Analysis of Guess and Determined Attack on Non Linear Modified SNOW 2.0 Using One LFSR

Madiha Waris [#1], Malik Sikandar Hayat Khiyal[#2] , Aihab Khan [#3]
Department of Software Engineering Fatima Jinnah Women University, Old Presidency, The Mall, Rawalpindi, Pakistan

***Abstract*—stream ciphers encrypt the data bit by bit. In this research a new model of stream cipher SNOW 2.0 has been proposed i.e. Non linear modified SNOW 2.0 using one Linear Feedback Shift Register (LFSR) with the embedding of non linear function in the model. The analysis of Guess and Determined (GD) attack has been done to check its security with respect to previous versions. The proposed model contains one Linear Feedback Shift Register (LFSR) along with the non linear function which increases the strength of the stream cipher, to make the static nature of modified SNOW 2.0 dynamic. The Experimental analysis show that such a mechanism has been built which provides more security than the previous version of modified SNOW 2.0 in which non linearity was either not introduced or it was introduced using two Linear Feedback Shift Registers (LFSRs). It is concluded that this version is more powerful with respect to the security of plain text against Guess and Determined attack (GD) as compared to the previous versions.**

Keywords-component; Linear Feedback Shift Register; Guess and Determined Attack; Finite State Machine .

I. INTRODUCTION

A stream cipher is a cryptographic way to achieve the confidentiality on communication channel [1]. They are broadly used for the provision of security for communication and in network streams.

Linear Feedback Shift Register (LFSR) is the frequently used device as key stream generator. It is mostly used in many key stream generators due to its simplicity. The SNOW family is a typical example of word oriented stream cipher, based on Linear Feedback Shift Register [2].

The initial version of SNOW was presented to NESSIE project in 2000, which wasn't accepted due to the weaknesses present in it against the Guess and Determined (GD) attack. Then the new version SNOW 1.0 was developed by Thomas Johansson and Patrik Ekdahl and it was also discarded due to Guess and Determined (GD) attack. Then these authors presented a new version SNOW 2.0 which was the modified version of SNOW 1.0 with the enhancement of features for secure communication. It was claimed to solve the weaknesses and improvement of the performance. Later on a Modified version of SNOW 2.0 was built by Hadi Ahmadi which was static in nature and it was also less secure against the Guess and Determined (GD) attack [3].

In this paper, the static feedback based modified SNOW 2.0 has been converted into dynamic feedback based modified SNOW 2.0 by using one Linear Feedback Shift Register (LFSR) and with the addition of non linear function which enhances the security performance of the model by using irregular clocking. This will increase the complexity for the attacker to guess the input. The proposed model of Non linear SNOW 2.0 with one Linear Feedback Shift Register (LFSR) is checked for security against Guess and Determined (GD) attack and by experimental analysis it is observed that it is more secure.

The paper is organized in such a way that: section 2 discusses related work to proposed schemes, section 3 demonstrates the proposed framework, section 4 discusses proposed technique along with algorithm ,section 5 discusses analysis of proposed technique, section 6 describes the experimental results and at the end the conclusion is given in section 7.

II. RELATED WORK

Ahmadi and Salehani et al. [3] proposed a Modified Version of SNOW 2.0. He gave a criterion of modifying an LFSR-based stream cipher against Guess and Determined (GD) attacks. In this model a stream of pseudorandom digits in a synchronous stream cipher was independent of the plaintext and cipher text messages, and then combined with the plaintext for encryption or with the cipher text for decryption. IrfanUllah and Naz et al. [4] proposed a model of SNOW 2.0 and claimed that it contained a series of patterns of bits that were traceable. Two versions SNOW 1.0 and SNOW 2.0 were examined and concluded that if the plaintext that has to be encrypted is of small amount, modified Version of SNOW 2.0 should be used and if large data set has to be encrypted original snow 2.0 should be recommended. Khan et al. [2] proposed the model of dynamic feedback based modified SNOW 2.0 and compared the dynamic nature of modified SNOW 2.0 with the previous version of modified SNOW 2.0 that was static in nature. Also compared them on the basis of Guess and Determined (GD) attack and concluded that Dynamic Feedback based Modified SNOW 2.0 is more secure than static feedback based modified SNOW 2.0 for the encryption of plain text. Masood et al. [5] proposed the model for analysis of non linear Snow 2.0 for improved security and did it by embedding a non linear function using two Linear Feedback Shift Registers (LFSRs) in dynamic feedback based modified SNOW 2.0.

In this technique the linear behavior of static feedback based modified SNOW 2.0 has been converted to non linear behavior by introducing non linear function based on irregular clocking. For this the feedback change accepts values at

dynamic tap positions rather than static so its structure is considered as dynamic and non linear and it was found that this dynamic feedback mechanism for Linear Feedback Shift Register (LFSR) and nonlinear behavior was an effective method to improve the security of SNOW 2.0 and hence it resulted in increased complexity for attacker to guess the input.

III. PROPOSED FRAMEWORK

The proposed model comprises dynamic feedback based modified SNOW 2.0 with one Linear Feedback Shift Register (LFSR) along with the non linear function. For security provision in stream ciphers dynamic feedback mechanism is the best way as it changes a deterministic linear recurrence of some registers into probabilistic recurrence [2]. Due to this characteristic the stream cipher having dynamic feedback control mechanism remain protected against various attacks.

The attacker has to guess the some inputs to the non linear function for which he has to obtain a linear recurrence of the key stream. The irregular modification makes it impossible for the attacker to find the linear recurrence of the key stream obtained by some registers. In this way the security enhances.

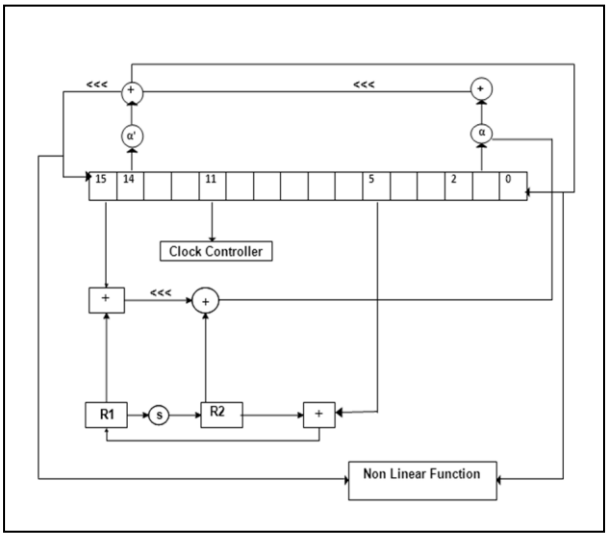

Figure 1. Proposed Model for Non linear Modified SNOW 2.0 with one LFSR

The Proposed model as shown in "Fig. 1"is constructed in such a way that it consists of one Linear Feedback Shift Register (LFSR), Finite State Machine (FSM) and a Non linear function having a dynamic feedback controller and two internal registers M1 and M2.

A. Symbols Specification of the Proposed Model

R1= 32 bit Register $\oplus$ = bit wise XOR

R2= 32 bit Register S= S-box

<<<= cyclic shift 7 steps left $\boxplus$ =addition modulo 2^{32}

B. Non linear function for proposed non linear SNOW 2.0.

The non-linear function of proposed model as shown in "Fig. 2" is fed the values of four of the tap positions of Linear Feedback Shift Register (LFSR) that are dynamically taken into R1, R2, L1, and L2 which are internal memories and outputs 64 bits of key-stream for every cycle.

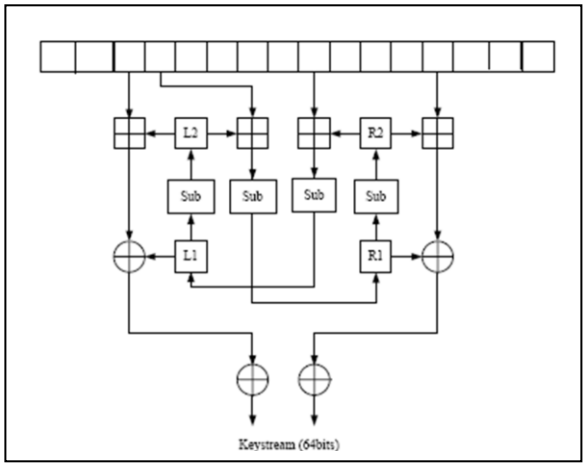

Figure 2. Nonlinear function model description using one LFSR.

IV. PROPOSED TECHNIQUE

A. Working Scenerio of the Proposed Model

The working of the proposed model is described in detail in this section. The whole process continues in such a way that:

1. At first the key initialization is done in order to initialize LFSR. The registers R1 and R2 of the Finite State Machine (FSM) are set to zero.
2. In the next step, the cipher clocks 32 times without producing any output and the FSM output is fed back into the Linear Feedback Shift Register (LFSR).
3. The steps for the proper working of cipher are as follows:
   - $tempf_t = S_{t+15} \boxplus R1_t$
   - Left shift circular $S_{t+15} \boxplus R1_t$, and then Xor it with R_2.
   - $tempf_t = (S_{t+15} \boxplus R1_t) <<< 7$
   - $f_t = tempf_t \oplus R2_t$; when $t \geq 0$
4. The non linear function is implemented in such a way that at first initial vector (IV) values are initialized and a key is loaded. The dynamic tap positions are taken and the whole process continues as follows:
   - $f_{t1} = temp \oplus R3_t$; when $t \geq 0$
   - keystream 1= $f_{t1} \oplus$ dynamic no.
   - $f_{t2} = temp1 \oplus L_2$
   - keystream 2= $f_{t2} \oplus$ dynamic no.
5. The final keystream is determined as follows:
   Final keystream = keystream 1 $\oplus$ keystream 2
6. The next state of Finite State Machine (FSM) registers is determined as follows:

- $R1_{t+1} = S_{t+5} \boxplus R2_t$ and
- $R2_{t+1} = S(R1_t)$ $t \geq 0$

7. The next state of Linear Feedback Shift Register (LFSR) is determined as follows:
   $S_{16} = ((\alpha^{-1} S_{t+11}) <<<,7) \oplus S_{t+2} \oplus ((\alpha S_t) <<<, 7)$

B. Graphical Representation of the Proposed Model

The graphical model of the Non linear modified SNOW 2.0 using one Linear Feedback Shift Register (LFSR) is shown in "Fig. 3". It depicts the flow of the whole process. At first the dynamic number generator will generate dynamic numbers which will be fed to the shift registers.

The values form the shift registers will be then given to the clock-controller and the values of shift registers will be updated. The updated values will then be fed to the non linear function which will generate key stream.

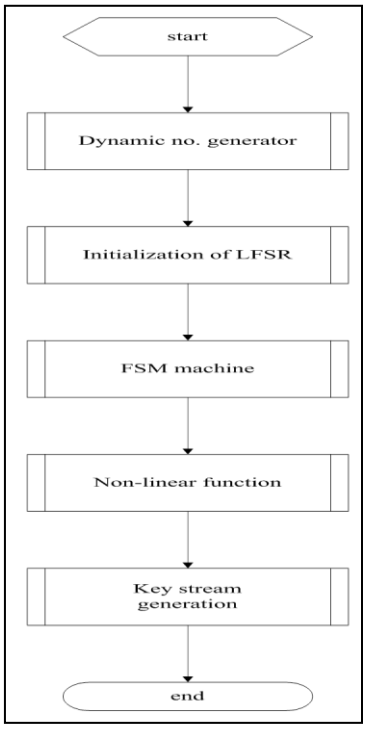

Figure 3. Graphical Model for Non linear Modified SNOW 2.0 with one LFSR

C. Algorithm of the Proposed Technique

1) Algorithm: Generation of Dynamic numbers

Input: Time

Output: srand

Read time.

srand= srand (time(NULL))

srand= return (rand()%16+1)

output srand.

2) Algorithm: Shift Registers

Input: IV values

Output: Keystream

Read initial values

ptemp = snow r1+*(snow_ptr+15)

ptemp1= ptemp<<7

snow_outfrom_fsm=ptemp^snow_r2

Output keystream.

3) Algorithm: Clocking

Input: FSM output

Output: no output

Read snow_outfrom_fsm

Update Interanls

No output.

4) Algorithm: Non linear Function

Input: Four numbers generated dynamically

Output: keystream

Read dynamic numbers

Add them to internal memories

Xor the resultant values with dynamic numbers

output keystream.

V. Analysis of Proposed Technique

The performance of proposed technique can be analyzed by the help of attack. Guess and Determined (GD) attack has been done on the proposed technique in order to measure its security position.

Guess and determined (GD) attacks have been affecting some stream ciphers. In this attack, the attacker judges the correlation between the cipher's building blocks [6].

In this attack the attacker at first guesses the initial states of the cipher, which is known as a basis. Then he finds the running key sequence. If his sequence matches the original key sequence it means that he has guessed the original key stream and if it does not match then he tries again to guess with new initial values and key until he finds the original key stream.

This process is based on the fact that, the attack complexity will be less if the basis size is small [7]. Due to presence of the nonlinear function, it is not possible for the attacker to guess the correct values.

The Guess and Determined (GD) attack occurs in the sequence as follows [8]:

a) The attacker guesses initial values for the Finite State Machine (FSM)

b) The attacker guesses the values for registers

c) The values obtained from registers are used by the attacker to guess the Linear Feedback Shift Register (LFSR) state.

d) The attacker generates a key stream and tests the values of Linear Feedback Shift Register (LFSR) and Finite State Machine (FSM) state and then he compares the produced key stream with the original key stream.

In the proposed system the attack is applied in this way that at first the initial values and secret key is guessed. Then the key is converted into binary form. This binary format is then converted into 32 bit format. Then key stream is determined with the help of this secret key initialization. At the end this key stream is compared with the original key stream.

VI. Experiment results and Analysis

The Guess and Determined (GD) attack has been applied on the proposed model and on the previous versions also to check the security standard of the proposed version. The comparison algorithm has been applied to compare the key streams generated with the guessed key streams. It works in such a way that the result is "1" if the key stream matches and it results "0" if the key stream is not matched.

Following are the two phases in which the results have been examined.

A. Analysis of Phase I

In order to determine the original key stream on basis of guess, 30 experiments have been performed in Phase I. 10 experiments are performed on each of Non linear Modified SNOW 2.0 using one Linear Feedback Shift Register (LFSR), Dynamic feedback based modified snow 2.0 using non-linear function, dynamic feedback based modified snow 2.0 and static feedback based modified snow 2.0. 1 attack is applied on each experiment and each attack has 10 guesses.

One attack generates 50 guess key streams; mean 10 attacks generate 500 key streams. Hence, 30 experiments have 1500 guesses in total.

Experimental analysis show that the proposed model show more resistance to Guess and Determined (GD) attack as compared to the previous versions. Results of the Phase I are shown in "Table I".

TABLE I. Evaluation of Phase I

Experiments	Non linear SNOW 2.0 using one LFSR	Non linear SNOW 2.0 using 2 LFSRs	Dynamic feedback based modified SNOW 2.0	Static feedback based modified SNOW 2.0
	Similarities	**Similarities**	**Similarities**	**Similarities**
1	375	381	397	406
2	351	345	400	410
3	405	409	439	456
4	357	357	434	466
5	382	380	409	471
6	360	364	392	495
7	404	407	420	452
8	372	390	376	415
9	387	396	456	442
10	363	363	456	404
Total	3756	3792	4179	4417

According to "Table I" the Non linear SNOW 2.0 using one Linear Feedback Shift Register (LFSR) is more secure as compared to the other defined versions of SNOW 2.0.

The graphical representation of Phase I is shown in "Figure 4".

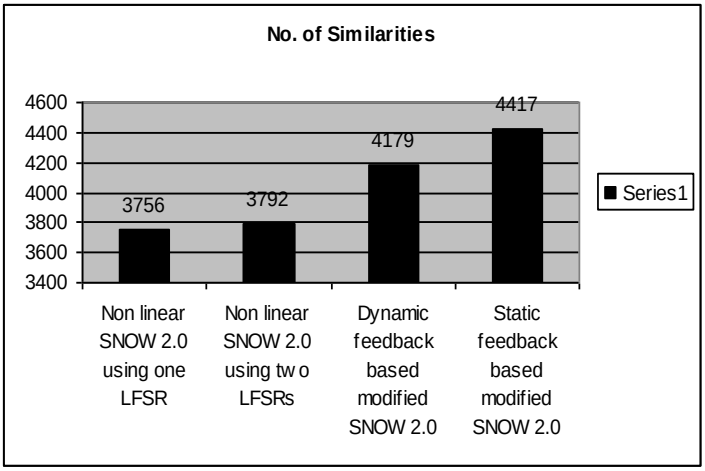

Figure 4. Graphical Representation of Phase I

B. Analysis of Phase II

In Phase II, 30 experiments have been performed for the analysis of key streams, each experiment has 10 attacks and each attack has 50 key streams. Similar to Phase I, 10 experiments contains 500 guesses.

10 experiments are performed on each of Non linear Modified SNOW 2.0 using one Linear Feedback Shift Register (LFSR), dynamic feedback based modified snow 2.0 using non-linear function, dynamic feedback based modified snow 2.0 and static feedback based modified snow 2.0. The only difference from Phase I is that, in this phase 40 key streams have been generated against each guess. As the number of key streams increase, the number of comparisons also increases.

Experimental analysis show that the proposed model show more resistance to Guess and Determined (GD) attack in Phase II as compared to the previous versions. Results of the Phase II are shown in "Table II".

TABLE II. EVALUATION OF PHASE II

Experiments	Non linear SNOW 2.0 using one LFSR	Non linear SNOW 2.0 using 2 LFSRs	Dynamic feedback based modified SNOW 2.0	Static feedback based modified SNOW 2.0
	Similarities	**Similarities**	**Similarities**	**Similarities**
1	818	840	863	851
2	759	816	854	825
3	780	728	803	830
4	807	827	84	938
5	751	822	867	907
6	762	810	859	943
7	814	830	864	903
8	783	798	874	901
9	733	736	789	934
10	750	806	865	934
Total	7757	8013	8512	8966

According to "Table II" the Non linear SNOW 2.0 using one LFSR is more secure as compared to the other defined versions of SNOW 2.0. The graphical representation of Phase I is shown in "Figure 4".

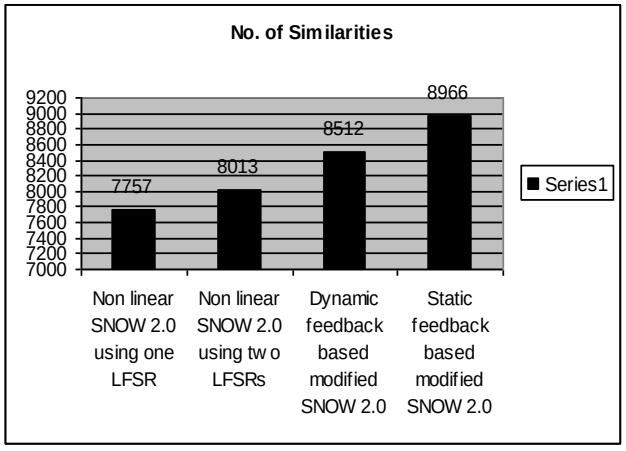

Figure 5. Graphical Representtion of Phase II

VII. CONCLUSION

In this paper the Guess and Determined (GD) attack has been applied on Non linear modified SNOW 2.0 using one Linear Feedback Shift Register (LFSR). The results concluded from Phase I and Phase II by comparison algorithm show that the proposed technique is more powerful with respect to security as compared to Non linear SNOW 2.0 using two Linear Feedback Shift Registers (LFSRs), Dynamic feedback based modified SNOW 2.0 and Static feedback based modified SNOW 2.0. The use of non linear function with one LFSR is a more reliable method with the reduction of complexity as compared to previous versions of SNOW 2.0.

REFRENCES

[1] P. Ekdahl, T. Johansson, *"A new version of the stream cipher SNOW"*, Proceedings of Selected Areas in Cryptography (SAC) 2002, Volume 2595 of LNCS, pages 47-61, Springer, 2002.

[2] Saira Khan, Aihab Khan, Malik Sikandar Hayat Khiyal, Tarranum Baz "Dynamic Feedback based Modified SNOW 2.0" IEEE International Conference on Emerging Technologies 2010 (ICET 2010), October 18-19, 2010, Islamabad, Pakistan.

[3] Ahmadi H., Esmaeili Salehani Y., "A Modified Version of SNOW2.0", International CSI Computer Conference, 2007

[4] Syed IrfanUllah, Tarannum Naz and Sikandar Hayat Khiyal " Traceable Bit Streams in SNOW 2.0 using Guess-and-Determine Attack" World Applied Sciences Journal, Volume 11, No. 2, pp 190-195, 2010.

[5] Mina Masood, Aihab Khan, Malik Sikandar Hayat Khiyal, Ghoosia Arshad " Analysis and Design of Non-Linear SNOW 2.0 for improved security" International Journal of Computer Technology and Engineering. (Submitted)

[6] Rohani, N.; Noferesti, Z.; Mohajeri, J.; Aref, M.R.; , "Guess and Determine Attack on Trivium Family," Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference, pp.785-790, 11-13 Dec. 2010

[7] Ahmadi, H.; Eghlidos, T.; , "Heuristic guess-and-determine attacks on stream ciphers," Jounal of IET- Information Security, Institute of Engineering and Technology, vol.3, Issue. no.2, pp.66-73, June 2009

[8] P. Hawkes and G. G. Rose. Guess-and-determine attacks on SNOW. In K. Nyberg and H. Heys, editors, *Selected Areas in Cryptography*- SAC 2002, volume 2595 of *Lecture Notes in Computer Science*, pages 37-46. Springer Verlag, 2002.

AUTHOR'S PROFILE

Madiha Waris 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. He was also involved at teaching in Computer Training Center, 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 Associate editor of IJCTE, and International Journal of Reviews in Computing. He is reviewer of the journals, IJCSIT, JIISIT, IJCEE, JCIE and CEE of Elsevier.

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.