1 is suffered. This causes the security problem[1].

In the proposed algorithm, the A5/1 algorithm is modified with two more LFSRs added to the original algorithm with new polynomials.

$f(x)=1+x^{14}+x^{17}+x^{18}+x^{19}$ (1)

$f(x)=1+x^{21}+x^{22}$ (2)

$f(x)=1+x^{8}+x^{21}+x^{22}+x^{23}$ (3)

$f(x)=1+x^{14}+x^{17}+x^{18}+x^{19}+x^{24}$ (4)

$f(x)=1+x^{21}+x^{22}+x^{25}$ (5)

It is noticed that the proposed LFSRs is higher of the original A5/1 algorithm. The best statistical properties is obtained by the sequences which passed the frequency test, serial test and the run test. S-box mechanism provides better randomness to the proposed algorithm than the original algorithm. The s-box is considered with the dimensions (4*16) with bits of o and 1 only. Three s-box is used to decide the order of s-box being used between s-boxes by a new method. It provides better randomness than the original. The three s-boxes used in this method are from Data Encryption Standard(DES) algorithm. The DES is used when the output of 3 LFSRs is zero. Otherwise, original A5/1 algorithm is used. One LFSR will decide the remaining two to obtain output. The clocking mechanism is changed and non linear function is added to improve the A5/1 algorithm. Mixing the register bits with the other bits is the clocking mechanism[2].

$M=C1.T1 \oplus C2.T2 \oplus C3.T3$

AND operation is performed for '.' and XOR operation is performed for '$\oplus$'. The tap bits of the equation T1,T2,T3 is represented as $T1 = R1\ (13) \oplus R1\ (16) \oplus R1\ (17) \oplus R1\ (18)$

$T2=R2\ (19) \oplus R2\ (20)$

$T3=R3\ (7) \oplus R3\ (19) \oplus R3\ (20) \oplus R3\ (21)$

C1, C2, C3 represent the clocking taps.

The proposed new nonlinear function is given below:

$Z(t)=f(X1,X2,X3) = (X1.X2) \oplus (X1 \oplus X3). (X2.X3).$

The proposed method generates new s-box based on mathematical rules. The quality of majority function is increased by using 5LFSR instead of 3LFSR with consuming time.

3.CLOCKING MECHANISM

To encrypt data stream A5/1 algorithm is widely used as encryption algorithm in GSM systems. The data is transmitted as a sequence of frames. The frame size is of 228 bit and each 114 bit is for communication in each of the direction. The algorithm is started by 64 bits, session key or the secret key with 22 bits and frame number or public key. It depends on the three LFSR.

$f(x)=1+x^{14}+x^{17}+x^{18}+x^{19}$ (6)
$f(x)=1+x^{21}+x^{22}$ (7)
$f(x)=1+x^{8}+x^{21}+x^{22}+x^{23}$ (8)

The clocking is based on majority rule using the three clocking bits X1,X2,X3 from three LFSR R1, R2, R3. The majority is counted as M=maj(X1,X2,X3). The value of M is 1 if two or more X have 1. Otherwise the value of M is 0. Only these registers are shifted regularly , the clocked bit of each register is equal to M[3].

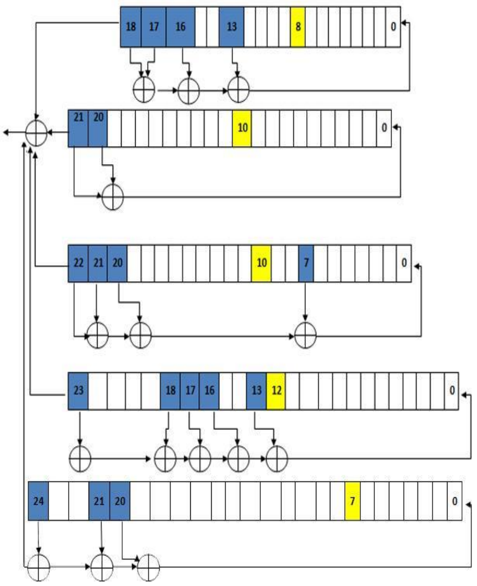

Fig -1: A5/1 with S-box majority function

4.NEW S-BOX GENERATION

Consider 5 LFSR. The s-box input will be 5 bits in which one bit from each taped register. The s-box value will decide the number of active register to be shifted from the 5 LFSR. The DES s-box concepts is used with the proposed s-box in which the first and last bits will represent the row number. The middle three bits will represent the column number. The row and the column value will be converted to decimal. There are two bits as a row data and 4 will be the maximum decimal number. For column data there will be three bits and 8 will be the maximum decimal number. Then the new s-box matrix will be 4x8 as shown in the table.
Simple mathematical calculations are used to generate new s-box as follows:
((A+B) MOD 5 = C+1)
Where,

A is the row value
B is the column value. MOD 5 is used to have values less than 5. Therefore, each value is added to one so that we have at least one register to be shifted.

Table – 1: New S-box generation

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	0	1	2	3	4	0	1	2
1	1	2	3	4	0	1	2	3
2	2	3	4	0	1	2	3	4
3	3	4	0	1	2	3	4	0

FUTURE ENHANCEMENT

By improving the algorithm versions for security further it can be more secured. A5/1 can be implemented further or A5/3 can be concentrated since these two versions provide stronger security.

CONCLUSION

The improvement to the original A5/1 algorithm and majority function(clocking mechanism) is succeeded by the proposed algorithm. The enhancement is applied to the clocking mechanism and it is found that the proposed approach has more regularity in its clocking operation. The cipher text of the proposed algorithm is more complex compared with the original algorithm. It can be concluded that cryptographically better sequences is provided by the proposed method than the original A5/1 algorithm of GSM.

REFERENCES

[1] M. Hell, T. Johansson, and W. Meier. Grain: A stream cipher for constrained environments. International Journal of Wireless and Mobile Computing, page86–93, 2007.

[2] Musheer A. and Izharuddin . Randomness Evaluation of Stream Cipher for Secure Mobile Communication. Proceedings of the 1st International conference on Parallel, Distributed and Grid Computing, IEEE(2010).page180-183.

[3] Timo G. (2008) “Hardware-Based Cryptanalysis of the GSM A5/1 Encryption Algorithm” researchgate library, pages 1-73.