IJCSC 0973-7391 Volume 8 • Issue 2 March 2017 - Sept 2017 pp. 5-11 available online at www.csjournalss.com

Cryptanalysis and Study of a Modern Stream Cipher-Grain

Rishav Chatterjee
School of Computer Science & Engineering, Kalinga Institute of Industrial Technology, Bhubaneswar, India
rishavpiku@gmail.com

Abstract: Grain is one of the most important and modern stream ciphers, which was found by M. Hell, T. Johansson [3] as a part of ECRYPT project while they called for proposals of stream ciphers. Grain is considered as efficient and it is less prone to attacks. It is best suited for hardware implementations. Grain-80 and Grain-128 are the two ciphers in the Grain family of ciphers. Grain-128a has been found as an alternative as researchers have found demerits in the previous members of the Grain family. It is more advantageous to use Grain Ciphers rather than using stream ciphers like E0 and A5/1, as far as complexion of hardware and throughput is concerned. Moreover, these ciphers are known as hardware oriented stream ciphers.
Index Terms: Grain, Cipher, attacks, e-Stream, (key words).

1. INTRODUCTION

We need to ponder about a quite number of aspects while assigning a cryptographic Cipher, for example, there are parameters like simplicity, speed, security aspects. We need to pursue further research on stream ciphers which falls under symmetric cryptographic, primitives. Stream Ciphers are unique and no unlike other stream ciphers. They can process bit by simply applying a very transparent and easy mechanism and an ever changing invertible transformation. The e stream [1] project throws a light on the fact that stream ciphers are undoubtedly useful. They are basically symmetric key algorithms which are essentially based on the concepts of PRGs. We need to rethink the case of binary and other additive stream ciphers, the secret key and an IV. We perform the binary XOR operation of the key stream and plain text in order to get the cipher text. The privacy of the binary additive stream cipher must be ensured and it is directly proportional to the changeability of the key stream which it holds. This eStream project was launched as previously the NESSIE [2] could not succeeded in finding a much more secure cipher. They proposed Grain as a modern cipher, which in turn proved to be successful. This cipher is based on hardware applications and it has a low maintenance cost.

Many of these ciphers are constructed using shift registers. One of them is linear feedback shift register, which has a length of 80 bit. The other one is called non-linear feedback shift register, which has a 64 bits of IV and 16 bits of 1s. Moreover, it has 80 bits of key. In total LFSR and NFSR comprises of 160 bits. This stream ciphers was developed by M. Hell, W. Meier, T. Johansson [3]. So, as a result of applying one Boolean function and choosing random bits from LFSR and NFSR, one key stream bit will be generated. LFSR Sequences is prone to attacks and hence doesn't guarantee security. When we join LFSR and NFSR together, it has been found to be much more secure. The founders of grain have proposed that there are no such faster methods than exhaustive key search. Grain is much more secure when compared to other ciphers like A5/1 and E0. E0 is used Bluetooth and A5/1 is used in GSM.

In this paper, we will broadly describe Grain and its members and will discuss the attacks mounted on them as well as, propose modification schemes for Grain. The ciphers of the Grain family namely Grain 1, Grain v1 and Grain 128 are known as bit synchronous stream ciphers as it has already been mentioned in [4].

This paper has been divided into five sections. Section 1 will give the detailed knowledge of Grain family of ciphers. Section 2 will describe the possible attacks on these ciphers. Section 3 will give us further modification schemes for using other designs. Section 4 will give us the possible attacks on Grain Ciphers and finally Section 5 concludes the paper.

I. Grain Family of Ciphers- Design & Analysis

The first section will give the descriptive study of the Grain Family of Ciphers. Now, we will get to know about the design of Grain from the following figure 1. This cipher is comprised of three blocks which are LFSR, NFSR and Non Boolean output function. The initialization vector is used to initialize the state. We need to increase the size of secret key and then, we run the state. The contents of both the LFSR and the NFSR are denoted by s_i, s_{i+1}, . . . , s_{i+79} and b_i , b_{i+1}, . . . , b_{i+79}. The output polynomial of the LFSR, f (x), is a primitive polynomial and it has a degree of 80. It has been shown as below

II.

$$f(x) = 1 + x^{18} + x^{29} + x^{42} + x^{57} + x^{67} + x^{80}.$$

The update function of LFSR is given as

$$s_{i+80} = s_{i+62} + s_{i+51} + s_{i+38} + s_{i+23} + s_{i+13} + s_i$$

The output polynomial of LFSR is used to update the state of the register and is represented as –

$$f(x) = 1 + x^{18} + x^{29} + x^{42} + x^{57} + x^{67} + x^{80}$$

The feedback polynomial of the NFSR, g(x), is defined as

$$g(x) = 1 + x^{17} + x^{20} + x^{28} + x^{35} + x^{43} + x^{47} + x^{52} + x^{59} + x^{65} + x^{71} + x^{80} + x17x20 + x43x47 + x65x71 + x20x28x35 + x47x52x59 + x17x35x52x71 + x20x28x43x47 + x17x20x59x65 + x17x20x28x35x43 + x47x52x59x65x71 + x28x35x43x47x52x59.$$

This is the update function of the NFSR. Please take a note that the bit s_i, which is embedded inside with the input, which is included in the update function itself.

$$b_{i+80} = s_i + b_{i+63} + b_{i+60} + b_{i+52} + b_{i+45} + b_{i+37} + b_{i+33} + b_{i+28} + b_{i+21} + b_{i+15} + b_{i+9} + b_i + b_{i+63}b_{i+60} + b_{i+37}b_{i+33} + b_{i+15}b_{i+9} + b_{i+60}b_{i+52}b_{i+45} + b_{i+33}b_{i+28}b_{i+21} + b_{i+63}b_{i+45}b_{i+28}b_{i+9} + b_{i+60}b_{i+52}b_{i+37}b_{i+33} + b_{i+63}b_{i+60}b_{i+21}b_{i+15} + + b_{i+63}b_{i+60}b_{i+52}b_{i+45}b_{i+37} + b_{i+33}b_{i+28}b_{i+21}b_{i+15}b_{i+9} + + b_{i+52}b_{i+45}b_{i+37}b_{i+33}b_{i+28}b_{i+21}.$$

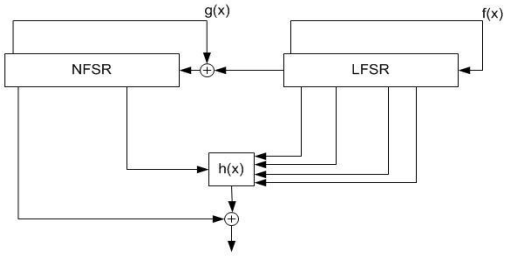


Fig. 1. The Grain cipher.

The shift registers, LFSR and NFSR, represents the states of the cipher. Variables are inserted into a Boolean function, h(x) right from the state. The output filter function is chosen to be balanced and has algebraic degree of 3. The ANF or Algebraic normal form of this non-linear filter function K is given as -

$$h(x) = x_1 + x_4 + x_0x_3 + x_2x_3 + x_3x_4 + x_0x_1x_2 + x_0x_2x_3 + x_0x_2x_4 + x_1x_2x_4 + x_2x_3x_4$$

where the variables x_0, x_1, x_2, x_3 and x_4 corresponds to the LFSR bits s_{i+3}, s_{i+25}, s_{i+46}, s_{i+64} and b_{i+63} respectively. The output function is fed into the bit b_i from the NFSR to produce the key stream.

III.

The Algebraic normal form of the key stream bits of the cipher at any clocking

$$z_i = \sum_{i+k} + h(s_{i+3}, s_{i+25}, s_{i+46}, s_{i+64}, b_{i+63})$$

Where $A = \{1, 2, 4, 10, 31, 43, 56\}$

A. KEY INITIALIZATION

The key initialization is done using finite state machine. Both IV and key are used for the same. The cipher is initiated with the help of the key and the IV before generating key stream. We generate the key stream by clocking .The secret key remains in the NFSR .The key is embedded inside the NFSR and the starting 64 bits in case of 80 bit ciphers is present inside the Initialization Vector [5]. The remaining bit portions are filled with all ones. We run this for 160 rounds and then we reach the initial step, then we clock it to get the key stream. The output of the function named h(x) is put into both the shift registers rather than just giving it as output. The cipher is clocked 2K times. Kucuk [6] stated that the makers chose to cover the 31 bits of LFSR by ones and last bit with zero so as to tackle the thrust in the modified Grain 128a. The initialization process has been shown in Figure 2.

-

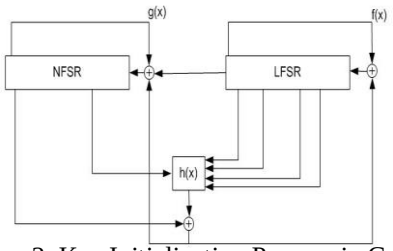


Figure 2. Key Initialization Process in Grain-80.

B. Attacks mounted on Grain V_0

An attack was mounted on Grain V0 by Cryptographers like Khazaei and Hassanzadeh [7] which essentially make use of the concept of linear sequential circuit approximation method given by Golic [8]. This distinguishing attack can differ a Grain feedback sequence from a random sequence with some complexity of O (2^n).

This type of attack was mounted by Barbein, Gilbert and Maximov [8] [9] that is essentially a key recovery attack, which has been mounted against Grain V0. Firstly, the linear approximation method is used to derive the LFSR bits in this attack and these bits are then reused to restore the initial state of NFSR and an idea of the key.

We have proposed *Grain* V_1 in order to tackle this situation.

C. Throughput Rate of the Grain

It is feasible enough to increase the speed of the cipher by increasing its Throughput rate. LFSR and NFSR are clocked such that they can produce an output of 1 bit/sec. The speed can be geared up to a certain level just by increasing the number of hardware components. This is simply done by implementing the output Boolean functions, f(x), g(x) and h(x) [3]. Actually, the last 15 bits of the registers are not fed into the feedback function. As a result, the speed gets enhanced to its 16 times, if sufficient and substantial amount of hardware is used.

III. Grain V_1

The output polynomial $g_1(x)$ of NFSR is given as:

$$g_1(x) = 1 + x^{18} + x^{20} + x^{28} + x^{35} + x^{43} + x^{47} + x^{52} + x^{59} + x_{65} + x_{71} + x_{80} + x_{17}x_{20} + x_{43}x_{47} + x_{65}x_{71} + x_{20}x_{28}x_{35} + x_{47}x_{52}x_{59} + x_{17}x_{35}x_{52}x_{71} + x_{20}x_{28}x_{43}x_{47} + x_{17}x_{20}x_{59}x_{65} + x_{17}x_{20}x_{28}x_{35}x_{43} + x_{47}x_{52}x_{59}x_{65}x_{71} + x_{28}x_{35}x_{43}x_{47}x_{52}x_{59}$$

And hence the new update function of NFSR as per the new feedback polynomial of NFSR is defined as:

$$b_{i+80} = s_i + b_i + b_{i+9} + b_{i+14} + b_{i+21} + b_{i+28} + b_{i+33} + b_{i+37} + b_{i+45} + b_{i+52} + b_{i+60} + b_{i+62} + b_{i+9}\,b_{i+15} + b_{i+33}\,b_{i+37} + b_{i+60}\,b_{i+63} + b_i{+}21\,b_i{+}28 b_{i+33} + b_i{+}45 b_{i+52}\,b_{i+60} + b_{i+15}\,b_{i+21} b_{i+60}\,b_{i+63} + b_{i+33}\,b_{i+37}\,b_{i+52}\,b_{i+60} + b_{i+9} b_{i+28} b_{i+45} b_{i+63} + b_{i+9} b_{i+15} b_{i+21} b_{i+28} b_{i+33} + b_{i+37} b_{i+45} b_{i+52} b_{i+60} b_{i+63} + b_{i+21} b_{i+28} b_{i+33} b_{i+37} b_{i+45} b_{i+52}$$

Here, the function gets modified slightly and hence the new key stream function is defined as:

$$zi = \sum i + k + h(si{+}3, si{+}25, si{+}46, si{+}64, bi{+}63)$$

Where $A = \{1, 2, 4, 10, 31, 43, 56\}$

A. Attacks mounted on Grain V_1.

1. Kucuk and Preneel [13] attacked Grain V_1 by using a defect in the initialization algorithm of Grain. This work has been done extensively on the work which Kucuk did in [6]. This attack led to an exploitation of the sliding property of Grain [8].
2. Secondly, a recovery attack has been mounted by Lee et al [14], who have extended and proposed a more sophisticated attack by exploiting the same weakness of related key in Grain V_1 [8].
3. TMTO attack [15] was proposed by Bjorstad using key stream bits which were known at the earliest.
4. Dynamic Cube was one of the renowned attacks [16], which was also proposed against the Grain V1 by Rahimi et al.

IV. Grain 128

When the key size of a stream cipher is S then a Time Memory Tradeoff attack can be mounted on it with a complexity of O ($2^{S/2}$) [8]. Suppose we take a cipher having 160 bit key and we eventually found that can be attacked with a complexity of order O (2^{80}) and the complexity is quite achievable. The new 128 bit version which was developed right after the Grain-80 series is known as Grain 128. It is more suitable for hardware environments. Grain 128 uses a 128 bits of both LFSR and NFSR that provides a 256 bit internal state equally divided among LFSR and NFSR while other design principles remained same. The Boolean function h(x) has also been updated.

Grain 128 uses a 128 bits of both LFSR and NFSR, which provides a total of 256 bit state and it has been symmetrically divided among LFSR and NFSR. The output Boolean function has been updated as well. We have described the process in

the below given Figure 2.

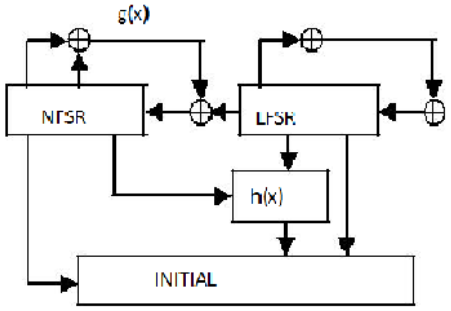


Figure 2: The process of key stream generation in Grain 128.

The feedback polynomials and update functions of LFSR and NFSR were updated accordingly.

Feedback polynomial of LFSR

$$f(x) = 1 + x^{32} + x^{47} + x^{58} + x^{90} + x^{121} + x^{128}$$

It is an primitive polynomial which has a degree of 128. The update function of LFSR is given as:

$$s_{i+128} = s_i + s_{i+7} + s_{i+38} + s_{i+70} + s_{i+81} + s_{i+96}$$

The feedback polynomial of NFSR has been defined as:

$$g(x) = 1 + x^{32} + x^{37} + x^{72} + x^{102} + x^{128} + x^{44}x^{60} + x^{61}x^{125} + x63x67 + x69x101 + x80x88 + x110x111 + x115x117$$

Now the update function of NFSR is given as:

$$b_{i+128} = s_i + b_i + b_{i+26} + b_{i+56} + b_{i+91} + b_{i+96} + b_{i+3}b_{i+67} + b_{i+11}\,b_{i+13} + b_{i+17}b_{i+18} + b_{i+27}b_{i+59} + b_{i+40}b_{i+48} + b_{i+61}b_{i+65} + b_{i+68}b_{i+84}$$

The filter function is given as:

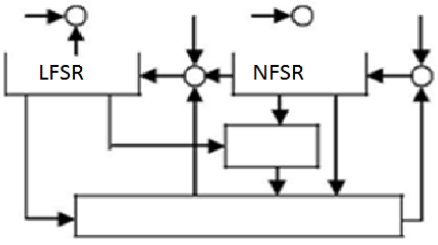
$$H(x) = x_0x_1 + x_2x_3 + x_4x_5 + x_6x_7 + x_0x_4x_8$$

Where we take two inputs from NFSR and seven inputs from LFSR and the variables from x_0 to x_8 has been taken respectively and then it corresponds to the tap position b_{i+12}, s_{i+8}, s_{i+13}, s_{i+20}, b_{i+95}, s_{i+42}, s_{i+60}, s_{i+79} and s_{i+95}.

The keystream function is defined as follows:

$$z_i = \sum_{i+j} + h(x) + s_{i+93}$$

Where $A = \{2, 15, 36, 45, 64, 73, 89\}$



A. Attacks mounted on Grain 128

1. Dinur et al presented a key recovery attack with the help of a dedicated reconfigurable hardware and based on cube testers [8] [14].
2. Grain 128 and Grain V_1 has a similar structure. So, the attacks are quite similar. A key recovery attack has been mounted by Lee et al [14].

3. A fault attack has been mounted on Grain 128 by Karmakar and Chowdhury [15] which targets NFSR and hence, it could compute the secret key with time a complexity of O (2^{21}) and space complexity of O (2^{22}).
4. Dynamic Cube attack [16] was also mounted on the Grain V1 by Rahimi et al.

V. Grain128a

Grain 128a was proposed in order to add the Message Authentication Code scheme and further it also came as a substitute for Grain 128 as it had few demerits. As a result, the designers of Grain have proposed a new design called Grain 128a where a stands for authentication.

Grain 128a is the strongest amongst other members in the Grain family of stream ciphers and has 128 bits. This design uses the same output polynomial in LFSR and same filter function which was previously used in Grain 128 but the feedback polynomial has been strengthened to newer highs, as far as various attacks proposed against Grain 128 are concerned.

The new Feedback polynomial of NFSR

$$g(x) = 1 + x^{32} + x^{37} + x^{72} + x^{102} + x^{128} + x^{44}x^{60} + x^{61}x^{125} + {}_x63_x67 + {}_x69_x101 + {}_x80_x88 + {}_x110_x111 + {}_x115_x117 + {}_x46_x50_x58 + {}_x103_x104_x106 + {}_x33_x35_x36_x40$$

Now the update function of NFSR is given as:

$$Rb_{i+128} = s_i + b_i + b_{i+26} + b_{i+56} + b_{i+91} + bi+96 + b_{i+3}b_{i+67} + b_{i+11}b_{i+13} + b_{i+17}b_{i+18} + b_i + 27b_{i+59} + b_i+40b_{i+48} + b_{i+61}b_{i+65} + b_{i+88}b_{i+92}b_{i+93}b_{i+95} + b_{i+22}b_{i+24}b_{i+25}$$

Both the filter function used in Grain 128 and 128a are same but there has been a noticeable change in the key stream function and is defined as:

$$y_i = h(x) + s_{i+93} + \sum_{i+j}$$

Where $A = \{2, 15, 36, 45, 64, 73, 89\}$

$$zi = y64+2i$$

A. Attacks on Grain 128a

1. The first 64 bits is not openly accessible until the authentication mode is present. It doesn't let the attackers to attack until (a) is ON. S.Mitra, Banik and Sarkar [16] mounted a differential attack on the MAC and not on the key stream.
2. Lin and Guan [17] attacked using 2^{96} of IV and 2^{104} of key stream bits in order to recover 128 bits of key. It is basically comes under Chosen IV attack and a key related attack.

VI. Comparative Analysis of Ciphers under Grain Family.

We will discuss and compare a couple of ciphers which we have discussed in the previous sections. The Main two ciphers in the Grain family are Grain-80 and Grain-128. Under Grain 80, there are two ciphers namely, Grain V_0 and Grain V_1.
Under Grain 128, there are two ciphers namely, Grain 128 and Grain 128a.
We will compare those on the basis of a parameter called padding.

Under Grain 80, both of the ciphers have a key length of 80 bits and an IV length of 64 bits. Under Grain 128, both of the ciphers have a key length of 128 bits and IV length of 96 bits. In both the Ciphers in the Grain family, last 16 and 32 bits are basically 1s. Hence, we differentiate on the basis of Padding:-

CIPHERS	PADDING IN IV
1. GRAIN V_0	TTTT
2. GRAIN V_1	TTTT
3. GRAIN 128	TTTTTTTT
4. GRAIN 128a	TTTTTTTF

Table 1 gives us the *padding values of the grain family of ciphers.*

Table 1 gives us the padding values and bits for each stream cipher in the Grain family. Hence, we have noticed that the last bit of LFSR bit in the Grain 128a is 0.
The other bits in the other ciphers in the Grain Family are all 1s.
'0' has been included in the last bit in order to avoid the attack made by Kucuk [6].
Now, we will classify them on the basis of Gate Count.

TYPE OF CIPHERS	NET GATE COUNT FOR LFSR AND NFSR	NET GATE COUNT FOR OUTPUT BOOLEAN FUNCTION	RESULTANT GATE COUNT
GRAIN-80	640	640	1440
GRAIN-128	1024	1024	2145.5
GRAIN-128a	1024	1024	2769.5

Table 2. Gate count values for the ciphers in the Grain family.

Table 2 gives the values of Gate count for the ciphers in the Grain family respectively. Gate count is one of the important parameters to decide whether a cipher is a good one or not. The Cipher, which has a higher gate count is more preferred over the other. The table shows us that Grain 128a has higher gate count value than Grain 128. It basically resembles that Grain 128a can be used more easily and efficiently rather than using the other. Grain family of stream cipher is known for its less complexion in hardware and Grain 128a has a less complexion in hardware, being the strongest stream cipher in its family.

VII. **CRYPTANALYSIS**

In this section, we have tried to show few attacks that can attacked on these ciphers in the family of Grain. However, we could find that there can be no attack that can be faster than brute force search or simple known as exhaustive key search. Grain is a modern cipher and it has a good resistant property such that it is not prone to these kind of attacks. There are few of them which can do the initial attack but have less chance to get through.

The attacks are namely-

1. Correlation Attacks

The bits in the LFSR are properly balanced. In NFSR, the bits are not properly balanced. However, when we perform XOR operation between the output function and the LFSR, the bit sequences in the NFSR are balanced in such a way that they are adequately placed. Moreover, recall that g(x) is a balanced function. Therefore, the bits in the NFSR are supposed to be uncorrelated to the LFSR bits.

The function h(x) is chosen to be correlation immune of first order [18]. When one input is taken from the NFSR and h(x) is xored with a state bit of the NFSR, correlations of the output of the generator to sums of LFSR-bits will be so small that they will not be exploitable by (fast) correlation attacks.

2. Chosen-IV Attack

A necessary condition for defeating differential-like or statistical chosen-IV attacks is that the initial states for any two chosen IV's (or sets of IV's) are algebraically and statistically unrelated. The cycles in key initialization is chosen in such a way so that the Hamming weight of the differences in the full initial 160-bit state for two IV's after initialization is close to random. This should prevent chosen-IV attacks.

The efficiency of the key initialization can be easily increased by reducing the number of initial clocks. The state will depend on both the key and the Initialization vector. It is feasible to reinitialize the cipher with the same key, but with a different IV with a change in the bit positions [3].

3. Fault Attacks.

The strongest attacks, which can be mounted on any cipher, are fault attacks. Fault attacks were initiated to attack stream ciphers [18], and have shown to be efficient against many known constructions of stream ciphers. This suggests that it is hard to completely defeat fault attacks on stream ciphers [3]. The fault attacks doesn't affect the content of LFSR but they can affect the content of NFSR in a non-linear manner, but it is relatively tougher. A lot of research have not been done on these fault attacks and their effects on Grain.

VIII. CONCLUSION.

In this paper, we have shown a very descriptive analysis and design of the Grain family of stream ciphers along with the attacks, which are mounted on them. We have learnt the various demerits of the stream ciphers from this paper. We have shown a much precise comparative study on the family itself of the Grain stream ciphers. The results show that Grain family of stream ciphers and more specifically Grain 128a is the best suited one for hardware based applications as it is less complex.

IX. ACKNOWLEDGEMENT

I am really indebted to Prof. Sourav Mukhopadhyay, Department of Computer Science Engineering, IIT Kharagpur, for his extended support and guidance.

X. REFERENCES

[1] ECRYPT, "eSTREAM: ECRYPT Stream Cipher Project ". Available at http://www.ecrypt.eu.org/stream/ .
[2] NESSIE. New European Schemes for signature, integrity and Encryption. Available at http://www.cryptonessie.org
[3] M.Hell, T.Johansson, W.Meier, "Grain- a Stream Cipher for Constrained Environments", International Journal of Wireless and Mobile Computing. Special Issue on Security of Computer Network and Mobile Systems, 2006.
.[4] Martin Hell, Thomas Johansson, A. Maximov, Willi Meier, "The Grain Family of Ciphers, New Stream Cipher Designs, The eStream Finalists, LNCS 4986.
[5] Hell, Martin, et.al. "The Grain family of stream ciphers". New stream cipher designs. Springer Berlin Heidelberg, 2008. 179-190.
[6] Kucuk, O." Slide resynchronization attack on the initialization of Grain 1.0" eStream, ECRYPT stream project, Report 44 (2006):2006.
[7] Khazaei, Shahram, Mehdi Hassanzadeh, and Mohammad Kiaei. "Distinguishing attack on grain." 2005-12-01)[2009-01-12]. http://www. ecrypt. eu. org/stream/papersdir/071. Pdf (2005).
[8] Mohammad Ubaidullah Bokhar, Shadab Alam, Syed Hamid Hasan,"A Detailed Analysis of Grain family of Stream Ciphers", IJCNIS, vol.6, no.6, pp.34-40, 2014. DOI: 10.5815/ijcnis.2014.06.05
[9] Berbain, Côme, Henri Gilbert, and Alexander Maximov. "Cryptanalysis of grain."Fast Software Encryption. Springer Berlin Heidelberg, 2006.
[10] De Cannière, Christophe, Özgül Küçük, and Bart Preneel. "Analysis of Grain's initialization algorithm." Progress in Cryptology–AFRICACRYPT 2008. Springer Berlin Heidelberg, 2008. 276-289.
[11]Lee, Yuseop, et al. "Related-key chosen IV attacks on Grain-v1 and Grain-128."Information Security and Privacy. Springer Berlin Heidelberg, 2008.
[12] T.E. Bjørstad. Cryptanalysis of grain using time/memory/data tradeoffs. Available at http://www.ecrypt.eu.org/stream/papersdir/2008/012.pdf.
[13] Dinur, Itai, and Adi Shamir. "Breaking Grain-128 with dynamic cube attacks, "Fast Software Encryption. Springer Berlin Heidelberg, 2011.
[14] Dinur et al presented a key recovery attack with the help of a dedicated reconfigurable hardware and based on cube testers.
[15] Karmakar, Sandip, and Dipanwita Roy Chowdhury. "Fault analysis of grain-128 by targeting NFSR." Progress in Cryptology–AFRICACRYPT 2011. Springer Berlin Heidelberg, 2011. 298-315.
[16] Banik, Subhadeep, Subhamoy Maitra, and Santanu Sarkar. "A differential fault attack on grain-128a using MACs." Security, Privacy, and Applied Cryptography Engineering. Springer Berlin Heidelberg, 2012. 111-125.
[17] Ding, Lin, and Jie Guan. "Related Key Chosen IV Attack on Grain-128a Stream Cipher." Information Forensics and Security, IEEE Transactions on 8.5 (2013): 803-809.
[18] J.J. Hoch, A. Shamir. Fault Analysis of Stream Ciphers. CHES 2004, Springer Verlag, LNCS 3156, pp. 240–253.