# Some results on Related Key-IV pairs of Grain

**Subhadeep Banik**, Subhamoy Maitra and Santanu Sarkar

Applied Statistics Unit
Indian Statistical Institute, Kolkata
s.banik_r@isical.ac.in

# Grain Family of Stream Ciphers

# Grain Family

- Proposed by Hell et al in 2005
- Part of E-stream's hardware portfolio
- Bit-oriented, Synchronous stream cipher
- The first version (v0) of the cipher was crypatanalysed
  1. A Distinguishing attack by Kiaei et. al (Ecrypt : 071).
  2. A State Recovery attack by Berbain et.al (FSE 2006).
- After this, the versions Grain v1, Grain 128, Grain 128a were proposed.

# General Structure of the Grain Family

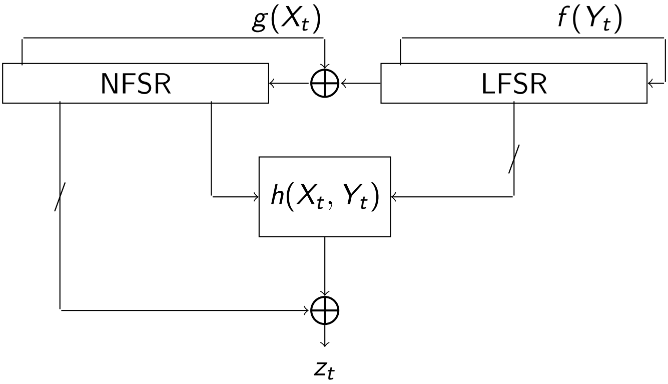



Figure: Structure of Grain v1

# Grain at a glance

| | Grain v1 | Grain-128 | Grain-128a |
|---|---|---|---|
| $n$ | 80 | 128 | 128 |
| $m$ | 64 | 96 | 96 |
| Pad | FFFF | FFFFFFFF | FFFFFFFE |
| $f(\cdot)$ | $y_{t+62} \oplus y_{t+51} \oplus y_{t+38}$ $\oplus y_{t+23} \oplus y_{t+13} \oplus y_t$ | $y_{t+96} \oplus y_{t+81} \oplus y_{t+70}$ $\oplus y_{t+38} \oplus y_{t+7} \oplus y_t$ | $y_{t+96} \oplus y_{t+81} \oplus y_{t+70}$ $\oplus y_{t+38} \oplus y_{t+7} \oplus y_t$ |
| $g(\cdot)$ | $x_{t+62} \oplus x_{t+60} \oplus x_{t+52}$ $\oplus x_{t+45} \oplus x_{t+37} \oplus x_{t+33}$ $x_{t+28} \oplus x_{t+21} \oplus x_{t+14}$ $x_{t+9} \oplus x_t \oplus x_{t+63}x_{t+60} \oplus$ $x_{t+37}x_{t+33} \oplus x_{t+15}x_{t+9}$ $x_{t+60}x_{t+52}x_{t+45} \oplus x_{t+33}$ $x_{t+28}x_{t+21} \oplus x_{t+63}x_{t+60}$ $x_{t+21}x_{t+15} \oplus x_{t+63}x_{t+60}$ $x_{t+52}x_{t+45}x_{t+37} \oplus x_{t+33}$ $x_{t+28}x_{t+21}x_{t+15}x_{t+9} \oplus$ $x_{t+52}x_{t+45}x_{t+37}x_{t+33}$ $x_{t+28}x_{t+21}$ | $y_t \oplus x_t \oplus x_{t+26} \oplus$ $x_{t+56} \oplus x_{t+91} \oplus x_{t+96} \oplus$ $x_{t+3}x_{t+67} \oplus x_{t+11}x_{t+13}$ $\oplus x_{t+17}x_{t+18} \oplus x_{t+27}x_{t+59}$ $\oplus x_{t+40}x_{t+48} \oplus x_{t+61}$ $x_{t+65} \oplus x_{t+68}x_{t+84}$ | $y_t \oplus x_t \oplus x_{t+26} \oplus$ $x_{t+56} \oplus x_{t+91} \oplus x_{t+96} \oplus$ $x_{t+3}x_{t+67} \oplus x_{t+11}x_{t+13}$ $\oplus x_{t+17}x_{t+18} \oplus x_{t+27}x_{t+59}$ $\oplus x_{t+40}x_{t+48} \oplus x_{t+61}$ $x_{t+65} \oplus x_{t+68}x_{t+84}$ $\oplus x_{t+88}x_{t+92}x_{t+93}x_{t+95}$ $\oplus x_{t+22}x_{t+24}x_{t+25} \oplus$ $x_{t+70}x_{t+78}x_{t+82}$ |
| $h(\cdot)$ | $y_{t+3}y_{t+25}y_{t+46} \oplus y_{t+3}$ $y_{t+46}y_{t+64} \oplus y_{t+3}y_{t+46}$ $x_{t+63} \oplus y_{t+25}y_{t+46}x_{t+63} \oplus$ $y_{t+46}y_{t+64}x_{t+63} \oplus y_{t+3}$ $y_{t+64} \oplus y_{t+46}y_{t+64} \oplus y_{t+64}$ $x_{t+63} \oplus y_{t+25} \oplus x_{t+63}$ | $x_{t+12}x_{t+95}y_{t+95} \oplus x_{t+12}$ $y_{t+8} \oplus y_{t+13}y_{t+20} \oplus x_{t+95}$ $y_{t+42} \oplus y_{t+60}y_{t+79}$ | $x_{t+12}x_{t+95}y_{t+94} \oplus x_{t+12}$ $y_{t+8} \oplus y_{t+13}y_{t+20} \oplus x_{t+95}$ $y_{t+42} \oplus y_{t+60}y_{t+79}$ |
| $z_t$ | $x_{t+1} \oplus x_{t+2} \oplus x_{t+4} \oplus$ $x_{t+10} \oplus x_{t+31} \oplus x_{t+43}$ $x_{t+56} \oplus h$ | $x_{t+2} \oplus x_{t+15} \oplus x_{t+36} \oplus$ $x_{t+45} \oplus x_{t+64} \oplus x_{t+73}$ $\oplus x_{t+89} \oplus y_{t+93} \oplus h$ | $x_{t+2} \oplus x_{t+15} \oplus x_{t+36} \oplus$ $x_{t+45} \oplus x_{t+64} \oplus x_{t+73}$ $\oplus x_{t+89} \oplus y_{t+93} \oplus h$ |

# Keystream generating routines

- **Key Loading Algorithm (KLA)**
  - $n$-bit key $K \rightarrow$ NFSR
  - $m$-bit ($m < n$) $IV \rightarrow$ LFSR[0]...LFSR[m-1]
  - $p = n - m$ bit pad $P \rightarrow$ LFSR[m]...LFSR[n-1]
- **Key Schedule Algorithm (KSA)**
  - For $2n$ clocks, output of $h'$ is XOR-ed to the LFSR and NFSR update functions
  - $y_{t+n} = f(Y_t) + z_t$ and $x_{t+n} = y_t + z_t + g(X_t)$
- **Pseudo Random bitstream Generation Algorithm (PRGA)**
  - The feedback is discontinued
  - $y_{t+n} = f(Y_t)$ and $x_{t+n} = y_t + g(X_t)$
  - $z_t = h'(X^t, Y^t)$

# Cryptanalytic Results on Grain

- After the KSA the LFSR may become all zero (Zhang and Wang: Eprint 2009/109) and if so it will remain in this state forever.
  1. Start with a random PRGA initial state $B_0||0^n$. ($B_0 \in \{0,1\}^n$)
  2. Since KSA is invertible, run KSA backwards to get the state $B||S||T$ ($B \in \{0,1\}^n, S \in \{0,1\}^m, T \in \{0,1\}^{n-m}$)
  3. If $T = P$, then $B, S$ is one such weak Key-IV.
  4. Probability of Success : Once in $2^{n-m}$ trials.
- For such weak Key-IVs: Distinguisher in Grain
  1. Grain v0 : $2^{12.6}$ Keystream bits
  2. Grain v1 : $2^{44.2}$ Keystream bits
  3. Grain v1 : $2^{86}$ Keystream bits
- If the LFSR does not become all zero then the internal state has a period which is a multiple of $2^n - 1$ (Hu et al. CACR 2011)

# Cryptanalytic Results on Grain

- Cube Attack on Grain-128 : Dinur/Shamir (FSE 2011)
- Fault Attack Grain-128 : Berzati et al. (IEEE HOST 2009), Karmakar et. al. (Africacrypt 2011)
- Slide Attack on Grain v1 : De Canniere et. al. (Africacrypt 2008)

# Related Key-IV Pairs

# Related Key-IV Pairs: Basic Idea

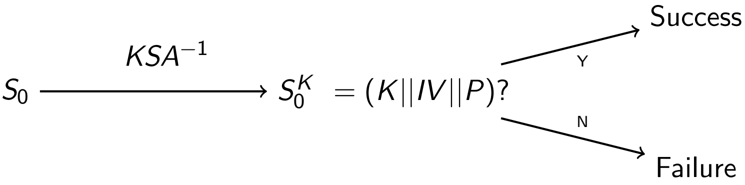
Given a Key-IV $(K, IV)$ in Grain, one can efficiently obtain another Key-IV $(K', IV')$ so that the generated output key-streams are

- almost similar in the initial part or
- exact shifts of each other throughout the key-stream generation.

We call these Key-IV pairs "related".

# Related Key-IV pair in Grain: Algorithm Idea

- Both the **KSA** and **PRGA** routines in the grain family are reversible.
- The inital state vector of the **PRGA** is of $2n$ bits.
- Take any $S_0 \in_R \{0,1\}^{2n}$ and compute $S_0^K =$**KSA**$^{-1}(S_0)$.
- If $S_0^K$ is of the form $K||IV||P$ then $S_0$ is a valid initial state of the **PRGA**.
- Since pad $P$ is of $p$-bits, performing this experiment $2^p$ times is expected to yield one valid state.



# Related Key-IV pair in Grain

- Consider two initial states $S_0, S_{0,\Delta}$ such that $S_0 \oplus S_{0,\Delta} = y_{n-1}$
- Then by the analysis of the differential trails, the following can be observed
  - In Grain v1, the states produce identical output bits in 75 out of initial 96 keystream bits, at rounds

$$k \in [0,95] \setminus \{15,33,44,51,54,57,62,69,72,73,75,76,80,82,83,87,90,91,93,94,95\}$$

  - In Grain-128, the states produce identical output bits in 112 out of initial 160 keystream bits, at rounds

$$k \in [0,159] \setminus \{32,34,48,64,66,67,79,80,81,85,90,92,95,96,98,99,106,107,112,114,117,119,122,124,125,126,128,130,131,132,138,139,142,143,144,145,146,148,149,150,151,153,154,155,156,157,158,159\}$$

  - Similar results in Grain-128a.

# How to obtain related Key-IV pairs

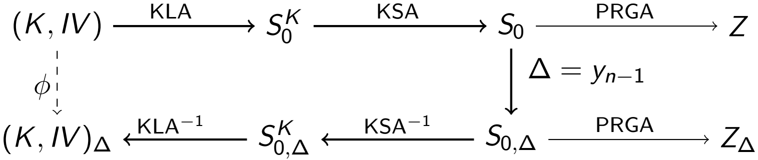



Figure: Construction of the Related Key-IV function.

It is expected that $2^p$ invocations of this routine will yield a valid related Key-IV pair.

# Example

| *Grain* | *Key* | *IV* | *S* |
|---|---|---|---|
| $v1$ | bf6689cead5ece39758c | bdfa0025ac44a4fe | 52f71a93959ff900ffa9<br>15c61a47522fffaf8a77 |
| | e166bc5aa1952733ab2a | aed6838b948399a0 | 52f71a93959ff900ffa9<br>15c61a47522fffaf8a76 |
| 128 | 60287a5ecf99724716a83bf81a9735cf | 62b6f21aa5d6511f43cb51f0 | 7bb026436bc29b585e676e90961830e0<br>7e86e48d2370eeda43ddd098a4b3e7d2 |
| | dc260a0042112620772443311b933f08 | c026cf1526950adee08fbe14 | 7bb026436bc29b585e676e90961830e0<br>7e86e48d2370eeda43ddd098a4b3e7d3 |
| 128$a$ | 54fd23a7e54f8fb096a45189b65f0fff | 5a7fb7b76c303592b74422c3 | 36a0589046e177ae325a4b60154084cd<br>fc74e3c99cad9a2f2fcbf394d44f15fd |
| | 1c21c39e9404b1c347ee8dc594f3d040 | 9db86204107b9ac4d401cc2d | 36a0589046e177ae325a4b60154084cd<br>fc74e3c99cad9a2f2fcbf394d44f15fc |

# Single Key-IV with multiple Differentials

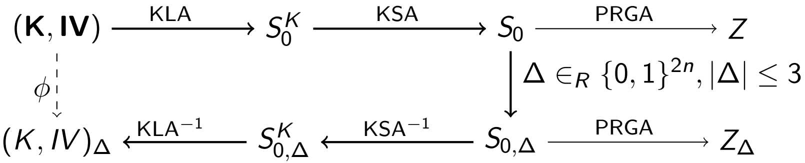



Figure: Construction of the Related Key-IV function.

1. Fix a randomly chosen Key-IV pair $(\mathbf{K},\mathbf{IV})$.
2. It is expected that a trial with $2^p$ randomly chosen differentials of weight at most 3, will yield a valid related Key-IV pair.

# Example: Grain v1

| *Key* | *IV* | *S* |
|---|---|---|
| bde8d3c319ff4d234706 | f363180e262b6cc5 | a74e7c7799b00f3c94e1 bf0315b589691f82085a |
| b223a57ce1578708677a | 371d2d93363b014b | a74e7c7799b00f3c94e1 bf0315b589681582085a |

$\Delta = \{y_{47}, y_{52}, y_{54}\}$ and 55 of the first 80 keystream bits produced by both the Key-IV pairs are equal.

# Key-IV pairs producing Shifted Keystream

- Each Key-IV in Grain is expected to have another related Key-IV that produces shifted Keystream
- Idea of the algorithm
  - Start with a Key-IV $K||IV$ and run **KSA** to get $S_0$ initial PRGA state
  - Check if any $i^{th}$ state of the PRGA $S_i$ is also a valid PRGA initial state
  - That is check if $S_i^K = \mathbf{KSA}^{-1}(S_i) = K_i||IV_i||P$
  - If yes then $K, IV$ and $K_i, IV_i$ produce $i$-round shifted keystream
- It is expected that $i \approx 1 \rightarrow 2^p$ will yield one related pair.

# How to obtain related Key-IV pair

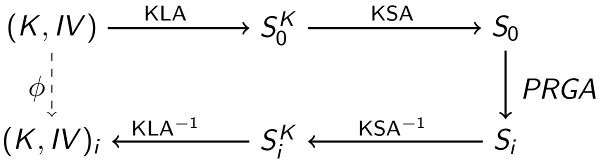



Figure: Construction of the Related Key-IV function.

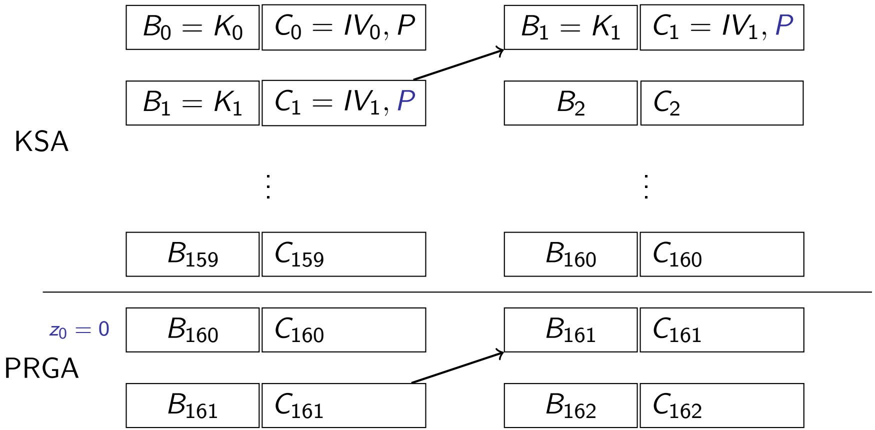
# Example

| Grain | Key-IV | Key-IV | Shift |
|---|---|---|---|
| v1 | `4567b66f51b956542319` `96b81c6c97ed8853` | `f0f9d3bc4f2d0001e11d` `67e95df014caf50a` | 72343 $\approx 2^{16.14}$ |
| 128 | `fca5c3705794a26266f58d06f7e87b9f` `cf74e27475fc36e159069606` | `990aa66d1d816db4d81cf42ab62937b2` `54345cb47fed0997dc1a73d4` | 236757088 $\approx 2^{27.82}$ |
| 128a | `2b953abc7427e1c260b2995039766123` `81a25f710a9a24aed1644d9f` | `01f8cda5aa35dece20154a986e24e4d8` `4bf4f64d462d379453928a7a` | 2642097831 $\approx 2^{31.30}$ |

# Shifted Keystreams with small shifts

- Idea first given by De Cannière et al.[**Africacrypt 08**]
- Let the initial KSA state be $B_0 = K_0$ and $C_0 = IV_0||P$. ($P =$`0xFFFF` for Grain v1 and `0xFFFF FFFF` for Grain-128)
- After the first round of KSA, state is $B_1||C_1$.
- If $C_1 = IV_1||P$ for $IV_1 \in \{0, 1\}^m$, then $B_1||C_1 = K_1||IV_1||P$ is another valid initial state of the KSA.
- If KSA starts with $B_1||C_1$ instead of $B_0||C_0$, it may produce one bit-shifted key-stream.
- Added sufficiency condition : The $1^{st}$ output bit produced by $B_0||C_0$ during the PRGA must be 0. This ensures that the $1^{st}$ PRGA state of $B_1||C_1$,equals $2^{nd}$ PRGA state using $(B_0, C_0)$.

# Shifted Keystreams with small shifts



# Conditions

- Both $C_1 = IV_1||P$ and $z_0 = 0$ for 1 bit shifted stream $\rightarrow$ Probability $\frac{1}{4}$.
- Similarly for $i$-bit-shifted streams the $2i$ conditions
  - A $C_i = IV_i||P$ for $i = 1, 2, \ldots, i$
  - B $z_{i-1} = 0$ for $i = 1, 2, \ldots, i$
- Probability $(\frac{1}{4})^i$ for randomly chosen Key-IVs.
- Can be improved to $(\frac{1}{2})^i$ by characterizing Key-IVs that satisfy [A].

# Algorithm

**Input**: $B_0, C_0$
**Output**: $B_i, C_i$, for $i = 1$ to $u$

**for** $i = 1$ *to* $u$ **do**

$y^{[i]} \leftarrow f(Y^{[i-1]})$ where $Y^{[i-1]} = y_0^{[i-1]}, y_1^{[i-1]}, \ldots, y_{n-1}^{[i-1]}$

$x^{[i]} \leftarrow y_0^{[i-1]} + g(X^{[i-1]})$ where $X^{[i-1]} = x_0^{[i-1]}, x_1^{[i-1]}, \ldots, x_{n-1}^{[i-1]}$

$z^{[i]} \leftarrow \bigoplus_{a \in A} x_a^{[i-1]} + h(X^{[i-1]}, Y^{[i-1]})$

$B_i = (x_0^{[i]}, x_1^{[i]}, \ldots, x_{n-2}^{[i]}, x_{n-1}^{[i]}) \leftarrow (x_1^{[i-1]}, x_2^{[i-1]}, \ldots, x_{n-1}^{[i-1]}, x^{[i]} + z^{[i]})$

$C_i = (y_0^{[i]}, y_1^{[i]}, \ldots, y_{n-2}^{[i]}, y_{n-1}^{[i]}) \leftarrow (y_1^{[i-1]}, y_2^{[i-1]}, \ldots, y_{n-1}^{[i-1]}, y^{[i]} + z^{[i]})$

**end**

**Algorithm 1**: Obtaining Grain KSA Relations

# The Solution

- Solve together algebraic equations of the form $y^{[i]} + z^{[i]} = 1$ for $i = 1, 2 \ldots$
- Using SAGE computer algebra software, solutions for upto $i = 1, 2, \ldots, 12$ could be found for Grain v1, 128.
- Attack does not work on Grain-128a because of the nature of the pad $P$ used in the cipher.

# Example

| Grain | Key-IV | Key-IV | Shift |
|---|---|---|---|
| v1 | 8ca87875d334c9de694a<br>5246f9d65f5eaef9 | 87875d334c9de694abbc<br>6f9d65f5eaef9fff | 12 |
| 128 | b8d3dac27cbfeae545a508e9e551c095<br>bba4d4a0465a4448627e22ed | 3dac27cbfeae545a508e9e551c095753<br>4d4a0465a4448627e22edfff | 12 |

# Thank You