Analysis and Design of Non Linear Snow 2.0 for Improved Security

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

Abstract—**In this paper, we propose a stream cipher; non-linear snow 2.0 by embedding non-linear function in dynamic feedback based modified snow 2.0 along with analysis of Guess and Determine (GD) Attack. The proposed non linear snow 2.0 uses two linear feedback shift registers (LFSR) in addition to the non-linear function to make the static nature of modified snow 2.0 dynamic. In non linear snow 2.0, the feed back change accepts values at dynamic tap positions rather than static so its structure is considered as dynamic and non linear. Experimental results show that proposed non-linear snow 2.0 has more resistance against guess and determine attack as compare to dynamic feedback based modified snow 2.0 without non-linear function and static feedback based modified snow 2.0. We conclude that for the encryption of plaintext non-linear snow 2.0 is more secure against guess and determine attack.**

Index Terms—**Dynamic feedback, guess and determine attack, linear feed back shift register (LFSR), modified SNOW 2.0, non-linear function, non-linear snow 2.0.**

I. Introduction

The Initial version of snow appeared in 2000 but number of weaknesses were identified due to which it could not pass the NESSIE test [3,6]. Modified versions of snow were presented by researchers to overcome these weaknesses. [1] Snow is a word oriented stream cipher based on linear feedback shift register with static nature. The use of static values may leave the peepholes for cryptanalysts therefore use of dynamic values may fill these peepholes and increase the security. [4,9] The versions of snow presented in literature are static in nature with regular clocking which results in low security [4,9].

The research presented in this paper converts static feedback based modified snow 2.0 into dynamic feedback based modified snow 2.0 by using two LFSRs. Also the linear behavior of static feedback based modified snow 2.0 is converted to nonlinear behavior by introducing non linear function based on irregular clocking. This dynamic feedback mechanism for LFSR and nonlinear behavior is an effective method to improve the security of snow 2.0 and results in increased complexity for attacker to guess the input. The proposed non linear snow 2.0 is evaluated againstguess and determines attack and experimental analysis shows increased security and performance.

The organization of paper is as follows:

Section II depicts the analysis of modified SNOW 2.0. Section III gives description of dynamic feedback. In section IV analysis of guess and determine attack is presented. Section V provides experimental analysis. Section VI discusses results. Section VII gives conclusion and at the end section VII gives the future work

II. Related Work

Ahmadi et al [1] proposed a Modified Version of snow 2.0 in which a stream of pseudorandom digits in a synchronous stream cipher is independent of the plaintext and cipher text messages, and then combined with the plaintext for encryption or with the cipher text for decryption. A class of stream ciphers whose cryptographic operations are applied on sets of w-bit strings called word, over Galois Field (GF) is called word-oriented stream ciphers. Some of these ciphers are based on a linear part that is an LFSR and a non-linear part also called NLF. SNOW 1.0 and SNOW 2.0 are two word-oriented LFSR-based synchronous stream ciphers developed by Thomas Johansson and Patrik Ekdahl. [2] Safdar. et al [8] implemented alternating step generator and shrinking generator and found that shrinking generator is secure at length of 64 and alternating step generator is secure at the length of 128 so shrinking generator is more efficient and secure than alternating step generator. This research attempt to provide solution to correlation attack by gradually increasing the lengths of initial input bits of linear feedback shift registers which result in increase of key length. Naz et al. [4,9] analyze the effect of guess and determine attack on snow 2.0 and modified version of snow 2.0 and verify 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. Saira et al. [5,10] analyze guess and determine attack against static and dynamic structure of snow 2.0 and compare its effect on dynamic feedback based modified snow 2.0 and static feedback based modified snow 2.0. As a result of the experimental work and analysis, it is concluded that, for the encryption of plaintext dynamic feedback based modified Version of snow 2.0 should be used. Dynamic feedback based modified snow is more secure and reliable for a secure communication as compare to static feedback based modified snow 2.0.

III. Proposed Framework

The main idea behind the proposed model shown in fig 1 is embedding of dynamic structure in modified snow 2.0

Manuscript received December 6, 2010; revised June, 22, 2011.

Mina Masood, Malik Sikandar Hayat Khiyal, and Ghoosia Arshad are with Department of Computer Science, Fatima Jinnah Women University, Rawalpindi, Pakistan (e-mail:menotee@yahoo.com, m.sikandarhayat@yahoo.com, ghoosia_arshad22@yahoo.com).

Aihab Khan is with Department of Computing and Technology, Iqra University, Islamabad, Pakistan (E-mail:aihabkhan@yahoo.com).

presented in [5,10]. A dynamic feedback control for linear feedback shift register is effective method to improve security of stream ciphers. The dynamic feedback control mechanism improves the security of a stream cipher because it changes a deterministic linear recurrence of some registers into probabilistic recurrence. This property efficiently protects against numerous attacks. An attacker has to obtain a linear recurrence of the key stream derived from the linear recurrence of some registers. By irregular modification, the linear recurrence exists with a low probability. An attacker has to guess some inputs to the non-linear function for some attacks; however irregular modification makes it impossible. The attacker has to guess the inputs to the dynamic feedback controller first. Thus, irregular modification of the feedback function improves the security of the stream cipher.

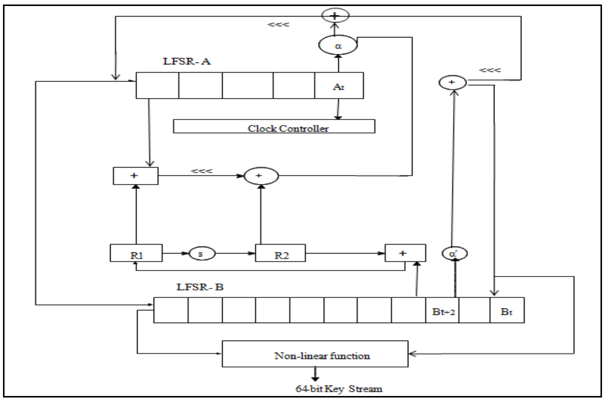

Fig. 1.Proposed model of non linear snow 2.0

The proposed model consists of two linear feedback shift registers (LFSRs), LFSR-A and LFSR-B, a non-linear function with two internal registers M1 and M2, and a dynamic feedback controller. The size of each register is 32 bits. LFSR-A has five tap positions, and LFSR-B has 11 tap positions, also greatest common divisor (GCD) of 5 and 11 is 1 which increases security of stream cipher.

A. *Non-linear function of proposed non linear snow 2.0*

The non-linear function shown in fig 1 is elaborated in fig [2].

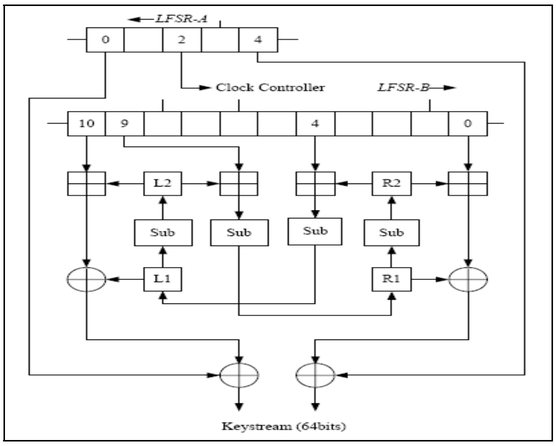

Fig. 2.Model of non-linear function [7]

The non-linear function of proposed model fed the values of two tap positions of LFSR-A and four tap positions of LFSR-B and that of internal memories R1, R2, L1, L2, and outputs 64 bits of key-stream for every cycle.

IV. Proposed Technique

The graphical model of the Non-linear snow 2.0 is shown in fig 3. Dynamic number generator generates dynamic numbers which are fed to the shift registers. The values from the shift registers are then given to the clock-controller and the values of shift registers are updated by updation function. These updated values are fed to the non-linear function which generates 64-bit key stream.

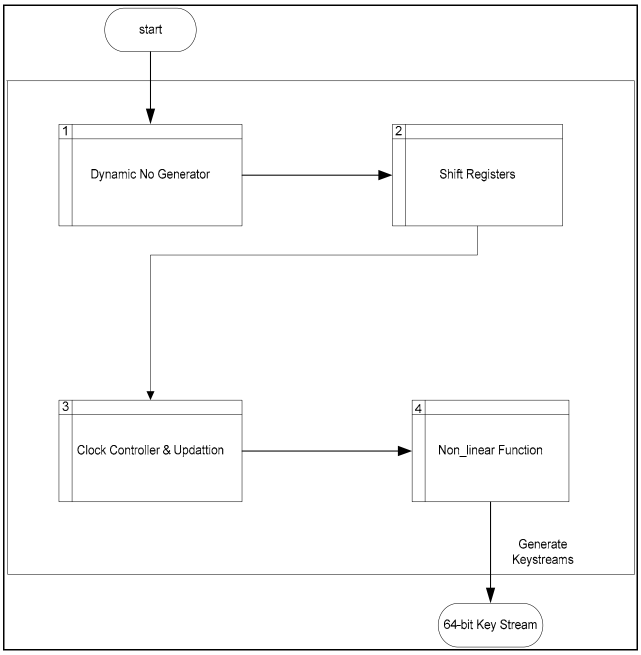

Fig. 3.Graphical model of non linear snow 2.0

The algorithms used in fig 3 are elaborated as follows :

Algorithm: Dynamic no. generator
Input: Time
Output: srand
Read time.
srand= srand(time(NULL))
srand= return(rand()%16+1
output srand.
Algorithm: Shift registers
Input: Initial vector values
Output: Keystream
Read Initial values.
Ptemp=snow_r1+*(snow_ptr+15)
Ptemp1=ptemp<<7
Snow_outfrom_fsm=ptemp1^snow_r2
Output keystream
Algorithm Clocking
Input: Output generated from fsm
Output: nothing
Read snow_outfrom_fsm.
Update internals.
Output nothing
Algorithm: **N**on-linear-function
Input: Dynamic numbers
Output: 64-bit keystream
Read dynamic numbers.
Add internal memories to the dynamic numbers
Xor resultant values with the dynamic numbers
Generates 64-bit keystream.

V. Experimental Results

Guess and determine attack is applied on proposed Non-linear snow 2.0 and previous versions like static feedback based modified snow 2.0 and dynamic feedback based modified snow 2.0. Guess and determine attack work in such a way that the guess has been made on secret key and initialization values, which are used to initialize the LFSR and FSM's registers. By using these guesses, attacking key streams is generated and these key streams will be compared with the key streams generated by non-linear snow 2.0, dynamic feedback based modified snow 2.0 and static feedback based modified snow 2.0. The complete attack analysis includes two phases. For comparison of key stream, comparison algorithm is used which compare all the key stream of modified snow 2.0 with attacking key stream. Comparison algorithm work in such a way that index compare the key stream of original with attacking key stream, if similar represent it by one otherwise zero will be stored in table.

A. Evaluation of Phase I

TABLE I: Evaluation of Phase I

Experi ments	Non-linear snow 2.0	Dynamic feedback based modified snow 2.0	Static feedback based modified snow 2.0
	Similarities	Similarities	Similarities
1	381	397	406
2	345	400	410
3	409	439	456
4	357	434	466
5	380	409	471
6	364	392	495
7	407	420	452
8	390	376	415
9	396	456	442
10	363	456	404
Total	3792	4179	4417

In Phase I, 30 experiments are performed. Each experiment has 10 attacks, thus 30 experiments have 300 attacks. One attack generates 50 key streams hence 30 attacks will generate 15000 key streams. The experimental results show that, we cater 3792 similarities in non-linear snow 2.0, 4179 similarities in dynamic feedback based modified snow 2.0 without non-linear function and 4417 similarities in static feedback based modified snow 2.0. These results shows that static feedback based modified snow 2.0 and dynamic feedback based modified snow 2.0 has been more affected by guess and determine attack as compare to non-linear snow 2.0. The average percentage of attack on non-linear snow 2.0, dynamic feedback based modified snow 2.0 and static feedback based modified snow 2.0 is 4.74, 5.223 and 5.515 respectively. It is obvious that non-linear snow 2.0 has low average percentage which means non-linear snow 2.0 has more resistance against Guess and Determine attack. Results of experiments are shown in table 1.

Fig 4 shows graphical representation of the result presented in table 1.

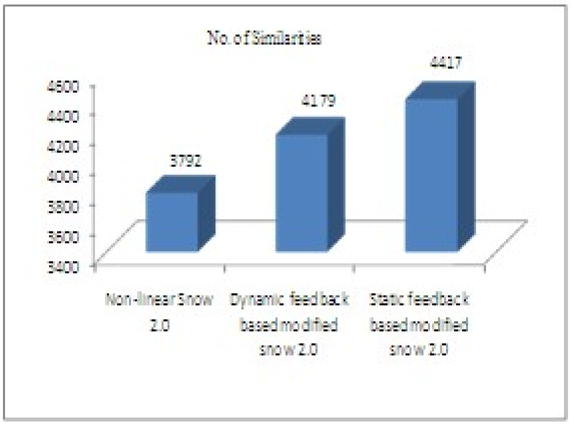

Fig. 4.Graphical representation of phase I

The results presented in table 2 and fig 5 shows the average percentage of attacks in phase 1.

TABLE II: Tabular representation for average percentage of attacks in Phase I

Experi ments	Non-line ar snow 2.0	Dynamic feedback based modified snow 2.0	Static feedback based modified snow 2.0
	%age	%age	%age
1	4.7625	4.9625	5.07
2	4.3125	5	5.12
3	5.1125	5.48	5.7
4	4.4625	5.425	5.8
5	4.75	5.1125	5.88
6	4.55	4.9	6.18
7	5.0875	5.25	5.65
8	4.875	4.7	5.18
9	4.95	5.7	5.52
10	4.5375	5.7	5.05
Total	4.74	5.223	5.515

The results presented in table 2 and fig 5 shows that

- Average Percentage of Attack on non-linear snow 2.0 = 4.74
- Average Percentage of Attack on dynamic feedback based Modified SNOW 2.0= 5.22

- Average Percentage of Attack on static feed back based Modified SNOW 2.0 =5.515

Hence the above results conclude that non-linear snow 2.0 has more resistance as compare to dynamic feedback based modified snow 2.0 and static feedback based modified snow 2.0.

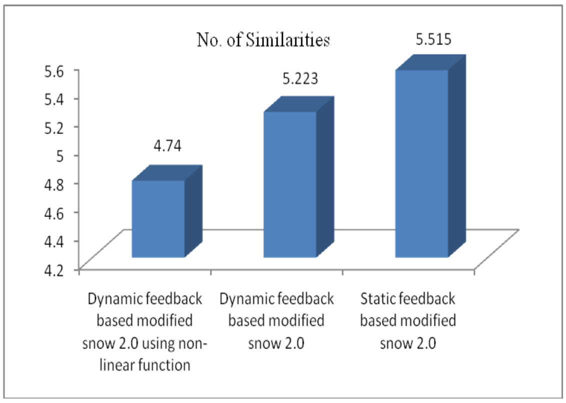

Fig. 5.Graphical representation for average percentage of attacks in phase I

B. Evaluation of Phase II

TABLE III: Evaluation of Phase I1

Experiments	Non-linear snow 2.0	Dynamic feedback based modified snow 2.0	Static feedback based modified snow 2.0
	Similarities	Similarities	Similarities
1	840	863	851
2	816	854	825
3	728	803	830
4	827	874	938
5	822	867	907
6	810	859	943
7	830	864	903
8	798	874	901
9	736	789	934
10	806	865	934
Total	8013	8512	8966

In Phase II, 30 experiments are performed. The only difference is that numbers of key streams are increased in this phase. Each experiment has 1 attack, thus 30 experiments have 30 attacks. 10 attacks are applied on 10 experiments of non-linear snow 2.0, also 10 attacks are applied on 10 experiments of dynamic feedback based modified snow 2.0 and 10 experiments of static feedback based modified snow 2.0. One attack generates 50 key streams hence 30 attacks will generate 1500 key streams. The experimental results show that, by 10 attacks on experiments of non-linear snow 2.0 we cater 8013 similarities, 10 experiments of dynamic feedback based modified snow 2.0 we cater 8512 similarities in dynamic feedback based modified snow 2.0 and also by applying 10 attacks on 10 experiments of static feedback based modified snow 2.0 we cater 8966 similarities in static feedback based Modified snow 2.0. These results shows that if we increase the number of key streams dynamic feedback based modified snow 2.0 without non-linear function and static feedback based modified snow 2.0 is more affected by guess and determine attack as compared to non-linear snow 2.0. Results of experiments are shown in table 3.

Fig 6 shows graphical representation of the result presented in table 1.

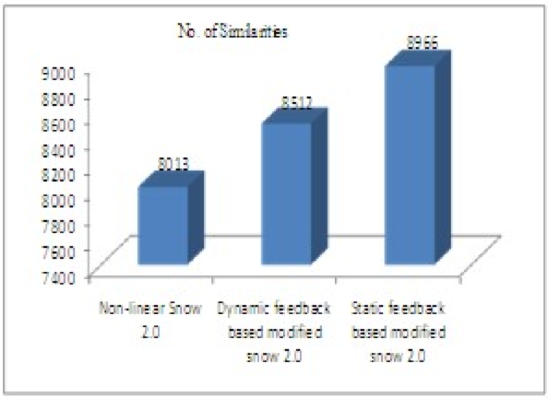

Fig. 6.Graphical representation of phase 1I

The results presented in table 4 and fig 7 shows the average percentage of attacks in phase 11.

TABLE IV : Tabular Representation for Average Percentage of Attacks in Phase I1

Experiments	Non-linear snow 2.0	Dynamic feedback based modified snow 2.0	Static feedback based modified snow 2.0
	%age	%age	%age
1	5.25	5.393	5.318
2	5.1	5.337	5.156
3	5.0375	5.018	5.187
4	5.168	5.462	5.862
5	5.1375	5.418	5.668
6	5.0625	5.368	5.893
7	5.1785	5.4	5.643
8	5.3175	5.462	5.631
9	5.00625	4.931	5.837
10	5.275	5.406	5.837
Total	5.153275	5.3195	5.6032

The results presented in table 4 and fig 7 shows that

- Average Percentage of Attack on dynamic feedback based Modified SNOW 2.0 using non-linear function= 5.153275

- Average Percentage of Attack on dynamic feedback based Modified SNOW 2.0 =5.3195
- Average Percentage of Attack on static feedback based Modified SNOW 2.0 =5.6032

Hence the result conclude that non-linear snow 2.0 has more resistance as compare to dynamic feedback based modified snow 2.0 and static feedback based modified snow 2.0.

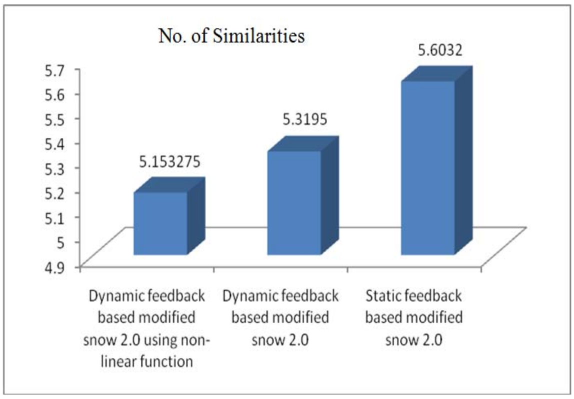

Fig. 7.Graphical representation for average percentage of attacks in phase I1

VI. Conclusion

In this research, guess and determine attack is applied on proposed non-linear snow 2.0, dynamic feedback based modified version of snow 2.0 without non-linear function and static feedback based modified version of snow 2.0. The guess and determine attack attack consist of two phases; Phase I and phase II and experimental results shows that non-linear snow 2.0 has more resistance against guess and determine attack, and Phase II conclude that for large number of key streams, Non-linear snow 2.0 becomes more secure. As a result of the experimental work and analysis, it is concluded that for the encryption of plaintext non-linear snow 2.0 is more secure and reliable for a secure communication as compare to dynamic feedback based modified snow 2.0 without using non-linear function and static feedback based modified snow 2.0. In future we want to convert static feedback based modified snow 2.0 into dynamic feedback based modified snow 2.0 by using non-linear function with one LFSR. Also memory usage and efficiency of the proposed non-linear snow 2.0 can be measured and may also be evaluated for other common attacks

References

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

[2] Patrik Ekdahl , Thomas Johansson, A New Version of the Stream Cipher SNOW, Revised Papers from the 9th Annual International Workshop on Selected Areas in Cryptography, p.47-61, August 15-16, 2002

[3] Yilmaz.E, "Two Versions of the Stream Cipher SNOW", A Thesis Submitted to the Graduate School of Natural And Applied Sciences of Middle East Technical University, in partial fulfillment of the Requirement for Degree of Master of Science, December 2004.

[4] Naz.Tarranum "Analysis of Two Versions of Snow Against Guess and Determine Attack", A Thesis Submitted to the Fatima Jinnah Women University, The Mall Rawalpindi, Pakistan, in partial fulfillment of the Requirement for Degree of Master of Computer Science, August 2008.

[5] Khan. Saira "Designing Modified Snow 2.0 and Analysis of Guess and Determine Attack", A Thesis Submitted to the Fatima Jinnah Women University, The Mall Rawalpindi, Pakistan, in partial fulfillment of the Requirement for Degree of Master of Computer Science, August 2009.

[6] 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.

[7] Shinsaku Kiyomoto, Toshiaki Tanaka and Kouichi Sakurai "A word oriented stream cipher using clock control." In SASC 2007 workshop record pages 260-74 [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

[8] Aihab Khan, Tarranum Naz, Malik Sikandar Hayat Khiyal "Analysis of LFSR Based Snow Family against Guess And Determine Attack" (ISP) 2009 International Conference on Information Security and Privacy, (ISP) 2009 Orlando, FL, USA. July 13-16, 2009 (Accepted)

[9] Saira Khan, Aihab Khan, Malik Sikandar Hayat Khiyal "Designing Dynamic Feedback based Stream Cipher Modified Snow 2.0 and Analysis of Guess and Determine Attack" IEEE International Conference on Emerging Technologies 2010 (ICET 2010), October 18-19, 2010, Islamabad, Pakistan

Mina Masood is a graduate from Dept. of Computer Science, 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 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

Mr. Aihab Khan works in the Department of Computing and Technology, Iqra University, Islamabad, Pakistan. His research interests are in the field of Software Engineering, Databases, Information and Network Security. He has about fifty research publications published in National and International Journals and Conference proceedings.

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