Analysis and Design of Alternating Step Shrinking Generator (ASSG) for Improved Security

Ghoosia Arshad, Aihab Khan, Malik Sikandar Hayat Khiyal, and Mina Masood

Abstract—**In this paper, we propose a model for alternating step shrinking generator (ASSG) by combining models of shrinking generator (SG) and alternating step generator(ASG) for improved security and analysis of correlation attack is performed. This research also compares for alternating step shrinking generator with shrinking generator and alternating step generator for correlation attack. The model of alternating step shrinking generator becomes more complex, the length of generated key stream is much larger and correlation attack are found to be reduced. Also, in alternating step shrinking generator, features of both alternating step generator and shrinking generator are combined which increases security. This research concludes that for the encryption of plaintext, alternating step shrinking generator is more secure than shrinking generator and alternating step generator.**

Index Terms—**Alternating step generator, Correlation attack, Linear feedback shift register, Shrinking generator.**

I. Introduction

Shrinking generator and alternating step generator are two clock-controlled based stream ciphers for the generation of key stream. Shrinking generator is secure at length of 64 and alternating step generator is secure at the length of 128 against the correlation attack. Shrinking generator is more efficient than alternating step Generator [3].

This research combines the alternating step generator and shrinking generator to form alternating step shrinking generator (ASSG). Also, features of both alternating step generator and shrinking generator are combined for improved security though combined structure mechanism slows down the speed of the clock-controlled generator.

The weaknesses of the alternating step generator and shrinking generator can attempt to be removed if the alternating step generator and shrinking generator are combined, in this way the model becomes more complex for the attacker, the length of generated key stream would be much larger and correlation attack can be reduced. Combined structure is stronger than the individual structure of the ASG and SG, used in most stream ciphers. Combined structure mechanism for LFSR is found to be effective method to improve the security of the stream cipher.

This study also uses an approach, better than previous approaches as it imposes an additional check in addition to the security of the shrinking generator that is 2^2L and increases the security of stream ciphers by increasing length of the period considerably.

The organization of paper is as follows:

Section 2 discuss related work, Section 3 elaborates proposed framework. The proposed techniques along with algorithms are presented in Section 4. Section 5 discusses experimental results and the paper is concluded in Section 6.

Manuscript received December 6, 2010; revised June 27, 2011.

Authors are with Department of Computer Science, Fatima Jinnah Women University, Rawalpindi, Pakistan (ghoosia_arshad22@yahoo.com, aihabkhan@yahoo.com,m.sikandarhayat@yahoo.com, menotee@yahoo.com).

II. Related Work

Coppersmith et al, [9] described a shrinking generator which is a suitable crypto-generator for steam cipher applications for two reasons; firstly it has a large period and large linear complexity, and secondly, it has good statistical output**.** There structure is appropriate for both fixed as well as variable connection linear feedback shift registers. For fixed connection implementation only the seed that is the early contents of shift registers LFSR A and LFSR S comprise the secret key for the pseudorandom generator. If the variable connections are used then the value of these connections is also a part of the key. The difficulty of irregular output is severe in immediate applications there model gives the solution of using a small buffer for the shrinking generator output proposed to collect bits for the SG output. In their model they use variable connections which give a large degree of elasticity to the structure. Conventional attacks on linear feedback shift register based models are not valid to their model because of its different character. Kanso et. al. [6], discuss a clock-controlled alternating step generator. the clock-controlled alternating step generator is a sequence generator consisted of three FSRs A, B and C which are consistent, the output of one of the three FSRs (feedback shift registers) controls the clocking of the other two FSRs. If FSR A is 1 then FSR B is clocked but FSR C is not clocked, similarly if FSR A is 0 then FSR C is clocked but FSR B is not clocked. The output of these generators generate a key stream which is then XOR-ed with the plain text to make a cipher text .The period, the lower and upper bound of the linear complexity of the output sequences of the structure whose control register produces a de Bruin sequence and the other two registers produce m-sequences are recognized. Furthermore, it is traditional that the distribution of short patterns in these output sequences take place equally likely and that they are protected against correlation attacks. All these properties make it a suitable crypto-generator for stream cipher applications. Safdar et. al. [8], describes the performance evaluation of stream ciphers on large databases, caters correlation attack against shrinking generator and alternating step generator, by gradually increasing the length of initial input bits of linear feedback shift registers (LFSR's), which increases the length of the key. After implementing

both algorithms it is found at length of 64 shrinking generator is secure and at length of 128 alternating step generator is secure against correlation attack. It is also found that shrinking generator is more competent and secure than alternating step generator.

III. Proposed Framework

The main idea behind the proposed model is introducing the combined structure of alternating step generator and shrinking generator. The combined structure of clock-controlled generators is effective method to improve security of stream ciphers. Alternating step generator and shrinking generator are widely used stream ciphers for the generation of key stream. Both the generators have some common weaknesses which if analyzed properly can break the key stream. General attacks on these two stream ciphers are correlation attacks that is "if a cryptanalyst can in some way detect a correlation between the known output sequence and the output of one individual LFSR this can be used in a divide and conquer attack on the individual LFSR". The proposed model described in Fig. 4.1, will attempt to verify that combined structure of Alternating step generator and shrinking generator is more secure against Correlation attack.

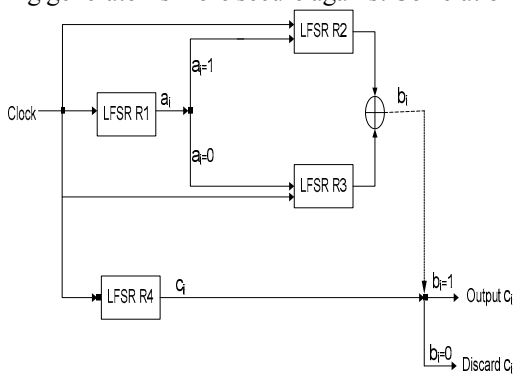

Fig. 1. Proposed Model of ASSG

The proposed model consists of four linear feedback shift registers (LFSRs), LFSR R1, LFSR R2, LFSR R3 and LFSR R4. The size of each register is varying. R1 is clocking register which controls the clocking function of other three registers, R2, R3 and R4 are generating registers which generate key stream.

IV. Proposed Technique

The graphical model of the proposed system is presented in figure 1 which shows that input to linear feedback shift registers is given, which generates sequences according to the number of linear feedback shift registers. The generated sequences then produce the key stream. Data from the database is retrieved which is first converted into binary form and then with the help of generated key stream, the original data is encrypted. Finally the encrypted data is decrypted when it is xored with the key stream.

The algorithms used in figure 1 are elaborated as follows:

Algorithm: Input to LFSRs
Input: combination of 0's and 1's
Output: Null
Read values (0's and 1's)
Output Null
Algorithm: Sequence Generation
Input: Values from LFSRs
Output: Sequence of bits
Read values of LFSRs
Seq=L [Length-1].To string ()
this.ListBox.Add(Seq)
Generates Sequence
Algorithm: Key Generation
Input: Generated Sequences
Output: Key Stream
Read generated sequence
Register R1 is clocked.
If the output of R1 is 1 then:R2 is clocked; R3 is not clocked but its previous output bit is repeated.(For the first clock cycle, the "previous output bit" of R3 is taken to be 0.)
If the output of R1 is 0 then:R3 is clocked; R2 is not clocked but its previous output bit is repeated.(For the first clock cycle, the "previous output bit" of R2 is taken to be 0.)
The output bits of R2 and R3 are X_ORed
Register R4 is clocked.
If the (R2 & R3) XoRed is 1 the output bit of R4 from part of key stream.
If the (R2 & R3) XoRed is 0 the output of R4 is discarded
Generates Key Stream.
Algorithm: conversion of characters into binary
Input: names from Database
Output: binary data
Read names from database
power = (int)Math.Pow(2, k)
Output binary data
Algorithm: Encryption
Input: Generated Key stream and Binary Data
Output: Encrypted Data
Read generated Key stream and Binary Data
XOR generated key stream and binary data
Generates Encrypted data
Algorithm: Decryption
Input: Encrypted Data and Key stream
Output: Original Data
Read encrypted data and Key stream
XOR encrypted data and key stream
Generates original data

V. Experimental Results

Table 1 shows Comparison of Alternating Step Generator, Shrinking Generator and Proposed Alternating Step Shrinking Generator.

After comparing the three algorithms it is found that if all the three algorithms are compared on the basis of linear feedback shift registers then proposed generator has more lfsr's then alternating step generator and shrinking generator which makes the proposed generator's structure more complex than ASG's and SG's structure which reduces the possibility of correlation attack. Secure length of linear feedback shift registers in case of proposed generator is 64

which is secure length against correlation attack.

TABLE1: COMPARATIVE ANALYSIS OF ALTERNATING STEP GENERATOR, SHRINKING GENERATOR AND PROPOSED ALTERNATING STEP SHRINKING GENERATOR

Claim	SG	ASG	ASSG
Linear Feedback Shift Registers	2	3	4
Construction(Logic Gates)	No Gates	And, Not	No Gates
Structure	simple	Complex	Complex
Period	$(2^{L2}-1).2^{L1}$	$2^{L1}.(2^{L2}-1)$ $.(2^{L3}-1)$	$2^{L1}.(2^{L2}-1).(2^{L3}-1)$ $(2^{L4}-1)$.
Security	2^{2L}	2^{L}	2^{2L}
Secure Length against correlation attack	64	128	64

After comparing all the three algorithms with respect to the properties in the table 1, it is found that Proposed Generator and Shrinking Generator provide same level of security and have a secure length against correlation attack but proposed generator uses more LFSRs which increase period. Proposed generator seems to be a better choice to generate a key stream because of its large period.

A. Comparison for period of Shrinking Generator, Alternating Step Generator and Proposed Generator

Test1

Shrinking generator has two LFSRs. By giving values 3 and 5 to respective LFSRs, period calculated is 2^8= 256. Alternating step generator has three LFSRs. By giving values 3, 4 and 5 to respective LFSRs, period calculated is 2^12= 4096. Proposed generator has four LFSRs. By giving values 3, 4, 5 and 7 to respective LFSRs, period calculated is 2^19= 524288.

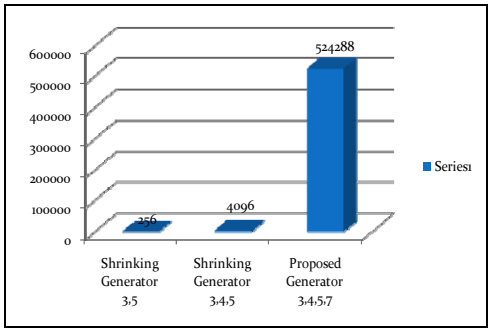

Fig. 2. Graphical representation of Case 1

Fig. 2 shows the graphical representation of the difference between the periods of shrinking generator, alternating step generator and proposed generator which shows that by increasing number of LFSRs period of the key-stream increases.

Test 2

Shrinking generator has two LFSRs. By giving values 11 and 13 to respective LFSRs, period calculated is 2^24= 16777216. Alternating step generator has three LFSRs. By giving values 11,13 and 13 to respective LFSRs, period calculated is 2^37= 1.3744*10^11. Proposed generator has four LFSRs. By giving values 11,13,13 and 13 to respective LFSRs, period calculated is 2^50=1.25899*10^15.

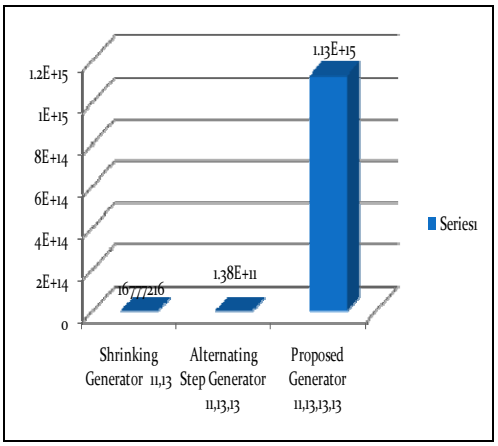

Fig. 3. Graphical representation of Case 2

Fig. 3 shows the graphical representation of the difference between the periods of shrinking generator, alternating step generator and proposed generator which shows that by increasing the length of LFSRs, period of the key-stream increases.

VI. CONCLUSION

Secure length of linear feedback shift registers in case of ASSG is 64 which is equivalent to the security of Shrinking Generator but the technique used in ASSG is stronger than that of SG's and ASG's. It is concluded that for the encryption of plaintext, combined generator is more secure. In future ASSG can be modified by using shrinking generator before alternating step generator that becomes SASG (shrinking alternating step generator) for which complexity and period of SASG can be calculated. Also security of ASSG can be checked against other attacks.

REFERENCES

[1] A. Menezes, P. van Oorschot and S. Vanstone "Handbook of Applied Cryptography" 1996
[2] Search\Stream cipher - Wikipedia, the free encyclopedia.htm, 2nd April 2010
[3] Stallings.W "Cryptography and Network security" fourth edition
[4] Search\Shrinking generator - Wikipedia, the free encyclopedia.htm, 5th April 2010.
[5] D. Coppersmith, H. Krawczyk, and Y. Mansour, "The shrinking generator," Ad-vances in Cryptology - CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 22-39, 1993.
[6] Kanso.A.A "Clock-Controlled Alternating Step Generator " King Fahd University of Petroleum and Minerals. 2002
[7] Don Coppersmith et.al "Shrinking Generator" IBM T.J. Watson Research Center Yorktown Heights NY 10598. 1988
[8] Malik Sikandar Hayat Khiyal, Aihab Khan, Saria Safdar "Performance Evaluation of Stream Ciphers on Large Databases" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.9, pp. 285-289, September 2008, USA
[9] Don Coppersmith "Shrinking Generator" IBM T.J. Watson Research Center Yorktown Heights NY 10598. 1988
[10] C. G. Gunther, "Alternating step generators controlled by de Bruijn sequences", In proceedings of Eurocrypt 87, lecture notes in computer science, Berlin: Spinglerverlag vol .309, 1988 ,pp 5-14.

Ghoosia Arshad is a graduate from Dept. of Computer Science, Fatima Jinnah Women University, Pakistan.

Mr. Aihab Khan works in Dept. of Computer Sciences Fatima Jinnah Women University Pakistan. His research interests are in the field of Data Mining, Data Warehousing as well as Information security.

M. Sikandar H. Khiyal born at Khushab, Pakistan. He is Chairperson Dept. Computer Sciences and Software Engineering in Fatima Jinnah Women University Pakistan. He Served in Pakistan Atomic Energy Commission for 24 years and involved in different research and development program of the PAEC. He developed software of underground flow and advanced fluid dynamic techniques. He was also involved at teaching in Computer Training Centre, PAEC and International Islamic University. His area of interest is Numerical Analysis of Algorithm, Theory of Automata and Theory of Computation. He has more than one hundred research publications published in National and International Journals and Conference proceedings. He has supervised more than one hundred and thirty research projects at graduate and postgraduate level. He is member of SIAM, ACM, Informing Science Institute, IACSIT. He is Co editor of the journals JATIT and International Journal of Reviews in Computing. He is reviewer of the journals, IJCSIT, JIISIT, IJCTE, IJCEE, JCIE and CEE of Elsevier.

Mina Masood is a graduate from Dept. of Computer Science, Fatima Jinnah Women University, Pakistan.