A New Distinguisher on Grain v1 for 106 rounds

Santanu Sarkar

Department of Mathematics,
Indian Institute of Technology Madras
Sardar Patel Road, Chennai 600036, India

NIST Gaithersburg

Presented by: Rebhu Johymalyo Josh

21 July, 2015

Outline of the Talk

- Grain v1
- Knellwolf et al. attack on Grain v1 for 97 rounds
- Our distinguisher on Grain v1 for 106 rounds

Grain Family

Proposed by Hell, Johansson and Meier in 2005

Part of eStream portfolio

Grain v1, Grain 128 and Grain 128a

Grain v1

Consists of an 80 bit LFSR and an 80 bit NFSR.

The LFSR update function is

$$y_{t+80} = y_{t+62} + y_{t+51} + y_{t+38} + y_{t+23} + y_{t+13} + y_t.$$

NFSR update

The NFSR state is updated as follows

$$x_{t+80} = y_t + g(x_{t+63}, x_{t+62}, x_{t+60}, x_{t+52}, x_{t+45}, x_{t+37}, x_{t+33}, x_{t+28}, x_{t+21},$$
$$x_{t+15}, x_{t+14}, x_{t+9}, x_t) \text{ where}$$

$$g(x_{t+63}, x_{t+62}, x_{t+60}, x_{t+52}, x_{t+45}, x_{t+37}, x_{t+33}, x_{t+28}, x_{t+21}, x_{t+15}, x_{t+14}, x_{t+9}, x_t)$$

$$\begin{aligned} = {} & x_{t+62} + x_{t+60} + x_{t+52} + x_{t+45} + x_{t+37} + x_{t+33} + x_{t+28} + x_{t+21} + \\ & x_{t+14} + x_{t+9} + x_t + x_{t+63}x_{t+60} + x_{t+37}x_{t+33} + x_{t+15}x_{t+9} + \\ & x_{t+60}x_{t+52}x_{t+45} + x_{t+33}x_{t+28}x_{t+21} + x_{t+63}x_{t+45}x_{t+28}x_{t+9} + \\ & x_{t+60}x_{t+52}x_{t+37}x_{t+33} + x_{t+63}x_{t+60}x_{t+21}x_{t+15} + \\ & x_{t+63}x_{t+60}x_{t+52}x_{t+45}x_{t+37} + x_{t+33}x_{t+28}x_{t+21}x_{t+15}x_{t+9} + \\ & x_{t+52}x_{t+45}x_{t+37}x_{t+33}x_{t+28}x_{t+21} \end{aligned}$$

Output Keystream

$$z_t = \bigoplus_{a \in A} x_{t+a} + h(y_{t+3}, y_{t+25}, y_{t+46}, y_{t+64}, x_{t+63})$$

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

$$\begin{aligned} h(s_0, s_1, s_2, s_3, s_4) = {} & s_1 + s_4 + s_0 s_3 + s_2 s_3 + s_3 s_4 + s_0 s_1 s_2 + s_0 s_2 s_3 \\ & + s_0 s_2 s_4 + s_1 s_2 s_4 + s_2 s_3 s_4 \end{aligned}$$

Key Scheduling Algorithm (KSA)

Grain v1 uses 80-bit key K, and 64-bit initialization vector IV.

The key is loaded in the NFSR

The IV is loaded in the 0^{th} to the 63^{th} bits of the LFSR.

The remaining 64^{th} to 79^{th} bits of the LFSR are loaded with 1.

Then, for the first 160 clocks, the key-stream bit z_t is XOR-ed to both the LFSR and NFSR update functions.

Pseudo-Random key-stream Generation Algorithm (PRGA)

After the KSA, z_t is no longer XOR-ed to the LFSR and the NFSR.

Thus, the LFSR and NFSR are updated as $y_{t+n} = f(Y_t), x_{t+n} = y_t + g(X_t)$.

Distinguisher on Grain v1

Knellwolf et al. in Asiacrypt 2010

80 bit key $k_0, \ldots, k_{79}$ and 64 bit IV $v_0, \ldots, v_{63}$.

Grain v1 is first intialised with $X_0 = [k_0, \ldots, k_{79}]$ and $Y_0 = [v_0, \ldots, v_{63}, \overbrace{1, \ldots, 1}^{16}]$.

Here X_0 corresponds to NFSR and Y_0 corresponds to LFSR.

The idea

Next start with NFSR $X_0' = [k_0, \ldots, k_{79}]$ but different LFSR $Y_0' = [v_0, \ldots, 1 \oplus v37, v_{63}, \overbrace{1, \ldots, 1}^{16}]$.

Thus two states S_0 and S_0' initialized by (X_0, Y_0) and (X_0', Y_0') different only at one position.

But when more and more KSA rounds are completed, more and more positions of the states will be differ.

Conditions of z_{12}, z_{34} and z_{40} of KSA

The idea

The idea is to delay the diffusion of the differential.

The conditions may be classified in to two types:

- **Type 1:** Conditions only on IV
- **Type 2:** Conditions on both Key and IV.

Attack Idea

z_t and z_t: Output bit produced in the t-th KSA round when states are loaded by (X_0, Y_0) and (X_0, Y_0).

The attack idea is as follows:

1. For $i = 0, \ldots, 11$, it is not difficult to show that $z_i = z_i$.
2. When $i = 12$, $z_i \oplus z_i = v_{15}v_{58} \oplus v_{58}k_{75} \oplus 1$.

Attack Idea

z_t and z_t: Output bit produced in the t-th KSA round when states are loaded by (X_0, Y_0) and (X_0, Y_0).

The attack idea is as follows:

1. For $i = 0, \ldots, 11$, it is not difficult to show that $z_i = z_i$.
2. When $i = 12$, $z_i \oplus z_i = v_{15}v_{58} \oplus v_{58}k_{75} \oplus 1$.
3. To make $v_{15}v_{58} \oplus v_{58}k_{75} \oplus 1 = 0$, set $v_{58} = 1$ and $v_{15} = 1 \oplus k_{75}$.
4. Thus we have one Type 1 condition $v_{58} = 1$ and one Type 2 condition $C_1 : v_{15} = 1 \oplus k_{75}$.
5. For $i = 13, \ldots, 29$, z_i will be always equal to z_i.

6. When $i = 30$, z_{30} will be always different from z_{30}.
7. z_i will be always equal to z_i for $i = 31$ and 32.
8. When $i = 34$, $z_{34} \oplus z_{34}$ will be an algebraic expression on Key and IV.
9. If attacker sets 13 Type 1 conditions $v_0 = 0, v_1 = 0, v_3 = 0, v_4 = 0, v_5 = 0, v_{21} = 0, v_{25} = 0, v_{26} = 0, v_{27} = 0, v_{43} = 0, v_{46} = 0, v_{47} = 0, v_{48} = 0$ and two Type 2 conditions

$$\begin{aligned} C_2 : v_{13} &= v_{23} \oplus v_{38} \oplus v_{51} \oplus v_{62} \oplus k_1 \oplus k_2 \oplus k_4 \oplus k_{10} \\ &\quad \oplus k_{31} \oplus k_{43} \oplus k_{56}, \\ C_3 : v_2 &= v_{18} \oplus v_{31} \oplus v_{40} \oplus v_{41} \oplus v_{53} \oplus v_{56} \oplus f_1(K), \end{aligned}$$

where $f_1(K)$ is a polynomial over Key of degree 7 and 39 monomials, $z_{34} = z_{34}$.

Attack idea

10. $z_i = z_i$ for $35 \leq i \leq 39$.
11. When $i = 40$, again $z_{40} \oplus z_{40}$ will be an algebraic expression on Key and IV.
12. However if attacker sets 13 Type 1 conditions $v_8 = 0, v_9 = 0, v_{10} = 0, v_{19} = 0, v_{28} = 0, v_{29} = 0, v_{31} = 0, v_{44} = 0, v_{49} = 0, v_{51} = 0, v_{52} = 0, v_{53} = 0, v_{57} = 0$ and two Type 2 conditions

    $$\begin{aligned} C_4 : v_6 &= k_7 \oplus k_8 \oplus k_{10} \oplus k_{16} \oplus k_{37} \oplus k_{49} \oplus k_{62} \oplus 1, \\ C_5 : v_7 &= v_{20} \oplus v_{23} \oplus v_{32} \oplus v_{45} \oplus f_2(K), \end{aligned}$$

    where $f_2(K)$ is a polynomial over Key of degree 15 and 2365 monomials, $z_{40} = z_{40}$.

Attack Idea

Total of 27 Type 1 conditions and 5 Type 2 conditions $C_1, \dots, C_5$. Hence IV space is reduced to $\{0,1\}^{64-27} = \{0,1\}^{37}$.

Corresponding to 5 Type 2 conditions, attacker divides this space into $2^5 = 32$ partitions.

That is since there are 5 expressions on unknown Key, attacker chooses all 32 options. Among these 32 options, one must be correct.

Attack idea

Knellwolf et al. observed experimentally for the correct guess on 5 key expressions, $z_{97} \oplus z_{97}$ is more likely to be zero.

This gives a distinguisher on Grain v1 for reduced round.

Five Type 2 conditions are crucial for Key recovery.

Attack idea

Knellwolf et al. observed experimentally for the correct guess on 5 key expressions, $z_{97} \oplus z_{97}$ is more likely to be zero.

This gives a distinguisher on Grain v1 for reduced round.

Five Type 2 conditions are crucial for Key recovery.

Differential on v_{61}: Banik's attack for 105 round

Attack for 106 rounds

Differential on v_{62}

1. For $i = 0, \ldots, 15$, $z_i = z_{i}$.
2. When $i = 16$, set $v_{19} = v_{41} = 1, v_{46} = 0$ and $v_0 = k_1 \oplus k_2 \oplus k_4 \oplus k_{10} \oplus k_{31} \oplus k_{43} \oplus k_{56} \oplus v_3 \oplus v_{13} \oplus v_{23} \oplus v_{25} \oplus v_{38} \oplus v_{51}$.
3. For $i = 17, \ldots, 26$, z_i will be always equal to z_{i}.
4. When $i = 27$, z_{27} will be always different from z_{27}.

5. z_i will be always equal to z_i for $i = 28, \ldots, 33$.
6. When $i = 34$, $z_{34} \oplus z_{34}$ will be an algebraic expression on Key and IV.

   17 Type 1 conditions

   $v_2 = v_{15} \oplus v_{18} \oplus v_{25} \oplus v_{31} \oplus v_{40} \oplus v_{53} \oplus v_{56} \oplus v_{59}$, $v_{63} = 0$, $v_{14} = v_{24} \oplus v_{39} \oplus v_{52}$, $v_{13} = v_{23} \oplus v_{38} \oplus v_{51}$, $v_{17} = v_{42}$, $v_{43} = 0$, $v_{47} = 0$, $v_{38} = 0$, $v_4 = 0$, $v_1 = 0$, $v_5 = 0$, $v_{20} = 0$, $v_{21} = 0$, $v_{26} = 0$, $v_{27} = 0$, $v_{37} = 0$, $v_{48} = 0$ and one Type 2 condition

   $$C_2 : v_{59} \quad = \quad f_1(K),$$

   where $f_1(K)$ is a polynomial over Key of degree 16 and 9108 monomials, $z_{34} = z_{34}$.

7. $z_i = z_i$ for $i = 35, 36$.
8. When $i = 37$, again $z_{37} \oplus z_{37}$ will be an algebraic expression on Key and IV. However if attacker sets 7 Type 1 conditions $v_{15} = v_{18} \oplus v_{25} \oplus v_{31} \oplus v_{53} \oplus v_{55} \oplus v_{56} \oplus v_{59}, v_{16} = v_{54}, v_{49} = 1, v_{28} = 0, v_6 = 0, v_{50} = 0, v_{23} = v_{45}$
   and two Type 2 conditions
   $$\begin{aligned} C_3 : v_3 &= k_4 \oplus k_5 \oplus k_7 \oplus k_{13} \oplus k_{34} \oplus k_{46} \oplus k_{59} \oplus k_{66} \\ C_4 : v_7 &= v_{29} \oplus f_2(K), \end{aligned}$$
   where $f_2(K)$ is a polynomial over Key of degree 15 and 1535 monomials, $z_{37} = z_{37}$.
9. $z_i = z_i$ for $i = 38, 39$.
10. If we set 7 Type 1 conditions $v_{58} = v_7, v_{57} = v_{44} \oplus v_{29}, v_{51} = 0, v_{52} = 0, v_{10} = 0, v_{32} = 0, v_{53} = 0$ and 2 Type 2 conditions
    $$\begin{aligned} C_5 : v_9 &= k_7 \oplus k_8 \oplus k_{10} \oplus k_{16} \oplus k_{37} \oplus k_{49} \oplus k_{62} \oplus v_{31} \\ C_6 : v_8 &= f_3(K), \end{aligned}$$
    where $f_3(K)$ is a polynomial over Key of degree 15 and 1572 monomials, $z_{40} = z_{40}$.

Attack up to 106 rounds

Type 1: 34

Type 2: 6

IV space is reduced to $\{0,1\}^{64-34} = \{0,1\}^{30}$

Experiment shows success probability of the distinguisher is 63%

Thank You!