THE NEW HEURISTIC GUESS AND DETERMINE ATTACK ON SNOW 2.0 STREAM CIPHER

Mohammad Sadegh Nemati Nia[1], Ali Payandeh[2]

[1,2]Faculty of Information, Telecommunication and Security Technologies, Malek-e-Ashtar University of Technology, Tehran, Iran
(m_s_nemati; payandeh)@mut.ac.ir

ABSTRACT

SNOW 2.0 is a word oriented stream cipher that has been selected as a standard stream cipher on ISO/IEC 18033-4. One of the general attacks on the stream ciphers is Guess and Determine attack. Heuristic GD attack is GD attack that represents an algorithmic method to analysis the stream cipher with the variables of the same size. The results of HGD attack on TIPSY, SNOW 1.0 and SNOW 2.0 stream ciphers led to less complexity rather than previously known GD attacks. In this paper, the authors use of two auxiliary polynomials to improve HGD attack on SNOW 2.0. This attack reduces the complexity and the size of the guessed basis from O (2^{265}) to O (2^{192}) and 8 to 6, respectively, compared with previous ad-hoc and heuristic GD attacks.

KEYWORDS

Cryptanalysis, Stream cipher, Guess and Determine attack, SNOW 2.0.

1. INTRODUCTION

Cryptology is the science that provides security for the storage and communication data. The cryptography is a branch of cryptology that studies design of cryptographic algorithms and protocols [1]. The stream ciphers are the classes of symmetric cryptographic algorithms that often use in the wireless and telecommunication security applications [2]. A5 family stream cipher use in the GSM mobile telephone and RC4 uses in the wireless LAN [3]. Unlike block ciphers that have a standard block cipher, it is AES, there is no one stream cipher as a standard stream cipher. Although, some competitions are hold around the stream cipher such as NESSIE project in 2000 and eSTREAM project in 2004, but no one stream cipher was standard. One of the reasons, there is no method to design of the stream cipher algorithms [4]. However, in the final portfolio of eSTREAM, after three stages in two profiles suitable for Software and Hardware applications, seven stream ciphers were proposed [5].

SNOW family are stream ciphers consist of four algorithms that evolved at six year. First, the SNOW 1.0 [6] was submitted to NESSIE project [7] by Ekdahel and Ericsson in 2000. Hawkes and Rose launched GD attack [8] on SNOW 1.0 that exploited the second power of LFSR polynomial of the algorithm. This attack show a weakness in tapping of LFSR equations. Another weakness of the cipher, the FSM takes one input from the Linear Feedback Shift Register that is led to linear cryptanalysis of SNOW 1.0 [9]. These weaknesses improved in new version of the algorithm that reintroduced to NESSIE project. At the end of the project, the new algorithm, was called SNOW 2.0, was suggested by evaluators [10].

Many general attacks are applied on stream ciphers for the security evaluation of them. The guess and determine attack is one of these general attacks. In this attack, the attacker,

first guesses some registers of the cipher and then determine remaining registers. Next, he running the keystream. If the resulted keystream is equal with the observed keystream, the guessed values is true and the cipher is broken. Otherwise the attacker guessed another values for registers and repeat the above stages. The elements of the cipher that is guessed by attacker is named as guessed basis [11]. Ahmadi and Eghlidos introduced a systematic algorithm for GD attack as Heuristic Guess and Determine (HGD) attack. This method improved the complexity of GD attacks on SNOW family [11]. In this paper, authors improve the complexity of HGD attack on SNOW 2.0 by the auxiliary equations from $O(2^{265})$ to $O(2^{192})$.

For this sake, the paper organized as follows. In section 2, the structure of SNOW 2.0 is described. In section 3, the new HGD attack launched on SNOW 2.0 and discussed on the result of the attack. The last section is allocated to the conclusion of the paper.

2. A SHORT DESCRIPTION OF SNOW 2.0

SNOW 2.0 is a word oriented stream cipher, with 18-registers internal state. The output words are holding 32 bits. The structure of the cipher like SNOW family, consists two parts: Linear feedback shift register (LFSR) and Finite state machine (FSM). The structure of the cipher is depicted in *Figure 1*.

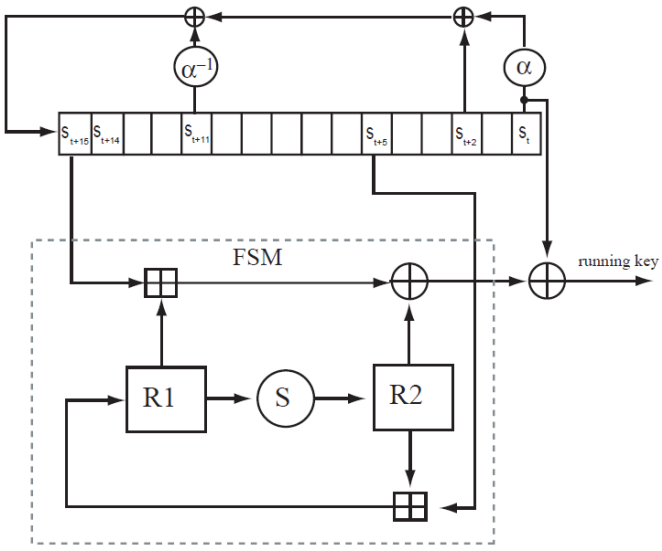

Figure 1. The structure of SNOW 2.0 *[10]*

The length of LFSR is 16 stages. The feedback polynomial of LFSR is as follows.

$$p(x) = \alpha x^{16} + x^{14} + \alpha^{-1}x^5 + 1 \in F_{2^{32}}[x] \qquad (1)$$

Where α is a root of $x^4 + \beta^{23}x^3 + \beta^{245}x^2 + \beta^{48}x + \beta^{239} \in F_{2^8}[x]$, and β is a root of $x^8 + x^7 + x^5 + x^3 + 1 \in F_2[x]$. The recursive equation of LFSR is given by

$$S_{t+16} = \alpha^{-1}S_{t+11} \oplus S_{t+2} \oplus \alpha S_t \qquad (2)$$

The FSM consists of two 32-bit registers, called *R1* and *R2* and is feed by two words input, taken from LFSR. The output of FSM is 32-bit word F. The recursive equations of FSM which update the registers *R1* and *R2* and generate the output F_t are given by

$$R1_t = R2_{t-1} + S_{t+4} \quad t \geq 1 \tag{3}$$

$$R2_t = S\_Box(R1_{t-1}) \tag{4}$$

$$F_t = (R1_t + S_{t+15}) \oplus R2_t \tag{5}$$

By substituting *(4)* in *R2* of *(3)* the following equation is yielded:

$$R1_t = S_{t+4} + S\_Box(R1_{t-2}) \tag{6}$$

The cipher has two modes of operation: key initialization mode and normal mode. In the key initialization mode, the cipher is initialized by two parameters as input values; a 128-bit or 256-bit word as a secret key and 128-bit word as *initialization vector* (IV). After the initialization the input values, the cipher is clocked 32 times. In this mode, the output of FSM is incorporated to feedback loop (see figure 3), and in the normal mode it XORed with the rightmost register of LFSR to produce keystream, see figure 2. The equation of outputs of algorithm as follows:

$$Z_t = S_t \oplus F_t \tag{7}$$

By substituting *(5)* in F_t and *(4)* in $R2_t$ the following equation is concluded:

$$Z_t = S_t \oplus (S_{t+15} + R1_t) \oplus S\_Box(R1_{t-1}) \tag{8}$$

3. HGD ATTACK ON SNOW 2.0

Heuristic guess and determine attack is a systematic GD attack that introduces an algorithm for GD attack on the stream ciphers. The main idea of the procedure is exploitation of *index tables.* The index tables are made corresponding to the equations induced by the update and output function of the stream cipher, according to [11]. The searching operation to selects the best index as a guessed candidate is performed according to the priority criteria [11]. Ahmadi and Eghlidos launched HGD attack on SNOW 2.0 stream cipher with complexity of $O(2^{265})$ with the size of guessed basis of 8. This attack exploit equations (2), (6), (8) and the square of recursive equation of LFSR equation. The index tables corresponding to these equations are shown on Table 1, respectively.

3.1. Improved HGD attack

The authors define two types of equations as following:

- Main equation: The equation is extracted from the cipher, directly.
- Auxiliary equation: The equation is the multiple of recursive equation of LFSR (as a main equation).

- *Table 1 Main Index tables corresponding to equations* (2), (6) *and* (8)

M1			
0	2	11	16
1	3	12	17
.	.	.	.
.	.	.	.
.	.	.	.
17	19	28	34
18	20	29	35

M2		
4	48	50
5	49	51
.	.	.
.	.	.
.	.	.
22	65	67
23	66	68

M3			
0	15	49	50
1	16	50	51
.	.	.	.
.	.	.	.
.	.	.	.
17	32	66	67
18	33	67	68

The algorithm exploit auxiliary index table corresponding to auxiliary equation to improve HGD attack. But the number of factor is infinitive and the complexity of selecting the best factor for recursive equation of LFSR is high. Therefore, we present a general form for factors that it gives a finite number of the factors. The auxiliary equation is convenient when its weight and maximum degree of the equation should be low. Therefore, the weight of the factor polynomial is chosen lowest weight, equals to 2. On the other hand to increase the efficiency of auxiliary index table, the indices of main index table should be repeated on it. Then one of the terms of binomial is constant. Then the form of the factor is ax^n+b. In the field of GF(2) or extension of it, "a" and "b" is 1. The our experiences show when the amount of n is chosen from set of different degrees of main polynomial, then the algorithm of HGD attack gives lowest guessed basis rather than n is chosen otherwise. The authors exploit from this method to improve the HGD attack on SNOW 2.0 stream cipher. The attack explain in the next.

3.2. Improved HGD attack on SNOW 2.0

To launch HGD attack on SNOW 2.0 is used index tables M1, M2 and M3 corresponding to main equations (2), (5) and (8). The authors use of auxiliary index tables corresponding to auxiliary equations to improve HGD attack. To make the auxiliary equations is used from factors x^2+1 and x^5+1 as following:

$$q_2(x) = (x^2+1)(\alpha x^{16} + x^{14} + \alpha^{-1}x^5 + 1) \in F_{2^{32}}[x] \quad (9)$$
$$= \alpha x^{18} + (\alpha+1)x^{16} + x^{14} + \alpha^{-1}x^7 + \alpha^{-1}x^5 + x^2 + 1$$

$$q_3(x) = (x^5+1)(\alpha x^{16} + x^{14} + \alpha^{-1}x^5 + 1) \in F_{2^{32}}[x] \quad (10)$$
$$= \alpha x^{21} + x^{19} + \alpha x^{16} + x^{14} + \alpha^{-1}x^{10} + (\alpha^{-1}+1)x^5 + 1$$

Where the recursive equations corresponding to polynomials as following:

$$S_{t+18} = S_{t+16} \oplus \alpha^{-1}S_{t+13} \oplus \alpha^{-1}S_{t+11} \oplus S_{t+4} \oplus (\alpha+1)S_{t+2} \oplus \alpha S_t \quad (11)$$

$$S_{t+21} = (\alpha^{-1}+1)S_{t+16} \oplus \alpha^{-1}S_{t+11} \oplus S_{t+7} \oplus \alpha S_{t+5} \oplus S_{t+2} \oplus \alpha S_t \quad (12)$$

and the auxiliary index tables corresponding auxiliary equations (11) , (12) are demonstrated in Table 2.

The stages of Improved HGD attack on SNOW 2.0 stream cipher shows in Table 3.

Table 2 Auxiliary Index tables corresponding to equations (11) *and* (12)

M4						
0	2	4	11	13	16	18
1	3	5	12	14	17	19
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
18	20	22	29	31	34	36
19	21	23	30	32	35	37

M5						
0	2	5	7	11	16	21
1	3	6	8	12	17	22
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.
18	20	23	25	29	34	39
19	21	24	26	30	35	40

Table 3 Consecutive stages of improved HGD attack on SNOW 2.0

Step	Known indices	Used equation(s) (index tables)	Determined indices	Step	Known indices	Used equation(s) (index tables)	Determined indices
1	guessed basis	–	18,62,16,14,63,20	27	13,57	M2	59
2	18,62	M2	64	28	5,20,55	M3	54
3	16, 62	M2	60	29	25,59,60	M3	10
4	14,60	M2	58	30	10,12,21	M1	26
5	14,63,64	M3	29	31	4,53,54	M3	19
6	18,20,29	M1	34	32	5,14,19	M1	3
7	30,63	M2	66	33	19,21,30	M1	35
8	16,18,29,34	M1,M4	27,32	34	19,63	M2	65
9	14,16,27,32	M1,M4	25,30	35	21,65	M2	67
10	13,20,22,25,27	M1,M4	9,11	36	23,67	M2	69
11	9,11,18,20,23	M1,M4	7,23	37	3,18,53	M3	52
12	18,20,23,25,29,34	M5	39	38	52,54	M2	8
13	7,9,1618,23	M1,M4	5,21	39	8,10,19	M1	24
14	16,18,21,23,27,32	M5	37	40	13,24,29	M1	15
15	5,7,11,16,21	M1,M5	0,2	41	4,15,20	M1	6
16	0,2,11,16,18	M1,M4	4,13	42	6,8,22	M1	17
17	11,13,17	M1	22	43	3,12,17	M1	1
18	22,66	M2	68	44	15,17,26	M2	31
19	13,62,63	M3	28	45	17,19,28	M1	33
20	14,23,28	M1	12	46	0,15,49	M3	50
21	12,58	M2	56	47	4,50	M2	48
22	7,22,56	M3	57	48	15,59	M2	61
23	11,57	M2	55	49	18,20,22,29,31,34	M4	36
24	9,55	M2	53	50	17,19,22,24,28,33	M5	38
25	7,53	M2	51	51	19,21,24,26,30,35	M5	40
26	5,51	M2	49	52	-	-	-

The rows of 12 and 15 are shown the effect of auxiliary index tables in Table 3. While each of auxiliary index tables isn't used in HGD attack, then the algorithm of HGD attack should guess number of indices {2,0,37,21,5,39}. Then the size of guessed basis and the computational complexity of the attack increases.

3.3. The complexity

During attack, the algorithm found six linear system of two equations and two unknowns. Though, the systems are linear and then the complexity of attack is resulted of the complexity of guessed basis. The guessed basis is {18, 62, 16, 14, 63, 20} and then the attack reduces the complexity of the pervious HGD attack from $O(2^{265})$ to $O(2^{192})$. Table 4, show the comparison of the GD attacks are applied on SNOW 2.0.

Table 4 compare Guess and Determine attack on SNOW 2.0 Stream cipher

Type of attack	Add hoc GD attack	HGD attack	Improved HGD attack
Guessed Basis	-	8	6
Complexity	-	$O(2^{265})$	$O(2^{192})$

4. CONCLUSIONS

In this paper, the authors presented new method for improve HGD attack by using additional equations are named auxiliary equations on SNOW 2.0 stream cipher. The auxiliary equations can improve the determine stage of HGD attack on stream cipher. The attack on SNOW 2.0 used two index tables corresponding two multiples of LFSR connection polynomial. The result shows decreasing the complexity and the size of guessed basis from $O(2^{265})$ to $O(2^{192})$ and 8 to 6, respectively, and implies using of auxiliary equations idea leads to significant reduction in complexity of GD attack.

REFERENCES

[1] J. LANO, *thesis: CRYPTANALYSIS AND DESIGN OF SYNCHRONOUS STREAM CIPHERS*, B. Preneel, Ed., KATHOLIEKE UNIVERSITEIT LEUVEN, 2006.

[2] A. Menezes, P. v. Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997. ISBN 0-8493-8523-7..

[3] A. Klein, Stream Ciphers, Ghent, Belgium: Springer-Verlag London, 2013.

[4] A. w. Dent and C. J. Mitchell, User's Guide to Cryptography and Standards, Norwood, US: Artech House, 2005.

[5] S. Babbage, J. Borghoff and V. Velichkov, "The eSTREAM Portfolio in 2012," Babbage, Steve ; Borghoff, Julia; Velichkov,Vesselin, Carlos Cid and Matt Robshaw ed., 2012.

[6] P. EKDAHL and T. JOHANSSON, "SNOW – a new stream cipher," First NESSIE Workshop, Heverlee, Belgium, 2000.

[7] P. B., "New European Schemes for Signature, Integrity and Encryption (NESSIE): A Status Report," in *5th International Workshop PKC 2002*, 2002.

[8] P. Hawkes and G. Rose, "Guess and determine attaks on SNOW," in *In Selected Area of Cryptography-SAC2002*, 2002.

[9] D. Coppersmith, S. Halevi and C. Jutla, "Cryptanalysis of stream ciphers with linear masking," in *Advances in Cryptology — CRYPTO 2002*, 2002.

[10] P. EKDAHL and T. JOHANSSON, "A New Version of the Stream Cipher SNOW," in *SAC 2002*, Berlin Heidelberg 2003, Springer_Verlag, LNCS 2595, PP. 47-61, 2002.

[11] H. Ahmadi and T. Eghlidos, "Heuristic guess-and-determine attacks on stream ciphers," in *Information Security IET, Vol.3, No.2, PP.66-73*, 20th January 2009.