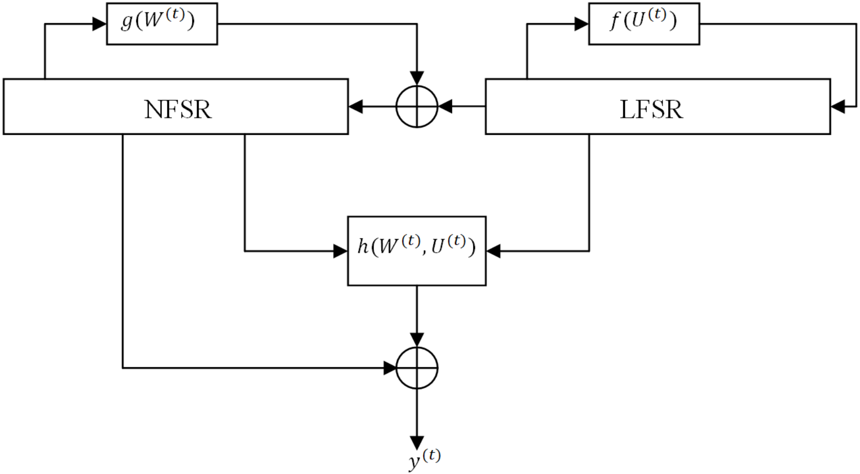
Fast correlation attack for GRAIN-128AEAD with fault

Katyshev S.U., Malov M.U.

CTCrypt, 2023.06.09

Content

Grain family



Grain-128AEAD

Relation for LFSR:

$$u_{127}^{(t+1)} = u_0^{(t)} \oplus u_7^{(t)} \oplus u_{38}^{(t)} \oplus u_{70}^{(t)} \oplus u_{81}^{(t)} \oplus u_{96}^{(t)} = \Sigma_u(U^{(t)}).$$

Relation for NFSR:

$$\begin{aligned} w_{127}^{(t+1)} = u_0^{(t)} \oplus w_0^{(t)} \oplus w_{26}^{(t)} \oplus w_{56}^{(t)} \oplus w_{91}^{(t)} \oplus w_{96}^{(t)} \oplus w_3^{(t)} w_{67}^{(t)} \oplus \\ \oplus w_{11}^{(t)} w_{13}^{(t)} \oplus w_{17}^{(t)} w_{18}^{(t)} \oplus w_{27}^{(t)} w_{59}^{(t)} \oplus w_{40}^{(t)} w_{48}^{(t)} \oplus w_{61}^{(t)} w_{65}^{(t)} \oplus w_{68}^{(t)} w_{84}^{(t)} \\ \oplus w_{22}^{(t)} w_{24}^{(t)} w_{25}^{(t)} \oplus w_{70}^{(t)} w_{78}^{(t)} w_{82}^{(t)} \oplus w_{88}^{(t)} w_{92}^{(t)} w_{93}^{(t)} w_{95}^{(t)} = u_0^{(t)} \oplus \Sigma_w(W^{(t)}). \end{aligned}$$

Output function:

$$y^{(t)} = h(w_{12}^{(t)}, u_8^{(t)}, u_{13}^{(t)}, u_{20}^{(t)}, w_{95}^{(t)}, u_{42}^{(t)}, u_{60}^{(t)}, u_{79}^{(t)}, u_{94}^{(t)}) \oplus u_{93}^{(t)} \oplus \sum_{j \in A} w_j^{(t)},$$

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

Grain family

Cipher	Attack	Complexity
Grain-V0, 2004	correlation	$T = 2^{84}, D = 2^{64}$
Grain-V1, 2006	fast correlation, 2018	$T = 2^{75}, D = 2^{77}$
Grain-128, 2006	dynamic cube, 2011	$T = 2^{84}, D = 2^{62}$
Grain-128a, 2011	fast correlation, 2018	$T = 2^{115}, D = 2^{114}$

Our results

Grain-128AEAD – fast correlation attack with fault $T = 2^{113}, D = 2^{113}$

Content

Some types of side-channel attacks

- Passive side-channel attacks
- Active side-channel attacks
- Invasive attacks
- Noninvasive attacks
- Data remanence attacks
- Fault attacks
- Differential fault attacks

Fault attacks

Basic consumptions in fault analysis

- The attacker is able to reset the system with the original Key-IV
- The attacker can inject a fault at any one random bit location
- The attacker has full control over the timing of fault injection

Main objectives:

- Finding location of fault
- Recovering key

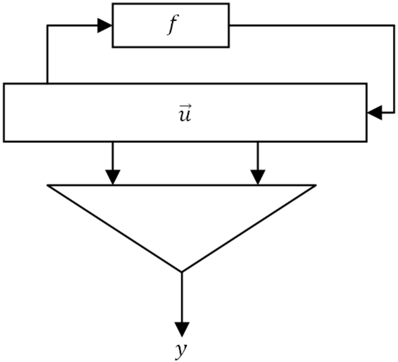
Fault attacks on Grain family

Main results

- A Differential Fault Attack on Grain-128a using MACs, 2012
- Differential Fault Attack against Grain family with very few faults and minimal assumptions, 2013
- Fault Analysis of Grain Family of Stream Ciphers, 2014
- Multi-Bit Differential Fault Analysis of Grain-128 with Very Weak Assumptions, 2014
- Combined Side-Channel and Fault Analysis Attack on Protected Grain Family of Stream Ciphers, 2015
- Phase-shift Fault Analysis of Grain-128, 2022

Content

Correlation analysis [Siegenthaler, 1985]



$\vec{u}^{(0)} = (u_0^{(0)}, ..., u_{n-1}^{(0)})$,
$\vec{y}^{(0)} = (y^{(0)}, ..., y^{(k)})$),
L_u, L_y — linear masks. :

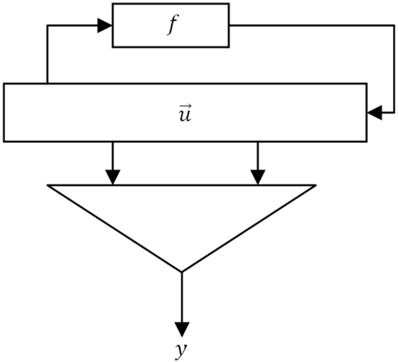
$$P\{\langle \vec{u}^{(0)}, L_u \rangle = \langle \vec{y}^{(0)}, L_y \rangle\} = q \neq \frac{1}{2},$$

Also we can use:
$\vec{y}^{(t)} = (y^{(t)}, ..., y^{(t+k)})$

$$P\{\langle \vec{u}^{(0)} \cdot S^t(f), L_u \rangle = \langle \vec{y}^{(t)}, L_y \rangle\} = q \neq \frac{1}{2},$$

$S(f)$ – the matrix for f.

Correlation analysis [Siegenthaler, 1985]



$\vec{u}^{(0)} = (u_0^{(0)}, \ldots, u_{n-1}^{(0)})$,
$\vec{y}^{(0)} = (y^{(0)}, \ldots, y^{(k)}))$,
L_u, L_y — linear masks. :

$$P\{\langle \vec{u}^{(0)}, L_u \rangle = \langle \vec{y}^{(0)}, L_y \rangle\} = q \neq \frac{1}{2},$$

Also we can use:
$\vec{y}^{(t)} = (y^{(t)}, \ldots, y^{(t+k)})$

$$P\{\langle \vec{u}^{(0)} \cdot S^t(f), L_u \rangle = \langle \vec{y}^{(t)}, L_y \rangle\} = q \neq \frac{1}{2},$$

$S(f)$ – the matrix for f.

Complexity: $O(N2^n)$

Fast correlation attack [Meier, Staffelbach, 1989]

Instead statistic

$$T(\vec{u}^{(0)}) = \sum_{t=0}^{N-1} \mathrm{Ind}\{\langle \vec{u}^{(0)}, L_u \cdot \big(S^t(f)\big)^T \rangle = \langle \vec{y}^{(t)}, L_y \rangle\},$$

Fast correlation attack [Meier, Staffelbach, 1989]

Instead statistic

$$T(\vec{u}^{(0)}) = \sum_{t=0}^{N-1} \mathrm{Ind}\{\langle \vec{u}^{(0)}, L_u \cdot \big(S^t(f)\big)^T \rangle = \langle \vec{y}^{(t)}, L_y \rangle\},$$

We can use statistic

$$\nu(\vec{u}^{(0)}) = \sum_{t=0}^{N-1} (-1)^{\langle \vec{u}^{(0)}, L_u \cdot \left(S^t(f)\right)^T \rangle \oplus \langle \vec{y}^{(t)}, L_y \rangle} =$$

$$= \sum_{\vec{x} \in \{0,1\}^n} \left(\sum_{t \in \{0,\dots,N-1 | L_u \cdot (S^t(f))^T = \vec{x}\}} (-1)^{\langle \vec{y}^{(t)}, L_y \rangle} \right) (-1)^{\langle \vec{u}^{(0)}, \vec{x} \rangle}.$$

Fast correlation attack [Meier, Staffelbach, 1989]

Instead statistic

$$T(\vec{u}^{(0)}) = \sum_{t=0}^{N-1} \mathrm{Ind}\{\langle \vec{u}^{(0)}, L_u \cdot \left(S^t(f)\right)^T \rangle = \langle \vec{y}^{(t)}, L_y \rangle\},$$

We can use statistic

$$\nu(\vec{u}^{(0)}) = \sum_{t=0}^{N-1} (-1)^{\langle \vec{u}^{(0)}, L_u \cdot \left(S^t(f)\right)^T \rangle \oplus \langle \vec{y}^{(t)}, L_y \rangle} =$$

$$= \sum_{\vec{x} \in \{0,1\}^n} \left(\sum_{t \in \{0,\ldots,N-1 | L_u \cdot (S^t(f))^T = \vec{x}\}} (-1)^{\langle \vec{y}^{(t)}, L_y \rangle} \right) (-1)^{\langle \vec{u}^{(0)}, \vec{x} \rangle}.$$

Walsh-Hadamard coefficient for $\nu(\vec{u}^{(0)})$:

$$\omega(\vec{x}) = \sum_{t \in \{0,\ldots,N-1 | L_u \cdot (S^t(f))^T = \vec{x}\}} (-1)^{<\vec{y}^{(t)}, L_y>}$$

Fast correlation attack [Meier, Staffelbach, 1989]

Main steps:

1. Calculating the values of the Walsh-Hadamard coefficients

$$\omega(\vec{x}) = \sum_{t \in \{0,\ldots,N-1 | L_u \cdot (S^t(f))^T = \vec{x}\}} (-1)^{<\vec{y}^{(t)}, L_y>}$$

2. Using the fast Walsh-Hadamard algorithm (FWH) we find the values of statistics

$$\nu(\vec{u}^{(0)}) = \sum_{t=0}^{N-1} (-1)^{\langle \vec{u}^{(0)}, L_u \cdot \left(S^t(f)\right)^T \rangle \oplus \langle \vec{y}^{(t)}, L_y \rangle}$$

3. Finding statistics $\nu(\vec{u}^{(0)})$ with high bias

Fast correlation attack [Meier, Staffelbach, 1989]

Main steps:

1. Calculating the values of the Walsh-Hadamard coefficients

$$\omega(\vec{x}) = \sum_{t \in \{0,\ldots,N-1 | L_u \cdot (S^t(f))^T = \vec{x}\}} (-1)^{<\vec{y}^{(t)}, L_y>}$$

2. Using the fast Walsh-Hadamard algorithm (FWH) we find the values of statistics

$$\nu(\vec{u}^{(0)}) = \sum_{t=0}^{N-1} (-1)^{\langle \vec{u}^{(0)}, L_u \cdot \left(S^t(f)\right)^T \rangle \oplus \langle \vec{y}^{(t)}, L_y \rangle}$$

3. Finding statistics $\nu(\vec{u}^{(0)})$ with high bias

Complexity: $O(N + n2^n)$

Fast correlation attack. Reduced complexity

Reduce involved secret-key bits and calculate the values of the Walsh-Hadamard coefficients for subfunction

1. Use some linear masks L_u
   For example, $L_u \cdot \left(S^t(f)\right)^T = (0, ..., 0, *, ...*)$
2. Use some pair linear masks L_u, L'_u (partial birthday problem)
   For example, $L_u \cdot \left(S^t(f)\right)^T \oplus L'_u \cdot \left(S^{t'}(f)\right)^T = (0, ..., 0, *, ...*)$
3. Use party check equation [Todo,... 2018]
   For example, $\langle \vec{u}^{(0)}, L_u \cdot \left(S^t(f)\right)^T \rangle \rightarrow \langle \vec{u}', \vec{G} \rangle$

Fast correlation attack. Reduced complexity

Reduce involved secret-key bits and calculate the values of the Walsh-Hadamard coefficients for subfunction

1. Use some linear masks L_u
   For example, $L_u \cdot (S^t(f))^T = (0, ..., 0, *, ...*)$
2. Use some pair linear masks L_u, L'_u (partial birthday problem)
   For example, $L_u \cdot (S^t(f))^T \oplus L'_u \cdot \left(S^{t'}(f)\right)^T = (0, ..., 0, *, ...*)$
3. Use party check equation [Todo,... 2018]
   For example, $\langle \vec{u}^{(0)}, L_u \cdot (S^t(f))^T \rangle \to \langle \vec{u}', \vec{G} \rangle$

Complexity: $O(N + (n - \beta)2^{n-\beta})$

Fast correlation attack. Reduced complexity

Reduce involved secret-key bits and calculate the values of the Walsh-Hadamard coefficients for subfunction

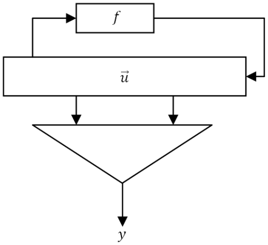
1. Use some linear masks L_u
   For example, $L_u \cdot (S^t(f))^T = (0, ..., 0, *, ...*)$
2. Use some pair linear masks L_u, L'_u (partial birthday problem)
   For example, $L_u \cdot (S^t(f))^T \oplus L'_u \cdot \left(S^{t'}(f)\right)^T = (0, ..., 0, *, ...*)$
3. Use party check equation [Todo,... 2018]
   For example, $\langle \vec{u}^{(0)}, L_u \cdot (S^t(f))^T \rangle \to \langle \vec{u}', \vec{G} \rangle$

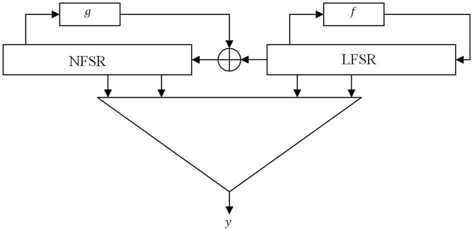
Complexity: $O(N + (n - \beta)2^{n-\beta})$

Complexity finding secret key for Grain-v1: 2^{75}

Content

Application for Grain128-AEAD





?????

$$P\{\langle \vec{u}, L_u \rangle = y\} \neq \frac{1}{2},$$

How apply to Grain Family?

Construct linear relation from LFSR bits only.

Application for Grain128-AEAD

Only odd bits are using for encryption!

$$
\begin{array}{lllllllll}
y^{(t)} & = u_{93}^{(t)} & \oplus w_{2}^{(t)} & \oplus w_{15}^{(t)} & \oplus w_{36}^{(t)} & \oplus w_{45}^{(t)} & \oplus \dots & \oplus h(\dots) \\
y^{(t+26)} & = u_{93}^{(t+26)} & \oplus w_{2}^{(t+26)} & \oplus w_{15}^{(t+26)} & \oplus w_{36}^{(t+26)} & \oplus w_{45}^{(t+26)} & \oplus \dots & \oplus h(\dots) \\
y^{(t+56)} & = u_{93}^{(t+56)} & \oplus w_{2}^{(t+56)} & \oplus w_{15}^{(t+56)} & \oplus w_{36}^{(t+56)} & \oplus w_{45}^{(t+56)} & \oplus \dots & \oplus h(\dots) \\
y^{(t+91)} & = u_{93}^{(t+91)} & \oplus w_{2}^{(t+91)} & \oplus w_{15}^{(t+91)} & \oplus w_{36}^{(t+91)} & \oplus w_{45}^{(t+91)} & \oplus \dots & \oplus h(\dots) \\
y^{(t+96)} & = u_{93}^{(t+96)} & \oplus w_{2}^{(t+96)} & \oplus w_{15}^{(t+96)} & \oplus w_{36}^{(t+96)} & \oplus w_{45}^{(t+96)} & \oplus \dots & \oplus h(\dots) \\
y^{(t+128)} & = u_{93}^{(t+128)} & \oplus w_{2}^{(t+128)} & \oplus w_{15}^{(t+128)} & \oplus w_{36}^{(t+128)} & \oplus w_{45}^{(t+128)} & \oplus \dots & \oplus h(\dots)
\end{array}
$$

Relation for NFSR:

$$w_{127}^{(t+1)} = u_0^{(t)} \oplus w_0^{(t)} \oplus w_{26}^{(t)} \oplus w_{56}^{(t)} \oplus w_{91}^{(t)} \oplus w_{96}^{(t)} \oplus [\text{Nonlinear part } W^{(t)}].$$

Application for Grain128-AEAD

Only odd bits are using for encryption!

$$
\begin{aligned}
y^{(t)} &= u_{93}^{(t)} \oplus w_{2}^{(t)} \oplus w_{15}^{(t)} \oplus w_{36}^{(t)} \oplus w_{45}^{(t)} \oplus \ldots \oplus h(\ldots)\\
y^{(t+26)} &= u_{93}^{(t+26)} \oplus w_{2}^{(t+26)} \oplus w_{15}^{(t+26)} \oplus w_{36}^{(t+26)} \oplus w_{45}^{(t+26)} \oplus \ldots \oplus h(\ldots)\\
y^{(t+56)} &= u_{93}^{(t+56)} \oplus w_{2}^{(t+56)} \oplus w_{15}^{(t+56)} \oplus w_{36}^{(t+56)} \oplus w_{45}^{(t+56)} \oplus \ldots \oplus h(\ldots)\\
y^{(t+91)} &= u_{93}^{(t+91)} \oplus w_{2}^{(t+91)} \oplus w_{15}^{(t+91)} \oplus w_{36}^{(t+91)} \oplus w_{45}^{(t+91)} \oplus \ldots \oplus h(\ldots)\\
y^{(t+96)} &= u_{93}^{(t+96)} \oplus w_{2}^{(t+96)} \oplus w_{15}^{(t+96)} \oplus w_{36}^{(t+96)} \oplus w_{45}^{(t+96)} \oplus \ldots \oplus h(\ldots)\\
y^{(t+128)} &= u_{93}^{(t+128)} \oplus w_{2}^{(t+128)} \oplus w_{15}^{(t+128)} \oplus w_{36}^{(t+128)} \oplus w_{45}^{(t+128)} \oplus \ldots \oplus h(\ldots)
\end{aligned}
$$

Relation for NFSR:

$$
w_{2}^{(t+128)} = u_{0}^{(t+2)} \oplus w_{2}^{(t)} \oplus w_{2}^{(t+26)} \oplus w_{2}^{(t+56)} \oplus w_{2}^{(t+91)} \oplus w_{2}^{(t+96)} \oplus [\text{Nonlinear part } W^{(t+2)}].
$$

Application for Grain128-AEAD

By summing we delete all linear variables from NFSR.

$$\sum_{j\in Z} y^{(t+j)} = \sum_{j\in Z} u_{93}^{(t+j)} \oplus \sum_{j\in Z} h(\dots) \oplus \sum_{i\in A} [\text{Nonlinear part } W^{(t_i)}]$$

with $Z = \{0, 26, 56, 96, 128\}$, $A = \{2, 15, 36, 45, 64, 73, 89\}$

Linear approximations

- The correlation between $h(\dots)$ and its linear approximation $\delta \in \{0, 2^{-4}, -2^{-4}\}$.
- Find linear approximation for [Nonlinear part $W^{(t_i)}$].
- Finally we find more 2^{24} Linear approximations with correlation not less 2^{-54}

Conclusion

Our attack result

The fast correlation attack will restore the true initial state
– with a probability equal to 0.9 with $\beta = 20$ fixed bits while the total complexity is $O(2^{113})$,
– with $\beta = 21$ the probability of successful completion of the attack is approximately 0.8, the total complexity is $O(2^{113})$.