Enhancement of GSM Stream Cipher Security Using Variable Taps Mechanism and Nonlinear Combination Functions on Linear Feedback Shift Registers

Darshana Upadhyay, Priyanka Sharma and Srinivas Sampalli

Abstract With the advance wireless communication, data security became a significant concern. The GSM standard hardware level encryption technique uses A5/1 algorithm circuit which embedded in the Mobile Equipment. A5/1 algorithm uses Linear Feedback Shift Register (LFSR) to produce a key streams for encode the information sent between the mobile station and the base station. It is a secure cipher among all the versions of ciphers using in GSM. However, latest research studies demonstrate that A5/1 can be subjected to several attacks owing to feeble clocking mechanism which results in a low rate of linear complexity. To overcome from these issues, we introduce a feedback tap mechanism enhanced by variable taps and four nonlinear combination functions. Analysis shows that the proposed method has a high algebraic degree of correlation immunity against basic correlation attack, mathematical attack, linear estimate attack and Berlekamp-Massey attack.

Keywords A5/1 algorithm · Linear feedback shift register (LFSR) · Correlation attack · Linear estimate attack · Nonlinear combination function · Polynomial primitives

D. Upadhyay (✉) · P. Sharma
Department of Computer Science and Engineering, Nirma University, Ahmadabad, Gujarat, India
e-mail: darshana.upadhyay@nirmauni.ac.in

P. Sharma
e-mail: priyanka.sharma@nirmauni.ac.in

S. Sampalli
Department of Computer Science, Dalhousie University, Halifax, NS, Canada
e-mail: srini@cs.dal.ca

S.C. Satapathy and S. Das (eds.), *Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems: Volume 2*, Smart Innovation, Systems and Technologies 51, DOI 10.1007/978-3-319-30927-9_18

1 Introduction

People converse over distances by wireless communication. Since huge exposure of wireless network, it's vulnerable by an eavesdropper. In the GSM communications security has offered by A5/1 stream cipher. Initially the cipher was kept undisclosed, but through leaks and reverse engineering it became public. The number of severe limitations in the cipher has been identified [1]. The A5/1 stream cipher designed using three Linear Feedback Shift Registers, length of 19, 22, and 23 bits respectively. The output of this these Linear feedback shift register is combined using XOR gate to generate the key stream for secure communication in GSM Technology.

Recent research, analysis gives you an idea about limitations of GSM cipher due to which it is vulnerable to a number of attacks [2, 3]. GSM cipher was first broken by Golic and a rough sketch of A5/1 was disclosed. After A5/1 was inverse plotted, it was investigated by Biryukov et al. [4], Dunkelman and Biham [5], Johansson and Ekdahl [6], Johansson et al. [7], and freshly by Biham and Barkan [8]. The GSM stream cipher have been poorly broken down using a range of attacks like faster time-memory trade off attack have need of some pre working out, basic correlation attack, mathematical attack, linear estimate attack, Bereleykamp-Massey attack, general inversion attack and also the brute force attack requiring no pre computation. A suitable preference of merging nonlinear function significantly advances the performance of the cipher from the security aspects. A combination function has to be impartial and nonlinear in nature; it should have high statistical degree and correlation immunity against attacks [1, 9]. Thus to carry out modifications by considering above points on the existing A5/1 algorithm to make it more robust and non-linear.

The rest of the paper is planned as follow. Section 2 stretches the comprehensive information on the A5/1 algorithm. In Sect. 3, the improved scheme of proposed A5/1 architecture is discussed. Section 4 explained the mathematical proof of proposed algorithm to enhance security of GSM stream cipher, finally conclude in Sect. 5.

2 GSM Stream Cipher—A5/1 Algorithm

The GSM stream cipher is a part of SIM card which provides security during GSM communication between Mobile station and Base station. Before start the communication the Mobile Equipment requires to acquire authentication on the network. The authentication procedure is carried out by an A3 algorithm using challenge- response mechanism by Subscriber Authentication Key Ki and a 128 bits nonce called RAND. After the authentication process A8 algorithm is used to generates the 64 bits session key Kc using Ki and RAND [10]. The Mobile station and Base station uses same 64 bits of session key to initialize the three LFSRs.

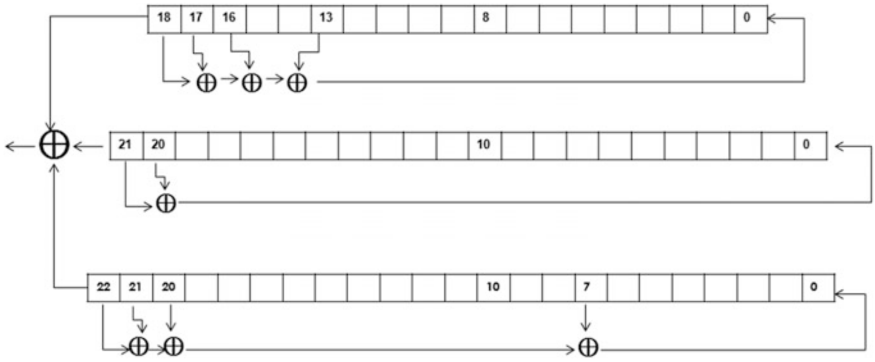

Fig. 1 Black-box view of conventional GSM stream cipher

The 64 bits of session key requires 64 clock cycles to load all the three registers. The GSM stream cipher as shown in Fig. 1 uses three LFSRs. The polynomial primitives of 19 bits, 22 bits and 23 bits are $x^{19} + x^{18} + x^{17} + x^{14} + 1$, $x^{22} + x^{21} + 1$ and $x^{23} + x^{22} + x^{21} + x^{8} + 1$ which is derived using Galois field [3]. After that 22 bits of frame counter (Fn) value is also loaded into the three LFSRs in the similar manner using 22 clock cycle. Subsequently the LFSR are irregularly clocked for 100 times using the majority rule. According to the majority rule if two or more LFSR's clocking bits are enable, then those LFSRs has been consider for that round and other become disable. Thus minimum two LFSRs has been enable in the particular round. To apply majority rule position 8 of 19 bit LFSR, position 10 for 22 bit of LFSR, and position 10 for 23 bit of LFSR is taken into consideration. These clocking bits are most irregular in nature and hence consider in majority rule. For this 100 clock cycles output bits are discarded. After that LFSRs are clocked for 228 times to generate 228 bits key stream where 114 bits are for uplink communication and 114 bits are downlink communication. This entire cycle repeats by incrementing the value of frame counter by one for a single session of communication in GSM Technology [5.10].

3 Proposed Algorithm of GSM Stream Cipher

The prototype of the suggested stream cipher involves primary modifications in the improvement in feedback tapping units as well in combining function of conventional A5/1 shown in Fig. 2. The feedback taps mechanism enhanced by six polynomial primitive for each LFSR and four nonlinear combination functions are introduced in the A5/1 stream cipher to make it more robust and protected. To rise the randomness of the output stream; instead of one polynomial primitive, to design LFSR, six polynomial primitives are used with the same degree of GF (2). Also, to

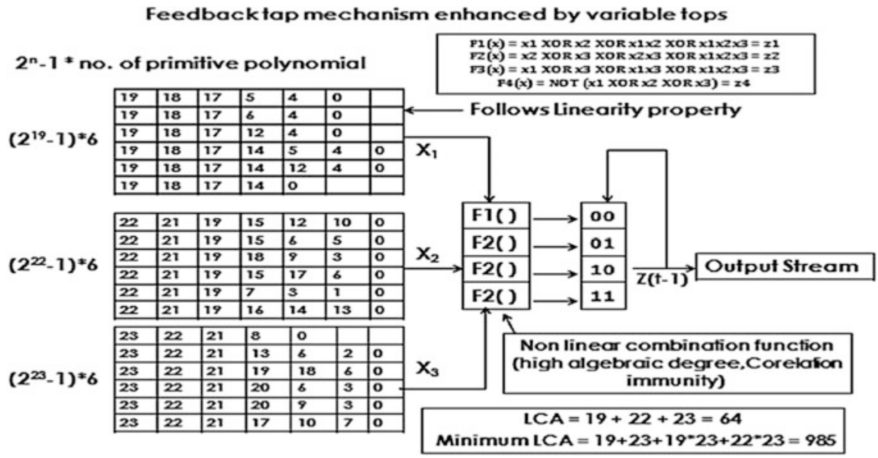

Fig. 2 Black-box view of proposed A5/1 stream cipher

decrease hardware complication, the polynomial primitives with minor distinction in tap positions is identified. Six polynomial primitives of each LFSR and access hardware requirement is also computed and state in Table 1. The key stream is produced based on four non liner function, which is known as the nonlinear combination function. Moreover, the combiner perhaps has flip-flops to store previous output key stream to compute next state of the key stream.

Table 1 Analysis of access hardware requirement

Degree of LFSR	Polynomial primitives	Access components required	
Degree of LFSR 1: 19	19, 18, 17, 14, 4, 5, 0 19, 18, 17, 14, 4, 12, 0	2 × 1 MUX	5—XOR gates
	19, 18, 17, 4, 5, 0 19, 18, 17, 4, 6, 0 19, 18, 17, 4, 12, 0	4 × 1 MUX	
	19, 18, 17, 14, 0		
Degree of LFSR 2: 22	22, 21, 19, 15, 5, 6, 0 22, 21, 19, 15, 5, 7, 0	2 × 1 MUX	10—XOR gates
	22, 21, 19, 15, 12, 10, 0 22, 21, 19, 15, 17, 6, 0	2(2 × 1 MUX)	
	22, 21, 19, 7, 3, 1, 0 22, 21, 19, 16, 15, 14, 0	3(2 × 1 MUX)	
Degree of LFSR 3: 23	23, 22, 21, 20, 3, 6, 0 23, 22, 21, 20, 3, 7, 0	2 × 1 MUX	7—XOR gates
	23, 22, 21, 8, 0 23, 22, 21, 13, 6, 2, 0 23, 22, 21, 19, 18, 6, 0 23, 22, 21, 17, 10, 7, 0	3(4 × 1 MUX)	

To enhance the linear complexity of the GSM stream cipher and to make it more conquer, four cryptography improved nonlinear functions are employed [9], each is having nonlinear order of degree three. Furthermore the combining functions are dynamic in nature using one selection bits from the preceding state of key stream P (t − 1). The four nonlinear functions f1(.), f2(.), f3(.) and f4(.) are as under:

$$f1(x) \rightarrow \alpha 1 \oplus \alpha 2 \oplus \alpha 1 \alpha 2 \oplus \alpha 1 \wedge \alpha 2 \wedge \alpha 3 = P1 \tag{1}$$

$$f2(x) \rightarrow \alpha 2 \oplus \alpha 3 \oplus \alpha 2 \alpha 3 \oplus \alpha 1 \wedge \alpha 2 \wedge \alpha 3 = P2 \tag{2}$$

$$f3(x) \rightarrow \alpha 1 \oplus \alpha 3 \oplus \alpha 1 \alpha 3 \oplus \alpha 1 \wedge \alpha 2 \wedge \alpha 3 = P3 \tag{3}$$

$$f4(x) \rightarrow \alpha 1 \oplus \alpha 2 \oplus \alpha 3 = P4 \tag{4}$$

4 Security Analysis of Proposed Algorithm

4.1 Linear Approximation Attack

It is easy to approximate linear function compare to nonlinear function by linear approximation attack. In the proposed scheme we convert linear function into nonlinear function to prevent key stream estimation [11] by linear approximation attack. Maximum linear complexity of proposed algorithm compare to original A5/1 algorithm is $LC \rightarrow 22 + 23 + 22 * 23 + 19 * 22 * 23 = 10165$ while conventional algorithm having linear complexity LC → 64, hence proposed mechanism is robust and resistive to this attack.

4.2 Correlation Attack

Firstly is intending at the nonlinear combiners, Siegen haler primary pioneered the correlation attack in the middle of the 1980s [12]. Correlation attack discovers the flaw in the combination function of given stream cipher which has numerous LFSRs series inputs and identify the relationship amongst input literals and output literals of combination function and then apply methodology to taking out information about the correlated input literals. Truth Table of input streams $\boldsymbol{\alpha 1}$, $\boldsymbol{\alpha 2}$, $\boldsymbol{\alpha 3}$ (output of each LFSR respectively) and output of nonlinear combination function **p1**, **p2**, **p3** and **p4** is as in Table 2. To pass up this attack in LFSR based stream ciphers is to decide the correlation probabilities of the function must be constant. To make it feasible, choose nonlinear function dynamically by applying a variation in its function. Correlation probabilities of sequences $\boldsymbol{\alpha 1}, \boldsymbol{\alpha 2}, \boldsymbol{\alpha 3}$ two key streams **p1(t)**, **p2(t)**, **p3(t)**, **p4(t)** is as in Table 3.

Table 2 Input stream output of nonlinear combination function

α_1	α_2	α_3	p1	p2	p3	p4
0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	1	1	0	1
0	1	1	1	1	1	0
1	0	0	1	0	1	1
1	0	1	1	1	1	0
1	1	0	1	1	1	0
1	1	1	0	0	0	1

Table 3 Correlation probabilities

$\text{prob}(\text{p1}(t) = \alpha 1) \rightarrow 5/8$ $\text{prob}(\text{p1}(t) = \alpha 2) \rightarrow 5/8$	$\text{prob}(\text{p2}(t) = \alpha 1) \rightarrow 3/8$ $\text{prob}(\text{p2}(t) = \alpha 2) \rightarrow 5/8$
$\text{prob}(\text{p3}(t) = \alpha 1) \rightarrow 5/8$ $\text{prob}(\text{p3}(t) = \alpha 2) \rightarrow 3/8$	$\text{prob}(\text{p4}(t) = \alpha 1) \rightarrow 4/8$ $\text{prob}(\text{p4}(t) = \alpha 2) \rightarrow 4/8$

When four nonlinear function **p1(t)**, **p2(t)**, **p3(t)**, **p4(t)** selected alternatively then correlation probabilities are as under.

Correlation Probability (CP) of α1:

$$\frac{1}{4}(\text{prob}(\text{p1}(t) = \alpha 1) + \text{prob}(\text{p2}(t) = \alpha 1) + \text{prob}(\text{p3}(t) = \alpha 1) + \text{prob}(\text{p4}(t) = \alpha 1)) \underset{\text{CP}(\alpha 1)}{\Rightarrow} 1/4\left[\sum_{i=1}^{4} \text{prob}(\text{pi}(t)\right] = \frac{5}{8} + \frac{3}{8} + \frac{5}{8} + \frac{4}{8} = 0.53 \tag{5}$$

Correlation Probability (CP) of α2:

$$\frac{1}{4}(\text{prob}(\text{p1}(t) = \alpha 2) + \text{prob}(\text{p2}(t) = \alpha 2) + \text{prob}(\text{p3}(t) = \alpha 2) + \text{prob}(\text{p4}(t) = \alpha 2)) \underset{\text{CP}(\alpha 2)}{\Rightarrow} 1/4\left[\sum_{i=1}^{4} \text{prob}(\text{pi}(t)\right] = \frac{5}{8} + \frac{5}{8} + \frac{3}{8} + \frac{4}{8} = 0.53 \tag{6}$$

Correlation Probability (CP) of α3:

$$\frac{1}{4}(\text{prob}(\text{p1}(t) = \alpha 3) + \text{prob}(\text{p2}(t) = \alpha 3) + \text{prob}(\text{p3}(t) = \alpha 3) + + \text{prob}(\text{p4}(t) = \alpha 3)) \underset{\text{CP}(\alpha 3)}{\Rightarrow} 1/4\left[\sum_{i=1}^{4} \text{prob}(\text{pi}(t)\right] = \frac{3}{8} + \frac{5}{8} + \frac{5}{8} + \frac{4}{8} = 0.53 \tag{7}$$

Therefore the correlation probability of output sequences $\boldsymbol{\alpha_i}$ of LFSRs and key stream **p(t)** can be removed as it is constant.

4.3 Algebraic Attack

The algebraic attack [11, 13–15] is reasonably fresh in the research literature but has so many reflexion [9]. The LFSR-based ciphers are susceptible against this attack and it has been successfully proved that the algebraic attack against a various stream ciphers is applied and well-organized [13–16]. To resist this attack, notion of algebraic degree is applied. Algebraic degree determined by the maximum number of variables employed to describe part of the function. In convention cipher an algebraic degree of the blend function is 1 instead in the proposed algorithm the algebraic degree of the blend function is 3. Hence proposed scheme offers more resistance to algebraic attack.

4.4 Berlekamp-Massey Attack

The notable Berlekamp-Massey algorithm is a very effective algorithm to determine the linear complexity of a finite binary series of bit length n within $O(n^2)$ bit operations [6, 17]. As greater the linear complexity avoids this attack. It identifies the shortest length of LFSR used in stream ciphers. This attack required twice of LC consecutive bits of the series generated by stream cipher in order to design LFSR of length LC which generates the same output key stream [1].

The change in polynomial primitive at Time instant t is

$$\text{19 bits LFSR}: 39 + 129 * t \ (38 + 44 + 46 = 128 \text{ where } \ t = 0 \text{ to } 5) \tag{8}$$

$$\text{22 bits LFSR}: 83 + 129 * t \ (38 + 44 + 46 = 128 \text{ where } t = 0 \text{ to } 5) \tag{9}$$

$$\text{23 bits LFSR}: 129 + 129 * t \ (38 + 44 + 46 = 128 \text{ where } \ t = 0 \text{ to } 5) \tag{10}$$

Thus a variable taps mechanism provides more prevention against Berlekamp-Massey attack.

5 Conclusion

This paper is attempted to upgrade security on GSM stream cipher using consolidating methodology applying on a linear feedback shift register using variable tap mechanism and nonlinear combination functions. Proposed algorithm improves keystrems in terms of randomness and offering more security. A5/1 has weak linear complexity and output keystream generation of A5/1 has a low rate of unpredictability. To defeat these issues we present variable tap system improved by six variable taps for every LFSR and four nonlinear combination functions. It has been mathematically inclined that proposed calculation is having high algebraic degree correlation immunity against correlation attack, linear approximation attack, algebraic attack and Berlekamp-Massey attack because of nonlinear combination generator on account of the nonlinear blending generator.

6 Future Work

Further work of this paper is to design existing algorithm as well as proposed algorithm using VHDL language, simulate using ISIM simulator and deploy it on FPGA-SPARTAN 6 Xilinx 12.4 ISE toolkit. NIST Statistical test suite is use to measure direct unpredictability of output key stream and compare it with an original A5/1 algorithm. Further extensions to this project is to build a generic framework of the pseudo random number generator.

Acknowledgment The authors would like to thank Nirma University and Dalhousie University for providing common platform for research collaboration. This work has been funded by Shastri research Grant—Canada. The authors would also like to thank program and member relations officer, Shastri Indo Canadian Institute for support and guidance related to project grant.

References

1. Shrestha, R., Paily, R.: Design and implementation of a linear feedback shift register interleaver for turbo decoding. In: VDAT'12 Proceedings of the 16th International Conference on Progress in VLSI Design and Test, Heidelberg (2012)
2. Sugimura, T., Shibata, K., Fujita, Y.: A method for deriving tap polynomials of LFSR generating syndromes by utilizing a matrix-reduction algorithm. Electron. Commun. Japan (Part III: Fundamental Electronic Science) **90**(1), 30–45 (2007)
3. Upadhyay, D.P., Sharma, P., Valiveti, S.: Randomness analysis of A5/1 stream cipher for secure mobile communication. Int. J. Comput. Sci. Commun. **3**, 95–100 (2014)
4. Biryukov, A., Shamir, A., Wagner, D.: Real time cryptanalysis of A5/1 on a PC. In: Advances in Cryptology, Proceedings of Fast Software Encryption'00, LNCS, pp. 1–18. Springer-Verlag (2001)
5. Biham, E., Dunkelman, O.: Cryptanalysis of the A5/1 GSM stream cipher. In: Progress in Cryptology, Proceedings of INDOCRYPT'00, LNCS, pp. 43–51. Springer-Verlag (2000)
6. Johanson, T., Ekdahl, P.: Another attack on A5/1. IEEE Trans. Inf. Theory **49**, 284–289 (2003)
7. Maximov, A., Johansson, T., Babbage, S.: An improved correlation attack on A5/1. In Proceedings of SAC 2004, LNCS, vol. 3357, pp. 1–18. Springer-Verlag (2005)
8. Barkan, E., Biham, E.: Conditional estimators: an effective attack on A5/1. In: Proceedings of SAC 2005, LNCS, vol. 3897, pp. 1–19. Springer-Verlag (2006)

9. Yamada, T., Nakajima, H.: Pseudorandom pattern built-in self-test for embedded rams. Syst. Comput. Japan **7**(12), 1–8 (2012)
10. Upadhyay, D.P., Shah, A., Sharma, P.R.: In: IEEE International Conference on Computational Intelligence and Communication Networks, Udaipur (2014)
11. Ahmad, M, Izharuddin.: Randomness evaluation of stream cipher for secure mobile communication. In: IEEE International Conference on Network Security (2010)
12. Courtois, N.T., Meier, W.: Algebraic attacks on stream ciphers with linear feedback. In: Lecture Notes in Computer Science, vol. 2656, pp. 345–359. Springer, Berlin (2003)
13. Ahmad, M, Izharuddin.: Enhanced A5/1 cipher with improved linear complexity. In: IEEE International Conference on Impact (2009)
14. Feregrino-Uribe, C., Kitsos, P., Cumplido, R., Morales-Sandoval, M.: Area/performance trade-off analysis of an FPGA digit-serial GF(2 m) Montgomery multiplier based on LFSR. Comput. Electr. Eng. **39**, 542–549 (2013)
15. Karpovsky, M., Wang, Z.: Design of strongly secure communication and computation channels by nonlinear error detecting codes. IEEE Trans. Comput. **63**(11), 2716–2728 (2014)
16. Hawkes, P., Rose, G.G.: The complexity of fast algebraic attacks on stream ciphers. In: Lecture Notes in Computer Science, Advances in Cryptology—CRYPTO2004, pp. 390–406. Springer, Berlin (2004)
17. Konheim, A.G.: Computer Security and Cryptography, p. 544. Wiley, California (2007)
18. Shah, T., Upadhyay, D.P., Sharma, P.: A comparative analysis of different LFSR based ciphers and parallel computing platforms for development of generic cipher compatible on both hardware and software platforms, Jaipur (2014)