Enhancement in Feedback Polynomials of LFSR used in A5/1 Stream Cipher

Rosepreet Kaur
Lovely Professional University
Punjab, India

Nikesh Bajaj
Lovely Professional University
Punjab, India

ABSTRACT

There is encryption algorithms used in GSM. This is for to encrypt the information when transmit from mobile station to base station during communication. As stated that A5/1 is strong algorithm but it cryptanalysis by cryptanalysts. This paper modified concept to improve A5/1 encryption algorithm by consideration of feedback combining function of LFSRs (Linear feedback shift register) use in A5/1 and modified version of A5/1 is fast and easy to implement. This is proved by the comparison of existing A5/1 and modified A5/1 with novel key stream generator using pseudorandom binary sequence. Basic security of A5/1 analysis by statistical tests given by national institute of standards and technology (NIST) in order to ensure the quality of bit stream produced by the generator.

Keywords: GSM, Encryption, A5/1 stream cipher, Clock Controlling Unit,Correlation, Statistical testing, NLFSR (non-linear feedback function)

1. INTRODUCTION

The Global system for mobile communication use various encryption algorithms[1].But the information should be secure that much nobody could interfere while communicating e.g. eavesdropper called a secret listeners. To protect our information, cryptography is used. However, for sending information mobile station to base station there is air interface serious security threat prevention between communicating parties [2]. Then question arise, how to protect during communication? For this there is encryption algorithms used in GSM as A5/x series. These algorithms used to encrypt voice and data over GSM link. The various different implementations of encryption algorithms are A5/0 has no encryption, A5/1 is strong version, A5/2 weaker version targeting market outside Europe and last A5/3 based in block ciphering strong version created as part of 3rd generation partnership project (3GPP)[3][4].

A5/1 is a strong version but exhibit weaker due to cryptanalysis. A5/1 based on stream ciphering [5] that is very fast doing bit by bit XOR. A5/1 made up of using linear feedback shift register. Initial value of LFSR is called seeds because operation of the LFSRs [6] is deterministic stream values produced by LFSRs is completely determined by its current or previous state. However, LFSR the well-chosen feedback function can produce a sequence of bits which appear random and which has long cycle [7].

Feedback shift registers is basic building block for many cryptographic primitive. Due to insecurities with LFSRs systems, the use of NLFSRs becomes very popular. In this paper, the modified structure for A5/1 is given. This modification is on LFSRs replace with NLFSRs. LFSRs are linear so it is easily predictable with BerlekampMessey algorithm.

This paper is organized in different sections as follows. In section 2 literature survey is given. In section 3 description of A5/1. In section 4 modified structure of A5/1 key stream generator. Then in last section there is included result which is given comparison between existing A5/1 and modified A5/1 using NIST test suite.

2. LITERATURE SURVEY

Mobile communication has become more convenient than ever due to openness of wireless communication. How to protect privacy was main issue for this concern focus on security of GSM and proposed architecture use public cryptography given by Chi-Chun-Lo and You-Jen Chen (1999) [8]. Stream cipher is recommended for encryption and decryption. Chi-Chun-Lo and You-Jen Chen (2000) research basis on key generator designed with respect to different level of security concerned. Research conducted by Prof. Dr. Jorg Keller, Rohde and Schwarz Gmbh from Germany present different attacks happened on A5/1 stream cipher under consideration known plaintext attack in FPGA shown that for longer communication A5/1 not secure one. Mi-Og Pak, Yeon-Hee Choi and Moon-Soeg Jun covered that stream cipher is usually used to protect data in wireless communication. New mechanism to make unsafe A5 secure used some 4*16 s-boxes and after that proposed model has better randomness and serial correlation characteristic than A5/1 [9].

Several times the A5/1 stream cipher was cryptanalysis. Another attack on A5/1 encryption algorithm is time memory trade-off based on idea of correlation attack analysis from PartrikEkdahl and Thomas Johansson (2001) [6]. And further he gave one more attack was different from others but also based on correlation attack. Whereas time memory trade off attack have complexity which is exponential with LFSRs length, complexity of the proposed scheme is independent on LFSRs [10]. In this first registers would clock irregular manner 100 times producing no output, expect after 101 irregular clocking LFSRs clock about 76 times with assumption and cryptanalysis through PartrikEkdahl and Thomas Johansson (2003) [11]. But bad property enable to launch a type of correlation attack is independent of LFSRs lengths. It depend on number of times LFSRs would clocked before producing the first output key stream that number is 100. If number increased attack become weaker.

In order to be used in future mobile communication. The improvement made by N. Komninos, B. Honary, M.Darnell (2002) in biased birthday and random sub graph attack impractical based on clocking mechanism of registers and there key set up routine. The linear complexity is important parameter for architecture A5/1 stream cipher. In modified version of A5/1 the linear complexity incremented. Encryption is process used in communication to protect information. A5/x encryption algorithm has different

encryption algorithm. The two version on stream cipher and third is block cipher i.e. A5/1/2/3. A5/1 is strong version as compared to A5/2 due export restriction. But A5/3 is based on kasumi strongest version use on 3G mobile systems. K.M.S Soyjaudah, M.A Hosany and A. Jamalloodeen (2004) [12].For generation of pseudorandom number LFSRs used but it exhibit some weakness. A5/1 algorithm use three LFSRs with majority function to add non-linearity. New design proposed from Mohamed Sharaf, Hala A.K. Mansour, HalaH.Zayed and M.L Shore (2005) [13]. Basic security of A5/1 key stream generator analysis by statistical tests applied to key stream given by National Institute Standards of Technology (NIST) is ensure quality of bit streams produces by generator covered by David Horan and Richard Guiner (2006).The research in communication security conducted by PetaBausker and Martin Drahansky (2008) there are some limitation exhibits by GSM including decryption and encryption with consideration cryptology included subscriber identity, integrity, confidentially, authentication and encryption etc [13].

Enhancements strictly needed in GSM due cryptanalysis. Cryptographic attacks like correlation, algebraic, linear approximation attack [14][15]. Proposed architecture has high linear complexity as compared to A5/1 encryption algorithm presented by Musheer Ahmed and Izharuddin (2008) [16]. Time memory trade off attack is based on birthday paradox. Goal of this attack on find any intersection between pre-computed LFSRs states set and set of states generating the output in actual execution of time. The weakness of A5/1 key stream clocking control bit at middle of LFSRs. To improve that there should be decrement of pre-processing and collision probability covered by HosseinKourkchi, HamidrezaTavakoli and MajidNaderi (2010) [17]. On the behalf of this literature survey this paper for to improve A5/1 algorithm by make linear operator a non-linear feedback mechanism.

3. DESCRIPTION OF A5/1

A5/1 is a stream cipher [18] provide key stream so called key stream generator. Made up of three linear feedback shift register of length 19, 22, 23 used to generate sequence of binary bits. GSM conversations are in form of frames as length of 228 bit i.e. 114 for each direction for encrypt/ decrypt data [12]. A5/1 initialize 64 bit key together with 22 frame number publicly known. It uses three LFSRs as R1, R2 and R3 correspondence feedback polynomial as (13, 16, 17, and 18) for R1, (20 and 21) for R2 and (7, 20, 21 and 22) for R3 respectively. Each LFSR is clock using rule called a majority rule. Clocking bit consider as A, B, C to correspondence registers R1, R2 and R3 as for R1 is 8, for R2 is 10 and for R3 is 10. Before register is clock feedback is calculated by using linear operator i.e. XOR. Then one bit shift to right (discarding the rightmost) bit produce by feedback location store leftmost locations of LFSRs. This cycle goes up to 64 times. This process done on basis of clocking rule the register is clocked irregularly according to majority rule. Majority rule is use on three clocking bits of LFSRs A, B, C. Among clocking bits if one or more is 0, then m=0 those LFSRs clocking bit value match with m that will clock. Similarly, if one or more clocking bits is 1, then whose values match with m that will clock. At each clocking LFSR generate one bit which combined by linear function i.e. XOR. In A5/1, the probability of an individual LFSR being clocked is ¾ [19]. The clocking bit generates bit m defined as using Boolean algebra function is (A ∧ B (+) B ∧ C (+) A ∧ C) where (+) for XOR gate, ∧ for AND gate as shown in figure 1.

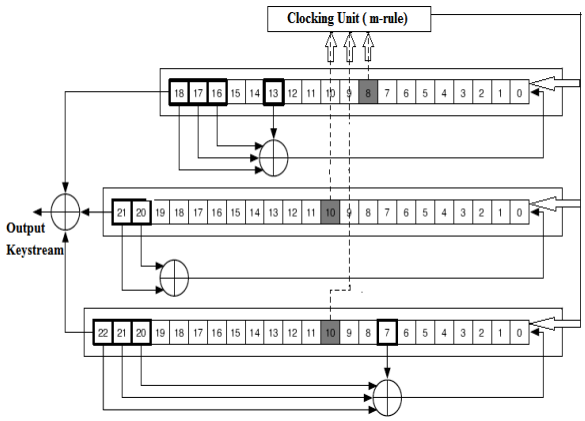

Figure 1: Structure of A5/1 stream cipher

4. NON-LINEAR FEEDBACK SHIFT REGISTERS

Feedback shift registers has many applications in cryptography. The FSRs with linear feedback function called linear feedback shift registers have many drawbacks like it is easy to find LFSRs with maximum period, it is linear so due that insecure for cryptographic applications and it is easily predictable using berlekamp-messey algorithm. Many attempt made to make this combining function non-linear because it adds irregularity to output streams or bits. That irregularity is play vital role for unpredictability of output stream. This type of FSRs called non-linear shift registers. There is no efficient method that feedback function finds the maximum period of NLFSRs. In this work, propose an A5/1 algorithm using NLFSRs.

The improvement in the feedback polynomial of A5/1 use by LFSRs present in A5/1 stream cipher. In LFSR1 is of length 19 similarly LFSR2 and 3 is of length 22 and 23. A5/1 consist feedback polynomial are for R1 is (18, 17, 16, 13), for R2 is (21, 20) and for R3 is (22, 21, 20, 7).

In the proposed structure of A5/1 encryption algorithm the feedback polynomials are not directly XOR as before register is clock feedback is calculated by using linear operator. Then one bit shift to right (discarding the rightmost) bit produce by feedback location store leftmost locations of LFSRs [20]. The proposed structure quite change the feedback polynomials present in existing A5/1 as for R1(18), R1(17), R1(16) and R1(13) similarly for R2(21) and R2(20) , for R3(22), R3(21), R3(20) and R3(7) before. The correspondence LFSRs feedback polynomials are directly bit-x-or. But in proposed idea it changes up to some extent where Θ for NOT gate, ∧ for AND gate, (+) for XOR gate illustrated in figure 2.This get by comparing thefigure 1 with figure 2.

5. NIST RESULT ANALYSIS

This section explores the comparison of A5/1 and modified A5/1.If comparesthe existing A5/1 and modified key stream generator. After implementation of both existing and modified A5/1 algorithms they are analysis with NIST Test Suite. It is verified that p-value of 100 different key streams each of length 10000. Average of 100 key streams shown in form of table that existing A5/1 and modified A5/1 both are pass all results because p-value is higher than 0.01 under consideration of NIST test suite as illustrated in figure 3[2]. But, the modified A5/1 algorithm is gives higher p-valuesthan the existing A5/1 key stream generator.

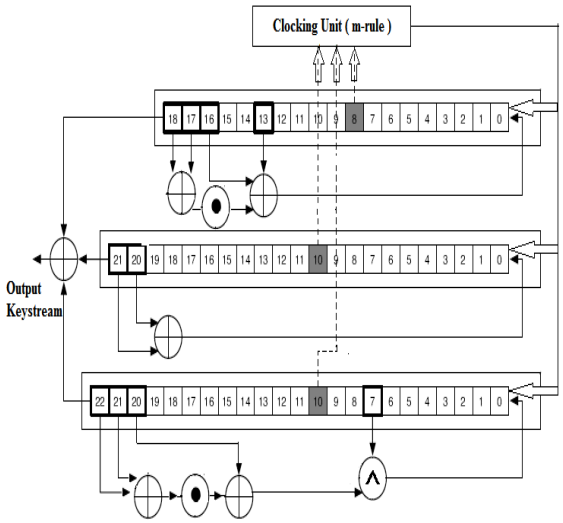

Figure 2: Structure of proposed A5/1 stream cipher

From the experiment, it can be seen that modified A5/1 design provides good source of random number for cryptographic purposes. In figure 4, average result of 100 key streams of length 10000 came. Refer table 1, Consider approximate entropy test this compare the frequency of overlapping blocks in bits against expected result for randomness calculated p-value which is higher and approaches to 1. The result for block frequency test is give higher p-value because focus on proportion of ones with in M-blocks is approximately M/2 i.e. 5000 because input bit was 10000. If M=5000 the p-value is 1 however based on M P-value will increase or decrease.

Table 1: Average of 100 Key Streams of A5/1

Tests	(A5/1) P-values	(Proposed A5/1) P-values	Result
Approximate Entropy	0.1129	0.1134	Success
Block Frequency	0.5092	0.5430	Success
Cum Sum Forward	0.4745	0.4907	Success
Cum Sum Reverse	0.4565	0.4765	Success
DFT	0.6144	0.6228	Success
Frequency	0.4785	0.4845	Success
Lempel Ziv	1	1	Success
Linear Complexity	0.4911	0.5033	Success
Longest Run	0.4610	0.5967	Success
Overlapping Template	0.4593	0.5113	Success
Rank	0.4312	0.4318	Success
Runs	0.5785	0.5034	Success
Serial Test 1	0.4655	0.4816	Success
Serial Test 2	0.4707	0.4925	Success

In cum-sum forward/reverse test about maximal excursion (from zeros) of random walk. It is to determine cumulative behavior of cumulative sum for random sequence is not too large or small. If cum-sum too large or too small then p-value goes to decrease but here increased. In DFT test to detect periodic feature that number of peak of DFT exceeding 95% threshold is significantly different than 5%. In this test p-value comes higher means peaks comes under threshold values is more. Frequency test is similar to block frequency but this for mono-bit not for block. Here number of zeros and ones approximate comes same as compared to existing A5/1. Linear complexity test for LFSRs to determine the sequence is complex enough to be considered random or not. By higher p-value it depict that the sequence is more complex that existing A5/1 sequence. For longest run test to determine consistency of ones if irregularity in expected length of longest runs of ones more that it directly disturbed the regularity of zeros so mean due to higher p-value regularity is more. The overlapping template test for to check number of occurrence pre- specified the target strings. The ranks test higher p-value because linear dependence among fixed length substring of original sequence is good. In run test, runs should be half of length of input bit sequence if it is half then p-value is 1 else if it decrease or increase corresponding p-value goes to decrease. Here in modified the runs test's p-value is only less due to its value deviated from value half of lengthof input bit sequence but difference is less. For serial test consider all possible overlapping m-bits patterns across the entire sequence. This test is determined the number of occurrences of the 2m m-bit overlapping patterns is approximately the same as would be expected for a random sequence[2].

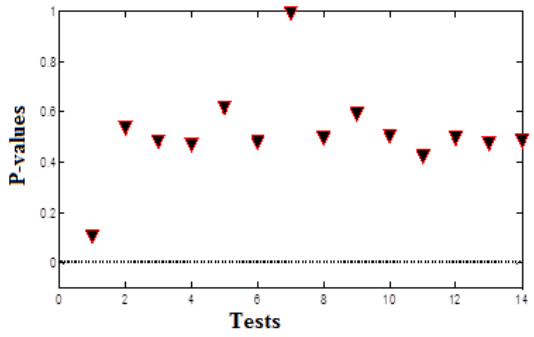

Figure 3: NIST Test result for 100 key Stream (P-Value ≥ α)

The run test is only which p-value is less existing A5/1 then modified A5/1 due number runs of 0s and 1s. But all other results are improved. Graph shown in form of bars through MATLAB (R2009A) between p-values against distinct tests as mentioned p-values illustrated in table 1. Compare the existing and modified A5/1 stream cipher with modification in combining function using for feedback polynomials. For existing A5/1 directly bit-x-or take place by using feedback polynomials but in proposed stream cipher change by using gate or Boolean algebra.

6. CONCLUSION

As concluded that A5/1 basically used for secure communication during air interface. A5/1 key stream generator is easy to implement and also efficient encryption algorithm used in communication application GSM. The encryption method uses the selective encryption approach where the coefficients selection. That done on MATLAB

(R2009A) as result obtained in form of graph. After analyses attacks happen through literature review and try to find A5/1 weakness. So, it exhibit weakness like length of LFSRs is short and basic correlation attack. After analysis these things decreased the possibility of correlation attack. A5/1 modified structure has been given which is easy to implement and fast to do. The proposed structure is converting LFSR to NLFSR. In proposed structure there is change in combining function for feedback polynomials. This paper proposes a high speed and minimum cost A5/1 key stream algorithms but minor increase in hardware.

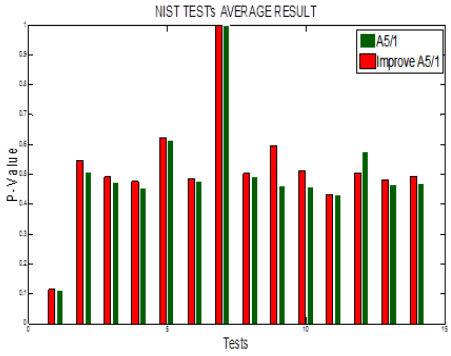

Figure 4: NIST Test result for 100 key streams for proposed A5/1

7. FUTURE WORK

The correlation and brute force attack is quite improved in this thesis. Apart from these attacks differential attack and algebraic attack are more attention from an analysis. And design as well as for condition something adds to or modify for future work. For construction of stream ciphers well documented strategies is not rich as for block cipher. Most theoretical results are concerned with Boolean combining function or non-linear filters. But stream ciphers are easy and fast to do more modification can add under this consideration. At last A5/1 encryption algorithm cryptanalysis many find weakness for these attacks and improvement also does on that behalf.

8. REFERENCES

[1] *Mobile networks security*,tklmarkuspeuhkuri ,2008-04-22

[2] http://csrc.nist.gov/groups/ST/toolkit/rng/documentation _software.html.

[3] Communication security in gsm networks petrbouška, martin drahanský*faculty of information technology, brno university of technology*

[4] *A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony* Orr Dunkelman, Nathan Keller, and Adi Shamir.

[5] *Instant cipher text-only cryptanalysis of GSM encrypted communication*, EladBarkan, Eli.

[6] On LFSR based stream cipher ,*analysis and design* , PatrikEkdahl.

[7] *GSM Security and Encryption by David Margrave*, George Mason University.

[8] *Stream Ciphers for GSM Networks*,Chi-Chun La and Yu-Jen Chen Institute of Information Management,NationalChiao-Tung University.

[9] Mi-Og Park, Yeon-Hee Choi, Moon-Seog Jun, Modified A5/1Stream Cipher using S-boxes.

[10] PatrikEkdahl and Thomas Johansson, *Another Attack on .A5/11*, ISIT2001, Washington, DC, June 24-29, 2001

[11] PatrikEkdahl and Thomas Johansson, Another Attack on A5/1, *IEEE transactions on information theory*, vol. 49, no. 1, January 2003

[12] *A précis of the new attacks on GSM encryption* Greg Rose, QUALCOMM Australia.

[13] MohmedSharaf I, HalaA.K.Mansour', HalaH.Zayed3, M L Shore, a *complex linear feedback shift register design for the a5 key stream generator*, Twenty Second National Radio Science Conference (NRSC 2005).

[14] David Horant and Richard Guinee, *A Novel Key stream Generator using Pseudo Random Binary Sequences for Cryptographic Applications*, ISSC 2006, Dublin Institute of Technology, June 28-30.

[15] Musheer Ahmad and Izharuddin, *Security Enhancements in GSM Cellular Standard*, ©2008 IEEE.

[16] *Enhanced a5/1 cipher with improved linear complexity* ,musheerahmad and izharuddin

[17] HadiKhorrami, Mahmoud Ahmadian, BehrouzHajian, *The New Results of Correlation Attack on A5/1*, IEEE-2010

[18] Bruce Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C*, Second Edition. Jon Wiley &Cons, Inc. 1996. ISBN 0-471-12845-7. Page 382 of section 16.4: Stream Ciphers Using LFSRs.

[19] *Security enhancements for a5/1 without losing hardware efficiency in future mobile systems*,n. komninos, 'b. honary, m. Darnel1

[20] Cagdas CALIK, meiltem SONMEZ TURAN and ferrukozbudak, "*On feedback functions of maximum length non-linear feedback shift registers",IEICE TRANS,2010*