Security Provisions in Stream Ciphers Through Self Shrinking and Alternating Step Generator

Hafsa Rafiq #1, Malik Sikandar Hayat Kiyal#2 , Aihab Khan #3
#Department of Software Engineering Fatima Jinnah Women University, The Mall, Rawalpindi, Pakistan

***Abstract*— in cryptography stream ciphers used to encrypt plain text data bits one by one. The security of stream ciphers depend upon randomness of key stream, good linear span and low probability of finding the initial states of pseudorandom generators. In this paper we propose a new stream cipher model use Feed back with carry shift registers (FCSRs) as building blocks which are considered as a source of long pseudorandom generator. Proposed model is the combined structure of alternating step generator and self shrinking generators which are commonly used stream ciphers generators. In this research we compare proposed generator against self shrinking generator (SSG), Alternating step generator (ASG) and alternating step self shrinking generator (ASSG) and we concludes that proposed generator architecture is best for encryption because it satisfies all necessary conditions of a good Stream cipher.**

Keywords-component; Alternating step generators; Feed back with carry shift registers; Self shrinking generators.

I. Introduction

Stream cipher is an important method for information encryption. “A stream cipher is a symmetric cipher which operates with a time-varying transformation on individual plaintext digits”[1]. Stream ciphers typically encrypt data efficiently and have very low memory requirements and therefore cheaper to implement in limited scenarios. Stream cipher techniques are usually best for the cases where the amount of data is either unknown, or continuous such as network streams.

Linear feedback shift registers (LFSRs) are mostly used in many key stream generators due to their simplicity but inherent linearity of LFSRs not sufficient to provide security to stream ciphers. Because of their linearity their initial vector can be determined by using Berlekamp-Massy algorithm. To improve the security a new type of pseudorandom binary sequence generator called FCSR is introduced. They have good statistical properties, having proved period, highly nonlinear in nature and have non degenerating states.[2].They are much similar to LFSRs except that instead of using addition modulo 2 FCSR uses carry propagations that bring non linearity in to their structure which is main characteristic of FCSR.

In this paper, we propose a model which combines two clock controlled keystream generators that are: alternating step generator and self shrinking generator to strengthen the security. Combined structure of both generators can help to avoid pitfalls that cause when these generators are used individually. Proposed generator is more secure because length of generated key stream is much greater than individual generators and complex structure is not easily breakable. Proposed model use FCSRs as a main building block and combine the output with full adder function.

The paper is organized in such a way that: section 2 discusses related work to proposed schemes, section 3 devoted to proposed framework, section 4 discuss proposed technique along with algorithm ,section 5 discuss simulation results and finally concluding remarks are given in section 6.

II. Related Work

Ali kenso [3] proposed a modified version of existing self shrinking generator proposed by Meier and Staffelbach based on selection rule which XOR pair of bits. MSSG constructed with single LFSR having length of n bits. The selection rule for the output of LFSR is that : select triple-bit($a_{3i,}a_{3i+1}$,a_{3i+2}) then XOR first pair of bit a_{3i} and a_{3i} if result of XOR is 1 then output of MSSG becomes 3rd bit a_{3i+2} else discard triple bit .MSSG satisfies the basic requirements of good stream ciphers that are long period ,high complexity and non-linearity and proved that period p satisfies $p^{n/3}$<=p<=p^{n-1} and linear complexity becomes greater than half the period. S.Shun-lung , Ko-ming Chiu, , and Lih-chyau Wuu [4], discuss “LFSR/FCSR based Alternating step generator” and a new combination function after analyzing existing ASG. According to the their analysis, the probability of finding the pairs of base sequence sequences (X_{n+1}, Y_{n+1}) which satisfy the condition of zero edit distance D(X_{n+1}, Y_{n+1},K;Z_n) with exclusive-or operation is larger than addition operation. A new stream cipher generator is proposed by Ghosia Arshad [7], which is combination of shrinking generator and alternating step generator. Model is analyzed against co relational attacks and concluded that its security becomes 2^{2L}.

Model consists of 4 LFSRs A, B, C, D.LFSR A control sequence of LFSR B and C if output of LFSR A is 1 it activates LFSR B otherwise activate LFSR C. output of LFSR B and C is XORed if its result is 1 then generate output keystream of LFSR D else discard output of D.

III. Proposed Framework

The proposed model combines the features of both self shrinking generator proposed by Ali Kanso [3] and alternating step generator [4] to generate the strong pseudorandom keystream sequence. Proposed stream cipher system model based on FCSRs that introduce non linearity in proposed structure and make difficult to investigate the right initial states of registers due to carry propagations. To achieve the high security and to ensure important properties of FCSRs following conditions must be satisfied.

- Connection integer q must be negative prime number.
- Size of FCSR must be $r = \lfloor \log_2 (q+1) \rfloor$ [5].
- Additional bits of memory must be $\lfloor \log_2 \lceil (r \rceil) \rfloor$
- The order of 2 modulo *q* is |*q*|-1[8].

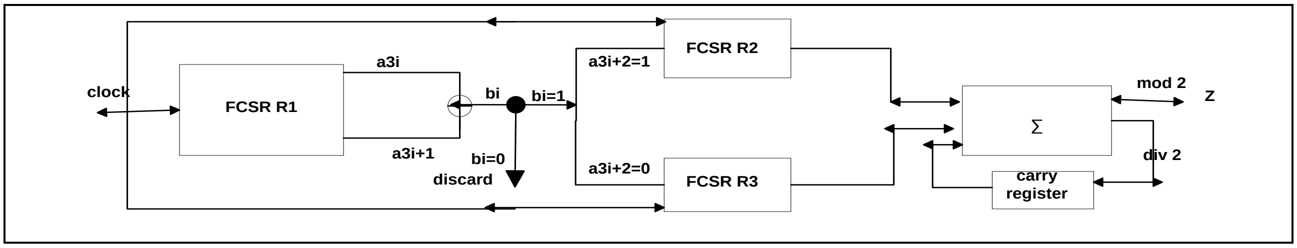

Figure 1: Detail structure of proposed model for stream ciphers generator

The Proposed model as shown in “Fig. 1”constructed in such a way that self shrinking generator is used to produce shrunken pseudorandom sequence and this shrunken output is used to control the remaining two registers. Output of these two registers is combined by full addition function and the resulting pseudorandom key stream is XORed with plain text to produce encrypted data. Resulting cipher data is again XORed with same key stream to obtain original plain text. Detail

IV. Proposed Technique

The graphical model of proposed generator is depicted in “Fig. 1”which shows that initial inputs to FCSRs are given, which generate sequences. The Generated sequence than produce key stream. Data from database is retrieved which is first converted to binary form and than encrypted with generated key stream.

A. Operational scenerio of proposed model

In this section we discuss the detail operation of our proposed generator .Initially before starting the process of key stream generation for each FCSR we should determine connection polynomial ***q***, size of register ***r*** and additional memory ***m.*** After that ***r*** cells of FCSRs are initialized with binary data.

1. Each FCSR process following steps:
   - Calculate $\sum_{k=1}^{\sigma n = r} q_k a_{n-k} + m_{n-1}$.
   - Output the rightmost bit a_{n-r} and all cells shift one step right.
   - Shift parity bit of σ_n (mod 2) in to leftmost cell and high order bit σ_n (div 2) in to carry cell.
2. Sequence of first FCSR is shrunken with self shrinking generator as follows:
   - Triple-bit ($a_{3i,}a_{3i+1},a_{3i+2}$) of first FCSR are taken at a time if ($a_{3i\ \mathrm{XOR}}\ a_{3i+1==1}$) than output becomes a_{3i+2} otherwise discard 3 bits .
3. Take shrunken sequence of FCSR as clock sequence and use to control other two base FCSRs sequences.
4. At each clock cycle output of two base sequences is added in to full addition function along with carry register. Output key stream is calculated as Z(mod2) and Carry register retained a new value Z (div2).
5. Output key stream is XORed with plain text bit to produce cipher text.
6. Plain text can be degenerate by XORing Cipher text with same keystream.

B. Algorithm:

Pseudo code of proposed model is

1) Algorithm: Input to connection number:

```
q=convert.Toint32 (q1text.Text)
FCSR_size =(int)(log2(q))
```

2) Algorithm: Input to FCSRs:

```
F1=R1.Text
```

3) Algorithm: Sequence Generation

```
SET seq=F1[0].ToString();
FOR i=initialR1.Length-1 TO 1
IF q[i] =1
SET sum+=F1[i];
END IF
ELSE
SET sum=0;
END ELSE
FOR temp=initialR1.Length-1 TO 1
F1 [temp]=F1[temp-1]
END FOR
```

```
        Sum=sum +m
        SET F1 [0] = mod (sum,2)
        m=div (sum, 2)
        END FOR
        DISPLAY seq;
```

4) // Algorithm: key Generation

a) SSG operation

```
        FOR i=0 TO SSG.Length-1
        b=a[3i]^a[3i+1]
        IF b=1
        Buffer[i]=a[3i+2]
```

b) ASG operation

```
        FOR j=0 TO buffer.Length-1
        DISPLAY Keystream
        IF buffer[j]=1
        Sum=R3prev+buffer[j]+carry
        END IF
        ELSE
        Sum=R2prev+buffer[j]+carry
        END ELSE
        Sum=mod(sum,2)
        Carry=div(sum,2)
        Keystream[i]=sum;
        END FOR
```

First input is given to connection integer which must be negative prime number then size of FCSR is calculated with connection integer. Initial value are given to each FCSR and with each FCSR we generate a unique sequence .

First FCSR behave like self shrinking generator and remaining two FCSRs act like alternating step generator. Output of these two FCSRs are combined with addition function.

V. Experiment Results and Analysis

A. *Probability of finding initial states:*

We can find the probability of success for finding correct initial values of registers R2 and R3 if addition modulo 2 is used as combined function as [4].

$$P = \frac{1}{2^{r2} + 2^{r3}} \qquad (1)$$

Here r2 and r3 are length of shift registers R1 and R2.

If full addition function is used as combination function then probability of success for initial states is determined as:

$$Padd = \frac{1}{2^{r2} + 2^{r3} + c1^{k1}} \qquad (2)$$

K1 is initial value of carry register of full adder function.

TABLE I. COMPARISON OF PROBABILITIES OF DIFFERENT GENERATORS

Generator	Probability
ASG	$Pasg = \frac{1}{2^{r2} + 2^{r3}}$
ASSG	$Passg = \frac{1}{2^{r2} + 2^{r3}}$
Proposed Generator	$Ppg = \frac{1}{2^{r2} + 2^{r3} + c1^{k1} + c1^{k2} + c1^{k3}}$

We have

$Ppg < pasg$ and $Ppg < Passg$

According to "Table 1" the structure of proposed generator is more secure than ASSG and SG because due to carry propagations it is difficult to estimate the right initial states of registers.

B. *Graphical comparison ofprobabilty of proposed model with other models:*

Case 1:

In case 1we compare the probabilities of success of finding right initial values of alternating step base registers.

For example by giving values 9 and 11 to ASG and ASSG registers r2 and r3 respectively we calculate probability as:

$$Pasg = Passg = \frac{1}{2^9 + 2^{11}} = 0.00039 \qquad (3)$$

Given values to proposed generator registers r2 r3 are 9 and 11.values to clock control sequence initial values of carry registers 1,2,3 are 7,1,2,3 respectively. then probability of Proposed generator(Ppg) becomes

$$Ppg = \frac{1}{2^9 + 2^{11} + 7^1 + 7^2 + 7^3} = 0.00037 \qquad (4)$$

So that Probability of finding right initial states is low in proposed model then other models as shown in "Fig 2" and its difficult to find initial states of registers .

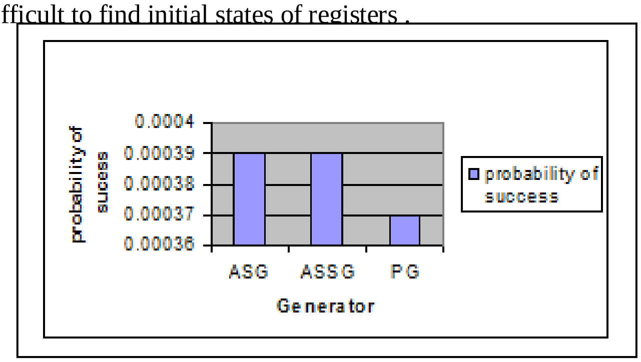

Figure 2: Case1: probability of success to find initial states

Case 2:

In case 2, we compare the probabilities of success of finding right initial values of alternating step base registers

For example, by giving values 3 and 5 to ASG and ASSG registers r2 and r3 respectively we calculate probability as:

$$Pasg = Passg = \frac{1}{2^3 + 2^5} = 0.025 \qquad (5)$$

Given values to proposed generator registers r2 r3 are 3 and 5.values to clock control sequence initial values of carry registers 1, 2, 3 are 5,1,2,0 respectively. Then probability becomes

$$Ppg = \frac{1}{2^3 + 2^5 + 5^0 + 5^1 + 5^2} = 0.0140 \qquad (6)$$

So that Probability of finding right initial states is low in proposed model then other models as shown in “Fig 3” ” and its difficult to find initial states of registers .

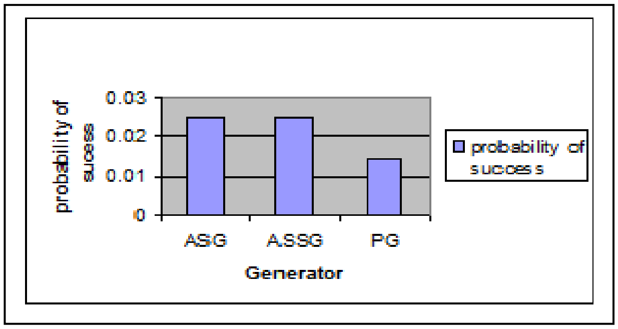

Figure 3: Case 2:probability of success to find initial states

C. *Comparison of proposed generator with other generators:*

Comparison of properties of proposed model with other models is shown in “Table 2”.

TABLE II. COMPARISON OF PROPOSED MODEL WITH OTHER MODELS

Properties	**SSG**	**ASG**	**SSG**	**Proposed generator**
Register type	LFSRs	LFSRs	LFSRs	FCSRs
number of registers	1	3	4	3
Logic gates	-	And ,Not	-	-
Combination function	-	XOR	XOR	Full adder, OR
structure	simple	complex	complex	complex
period	$(2^{L1-1}-1)$	$2^{L1}(2^{L2}-1)(2^{L3}-1)$	$2^{L1}(2^{L2}-1)(2^{L3}-1)(2^{L4}-1)$	(|q1|-1)/3(|q2|-1)(|q3|-1)

After comparing proposed generator with other generators it is found that proposed generator use FCSRs and full addition function which make structure highly non linear, so that proposed model is highly resistant to linear attacks as compared to other generators which uses LFSRs. Period of ASG and SSG is less than proposed generator while period of ASSG is greater because number of registers used in proposed generator less than ASSG registers which increase period of ASSG. Unless the period of proposed generator is less than ASSG it becomes more secure against attacks due to its non linearity [6].

VI. Conclusion

In this paper, we propose a model of keystream generator which is based on FCSRs and combine the features of both SSG and ASG to remove pitfalls that may occurs when these generators used individually. The description of proposed models and necessary conditions for model is well elaborated .The proposed model consists of 3 FCSRs which combine in such a way 1st FCSR used as clock sequence which controls the other 2 base FCSRs. Full addition function is used to combine the output of base registers.

Use of FCSRs, addition modulo2function and full addition function increase non linearity of proposed generator and make it more secure and highly resistant to external attacks .Next the comparison of proposed generator with other generators shows that it’s become a good choice because it is difficult to predict the right initial states of registers due to carry propagations in structure.

References

[1] A. Rueppel, Analysis and Design of stream ciphers. Springer-Verlag,1986.

[2] Arnault, F., Berger, T.” F-FCSR: design of a new class of stream ciphers,” Lecture notes in computer sciences, vol. 3557, pp. 83–97. Springer, Heidelberg 2005.

[3] A.Kenso, “Modified self-shrinking generator,” Journal of Computers

[4] and Electrical Engineering vol 36, pp. 993–1001, 2010.

[5] S.Shun-lung , Ko-ming Chiu, , and Lih-chyau Wuu, “The Cryptanalysis of LFSR/FCSR Based Alternating Step Generator,” International conference on Computer Engineering and systems, pp. 228–231, 2006 .

[6] A. Klapper and M. Goresky,”Feedback shift registers, 2-adic span, and combiners with memory,”Journal of Cryptology, vol 10,pp.11–147, 1997.

[7] Lihua Dong, Yong Zeng, Yupu Hu, "F-GSS: A Novel FCSR-Based Keystream Generator," , First International Conference on Information Science and Engineering, pp.1737-1740, 2009.

[8] Ghosia Arshad “Analysis and design of alternating step shrinking generator ”,IJCTE,in press.

[9] Yong Zeng, Ma Jianfeng , Pei Qinqi, Dong Lihua “A Hardware-Oriented Fast Encryption Keystream Generator for Digital Rights Management”,International Conference on Computational Intelligence and Security,vol 02,pp. 584 – 586,2009

Author’s Profile

Hafsa Rafiq is a graduate from Dept. of Software Engineering, Fatima Jinnah Women University, Pakistan.

Dr. 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. 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.

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