

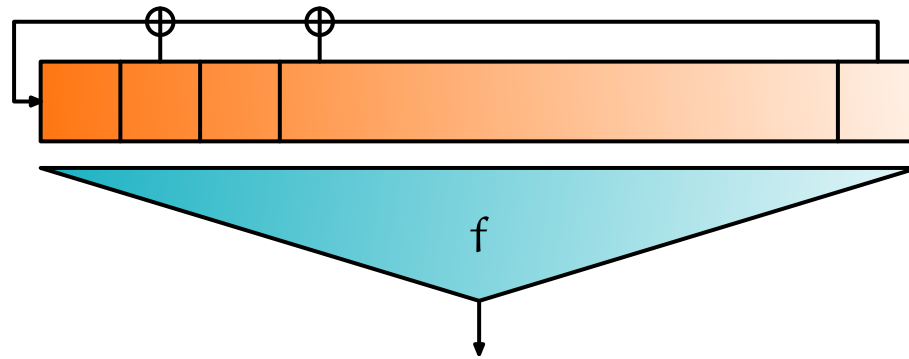
Algebraic Attacks against NFSR

Côme Berbain

January 9, 2008

Algebraic attacks

- introduced by Courtois and Meier and Ars and Faugère in 2003
- first applied against LFSR with Boolean function



- extended to other stream ciphers and block ciphers
- rely on solving a system of algebraic equations in the key bits (or an equivalent description)

Algebraic attacks

- classical attack: linearisation
 - ▶ every monomial is written as a new variable
 - ▶ Gauss elimination to solve the system
 - ▶ for equations of degree d in n variables, M equations are needed and the complexity is M^ω

$$M = \sum_{k=0}^d \binom{n}{k}$$

- Algebraic attacks tries to reduce the degree of the equations
- main technique: find annihilators

$$\forall x, f(x)g(x) = 0 \text{ or } (1 \oplus f(x))h(x) = 0$$

Fast Algebraic attacks

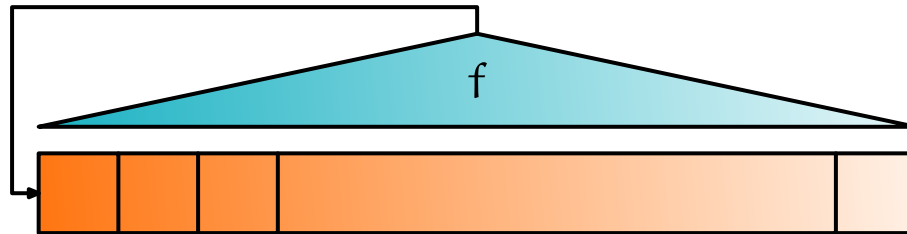
- instead of reducing the degree of a single equation, combine several equations

$$\forall x, f(x)g(x) = h(x)$$

- attack phases:
 - ▶ relation search step
 - ▶ precomputation step
 - ▶ substitution step
 - ▶ solving step

NFSR and algebraic attacks

- Algebraic attacks require
 - ▶ a large quantity of keystream bits
 - ▶ equations of fixed degree
- NFSR are believed to be resistant against algebraic attacks
 - ▶ NFSR produces equations with increasing degrees
 - ▶ keystream bits corresponding to a fixed (low) degree are scarce
- NFSR are combined with LFSR to keep interesting properties (period,...)

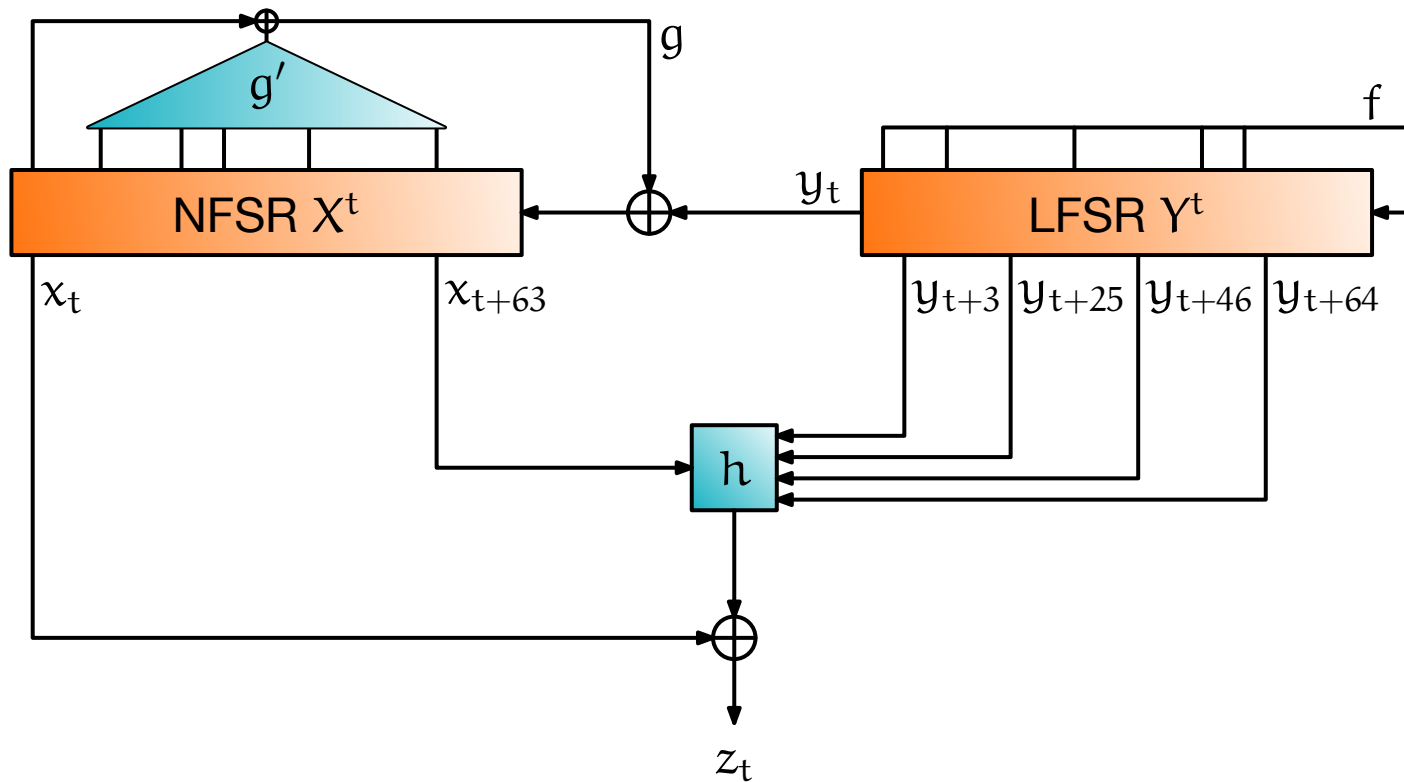


- Objective: mount algebraic attacks against certain NFSR and combination of NFSR and LFSR

Grain

Grain

- 80-bit Key, 64-bit IV, 160-bit internal state
- 80-bit NFSR $X^t = (x_t, x_{t+1}, \dots, x_{t+79})$
- 80-bit LFSR $Y^t = (y_t, y_{t+1}, \dots, y_{t+79})$
- nonlinear filtering function $h(X^t, Y^t)$



Grain Description

- The NFSR is perturbed by the LFSR:

$$\begin{aligned}x_{t+80} &= y_t \oplus g(x_t, x_{t+1}, \dots, x_{t+79}) \\ &= y_t \oplus x_t \oplus g'(x_{t+9}, \dots, x_{t+63})\end{aligned}$$

- The produced keystream bit:

$$\begin{aligned}z_t &= x_t \oplus h(y_{t+3}, y_{t+25}, y_{t+46}, y_{t+64}, x_{t+63}) \\ &= x_t \oplus x_{t+63}p_t \oplus q_t\end{aligned}$$

where p_t and q_t are the functions of $y_{t+3}, y_{t+25}, y_{t+46}, y_{t+64}$ given by:

$$p_t = 1 \oplus y_{t+64} \oplus y_{t+46}(y_{t+3} \oplus y_{t+25} \oplus y_{t+64}),$$

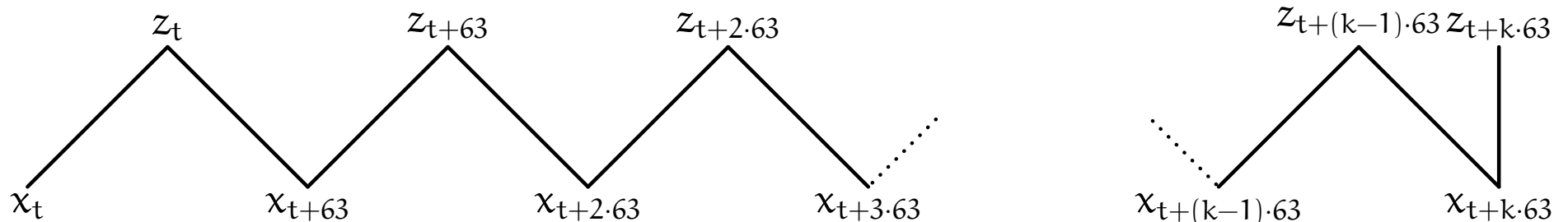
$$q_t = y_{t+25} \oplus y_{t+3}y_{t+46}(y_{t+25} \oplus y_{t+64}) \oplus y_{t+64}(y_{t+3} \oplus y_{t+46}).$$

Recovering the NFSR initial state

- Suppose the LFSR initial state is known, each keystream bit satisfies one equation of the form:

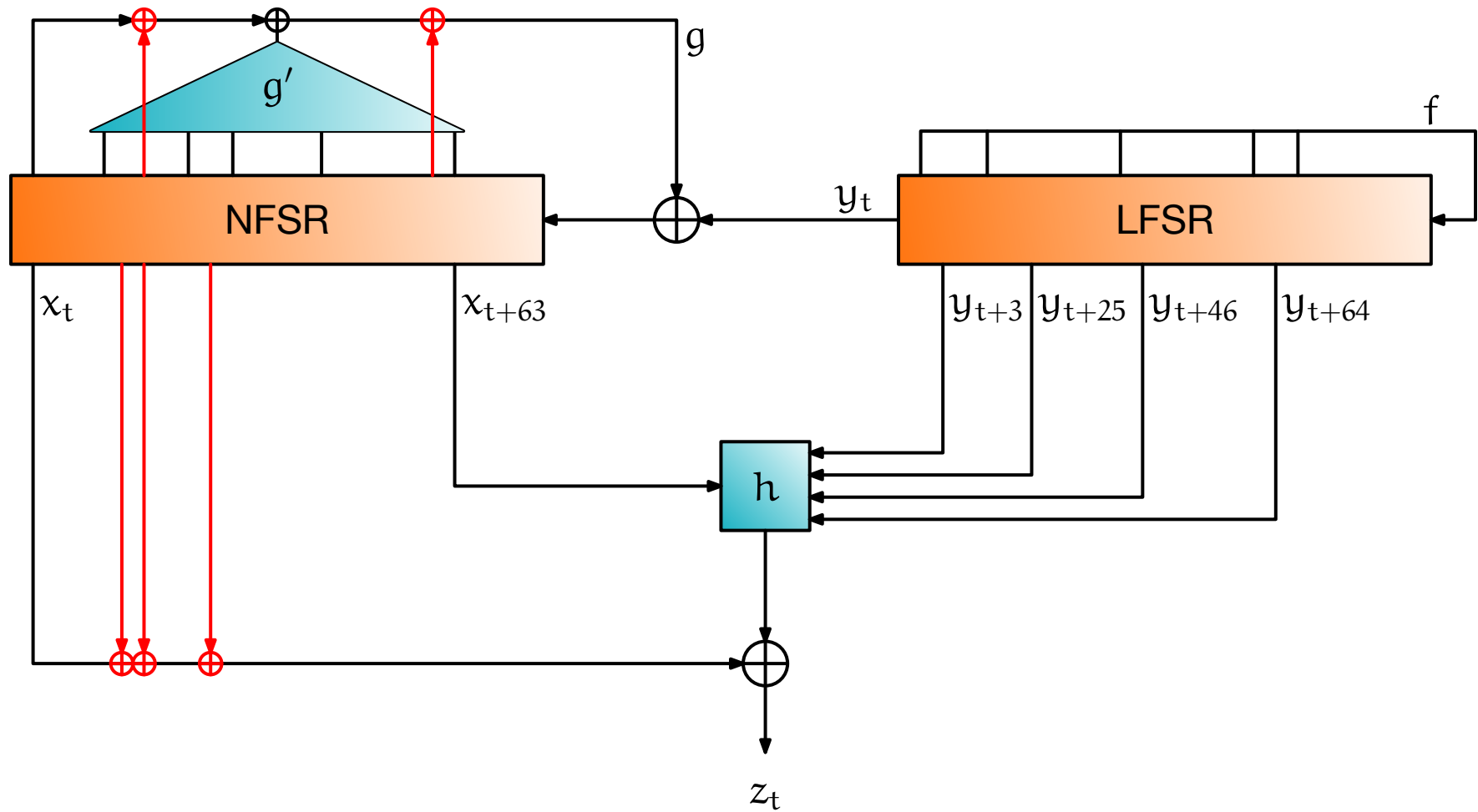
$$z_t = x_t (\oplus 1) \quad \text{or} \quad z_t = x_t \oplus x_{t+63} (\oplus 1)$$

- We can build chains for each bit of the initial state



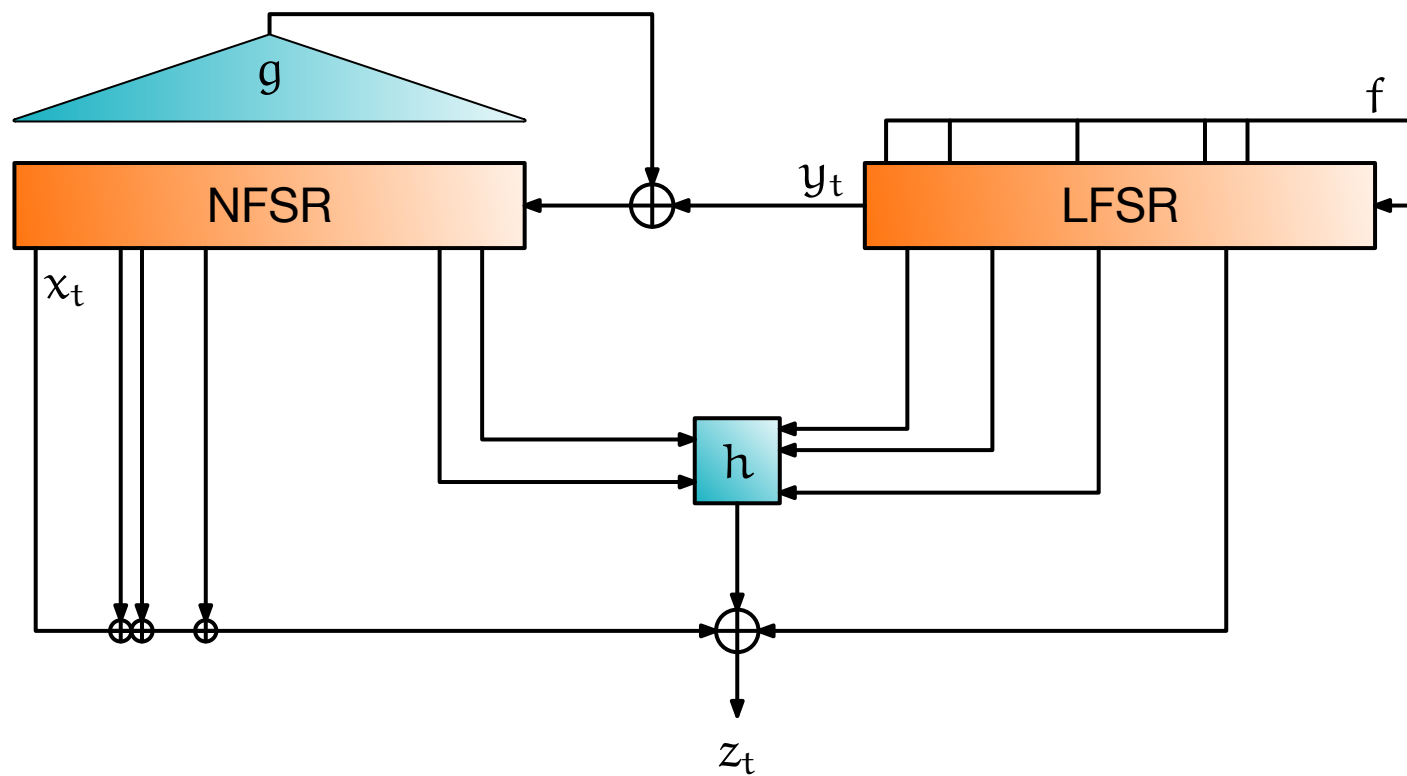
- A chain of length k appears with probability 2^{-k-1}
- This method provides us with all the initial state bits

Grain v1 [HJM05]



Grain 128 [HJM06]

- 128 bit NFSR $X^t = (x_t, x_{t+1}, \dots, x_{t+127})$
- 128 bit LFSR $Y^t = (y_t, y_{t+1}, \dots, y_{t+127})$
- two inputs from NFSR on h

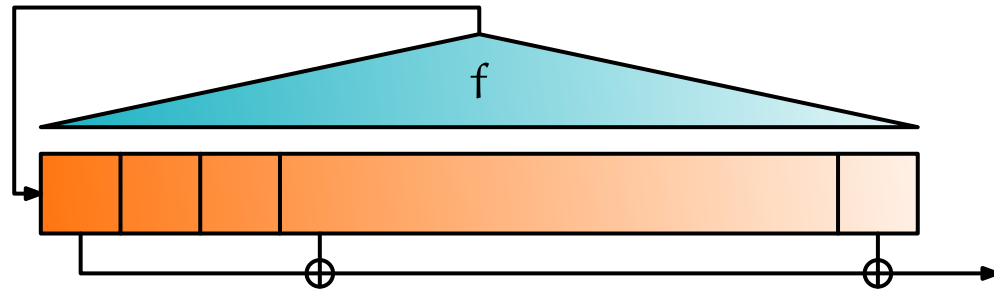


Algebraic Attacks

Attack against NFSR with linear output

- NFSR (x_0, \dots, x_{n-1}) with a non linear function f of degree d_f
- a very simple output function

$$g(y_0, \dots, y_{n-1}) = \bigoplus_{i=0}^{n-1} \alpha_i y_i$$



- x_i have increasing degrees due to function f
- equations from the keystream also have increasing degrees

$$z_t = \bigoplus_{i=0}^{n-1} \alpha_i x_{i+t}$$

Attack against NFSR with linear output

- our attack uses the same principle that the one on Grain
- we build chains of variables between x_t and the initial state (x_0, \dots, x_{n-1})

$$z_t = \bigoplus_{i=0}^{n-1} \alpha_i x_{i+t}$$

- i_k is the index of the k -highest non null coefficient α_i

$$x_{i_1+t} = z_t \oplus \bigoplus_{i=0}^{i_1-1} \alpha_i x_{i+t}$$

- on the same principle x_{i_2+t} can be expressed with $z_{t+i_2-i_1}$ and variables x_j with $j < i_2 + t$

Attack against NFSR with linear output

- we can write each x_i as a linear combination of the initial state and keystream bits
- replacing these relations into the expression of f gives equations of constant degree d_f

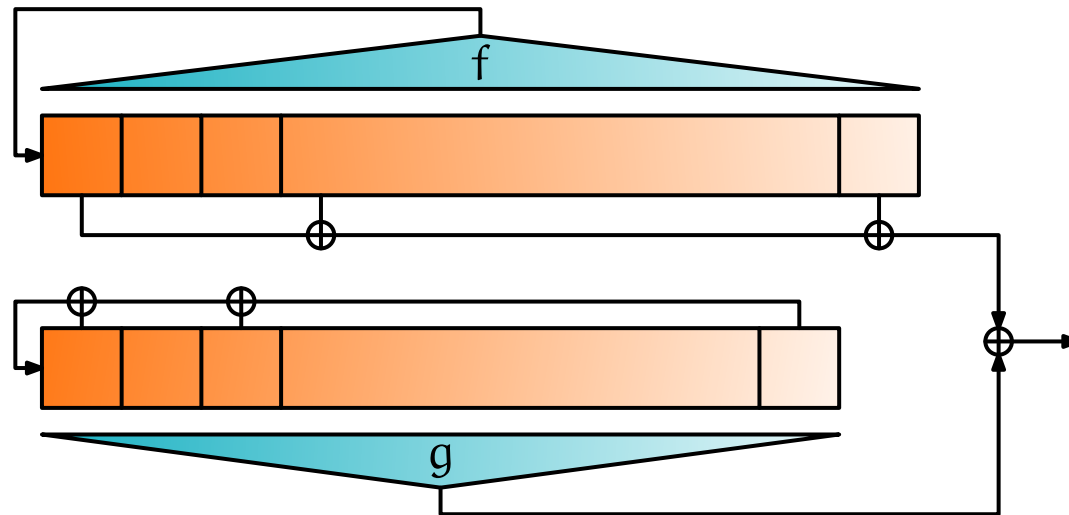
$$x_{n+t} = f(x_t, \dots, x_{n-1+t})$$

- we fall back on the classical case of a large number of equations of constant degree
- looking for annihilators of f can be useful

NFSR-LFSR Combination

- combine a NFSR with linear output with one or several LFSRs with non-linear output

$$z_t = \bigoplus_{i=0}^{n-1} \alpha_i x_{i+t} \oplus g(y_t, \dots, y_{t+m-1})$$



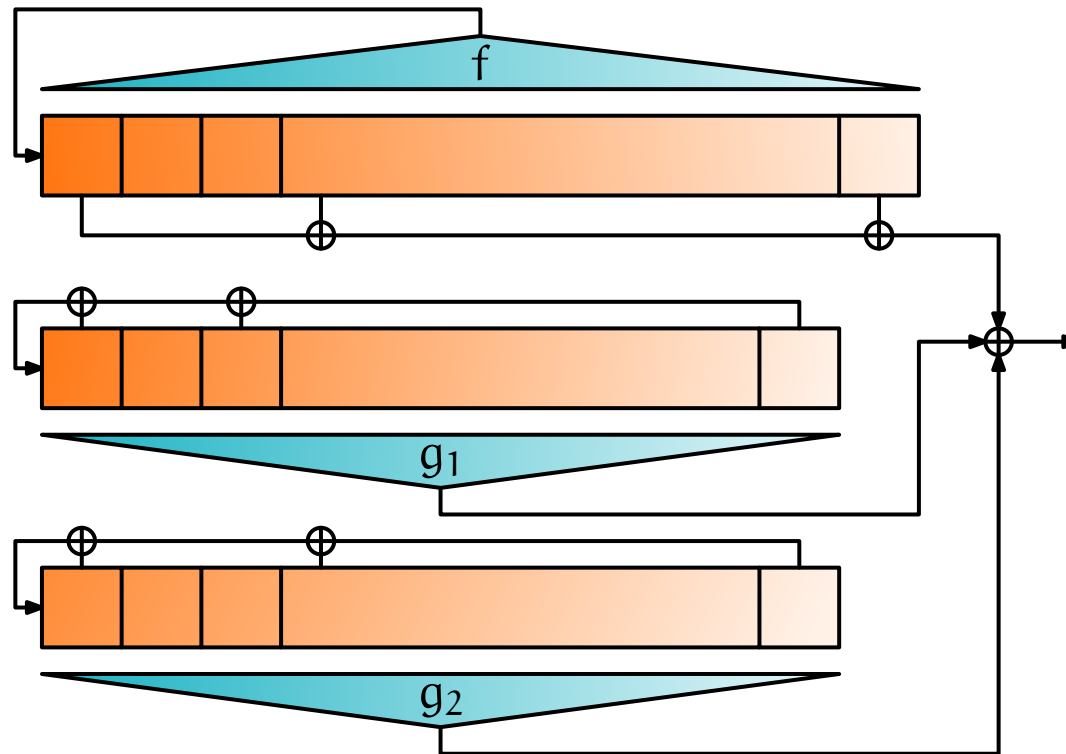
- we can use the same technique : build chain of variables

NFSR-LFSR Combination

- each x_t is now a linear function in variables x_i and a function of degree d_g in variables y_i with several terms of degree d_g
- an extra term of degree d_g appears for each new ring of the chain, i.e. new intermediate variable x_i
- replacing these relations into the expression of f gives equations of constant degree $d_f \cdot d_g$
- annihilators of f are useful

NFSR-LFSR Combination

- considering p different LFSRs

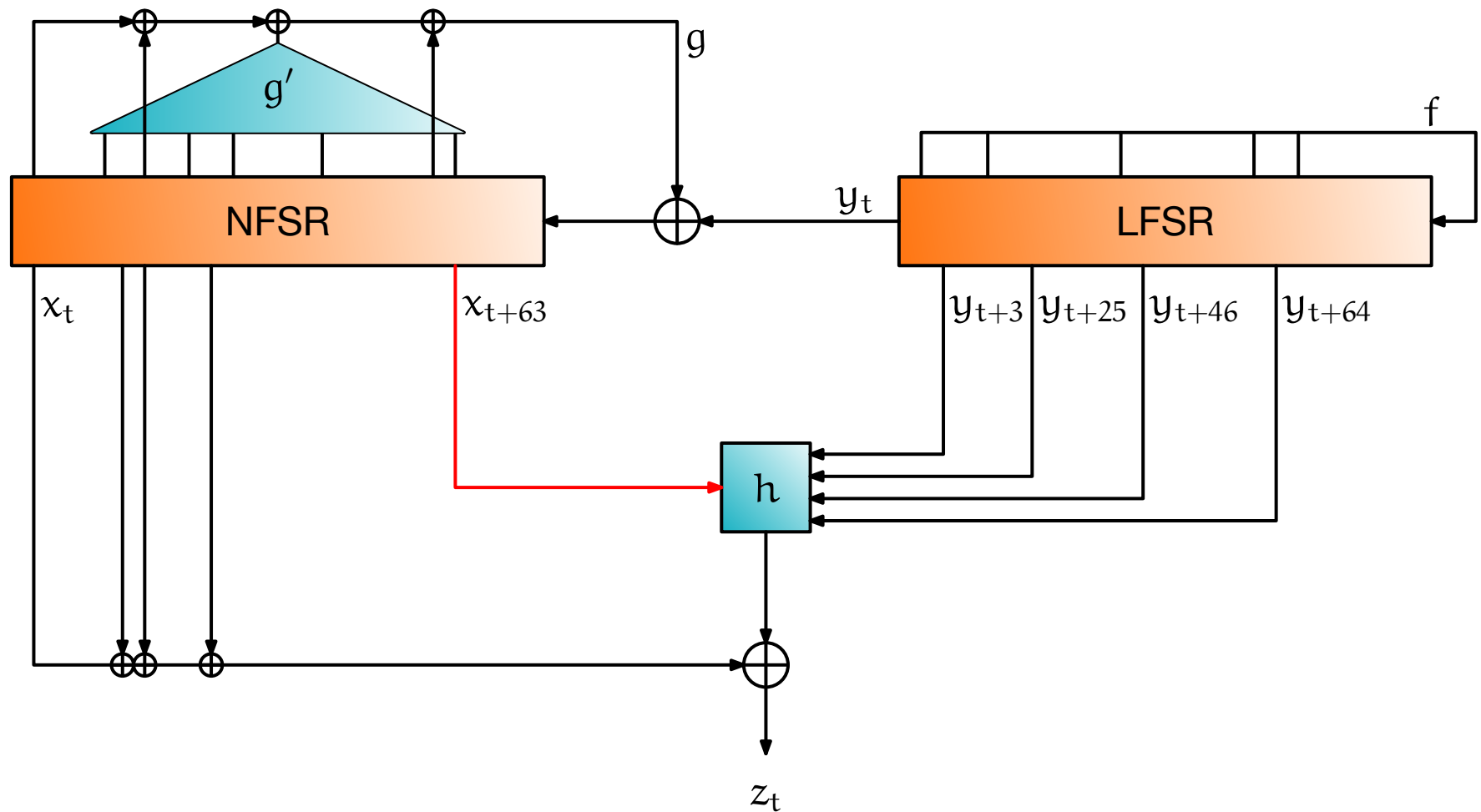


- we get equations of degree $d_f \cdot \max\{d_{g_i}\}$

Application to Grain

A modified version of Grain v1

- we remove the non-linearity of x_{t+63} in function h



A modified version of Grain v1

- we apply our attack against the modified version

- we get equations of degree $d_g \cdot d_h = 6 \cdot 3 = 18$

- a partial annihilator of g exists

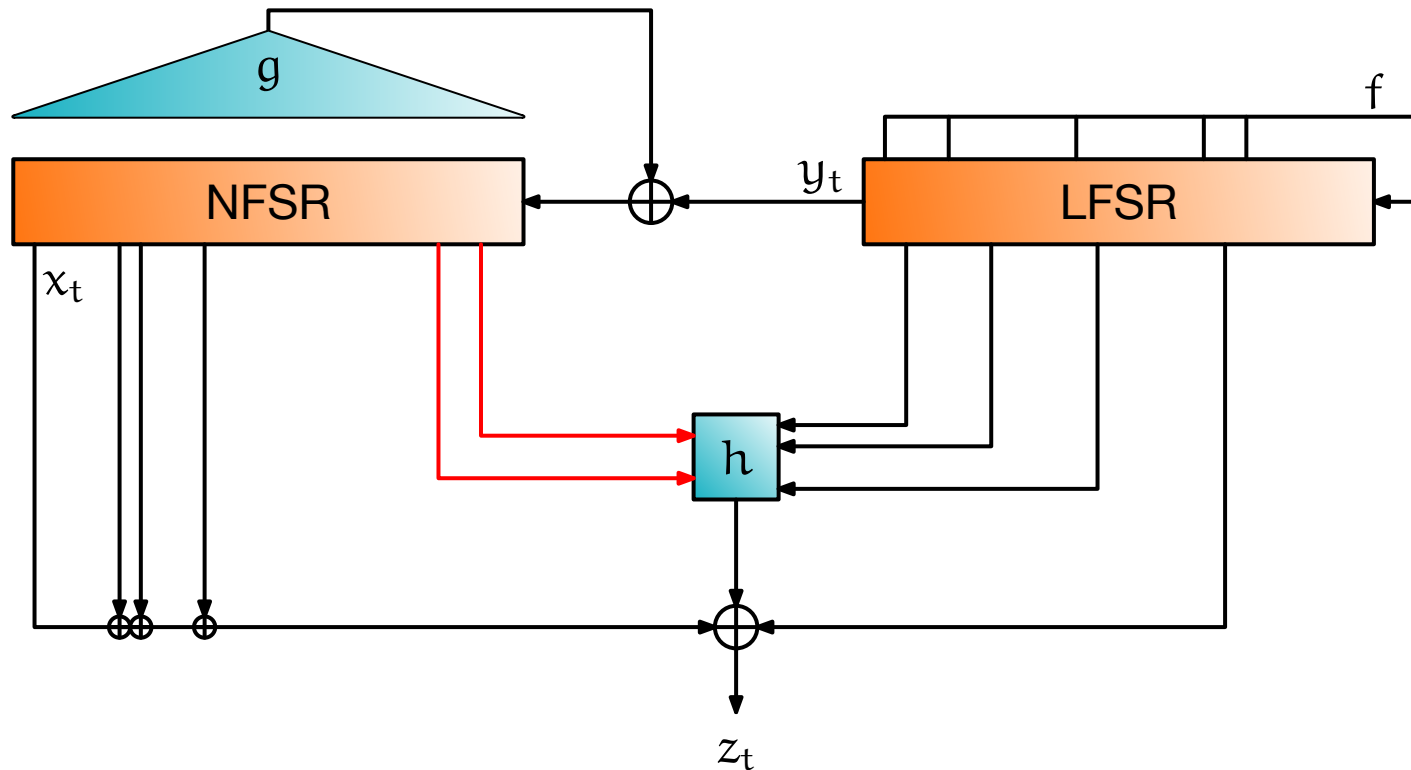
$(1 \oplus x_{t+28})(1 \oplus x_{t+60})g(x_t, \dots, x_{t+79})$ is of degree 4

- this reduce the degree of the equations to 12

- complexity: about 2^{139}

A modified version of Grain 128

- we remove the non-linearity of x_{t+12} and x_{t+95} in function h



- we apply our attack against the modified version
- we get equations of degree $d_g \cdot d_h = 2 \cdot 3 = 6$
- complexity: about 2^{78}

Applicability to Grain v1 and Grain 128

- Grain v1: a product between a variable from χ and a function of degree 2 of γ

$$z_t = \bigoplus x_{t+i} \oplus x_{t+63}p_t \oplus q_t$$

- Grain 128:
 - ▶ two products between a variable from χ and a variable of γ
 - ▶ a monomial of degree 3: 2 variables from χ and a variable from γ

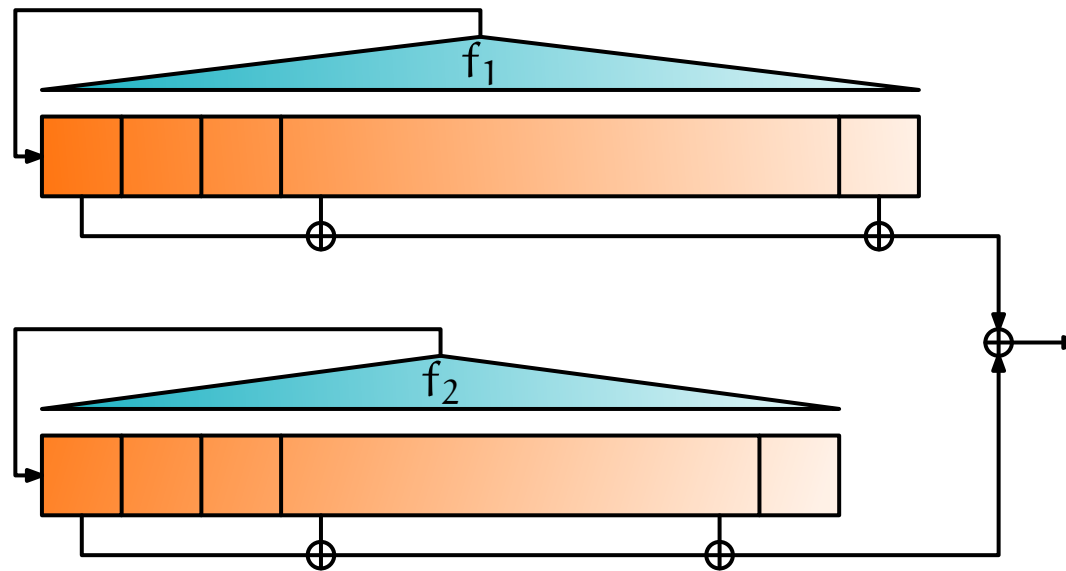
$$z_t = \bigoplus x_{t+i} \oplus x_{t+12}p_t \oplus x_{t+95}q_t \oplus x_{t+12}x_{t+95}r_t \oplus s_t$$

- our attacks are not applicable to Grain v1 and Grain 128

Open Problems

Open Problems

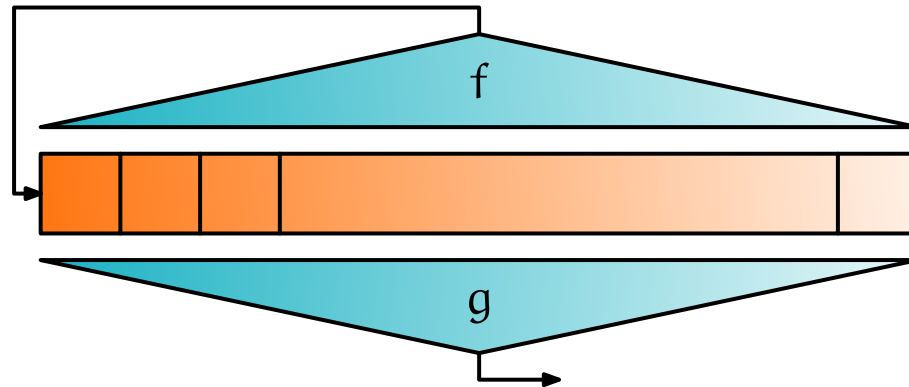
- combination of several NFSRs with linear outputs



- one can express the variables of the smallest NFSR as linear functions of the variables of the second one

Open Problems

- general case (when the output is not linear)



- other approach: try to exploit special properties of the equations (sparsity) to solve them

Conclusion

- Algebraic attacks against NFSR exists in special cases
- NFSR with linear output is equivalent to LFSR with non-linear output
- Algebraic immunity of the update function of the NFSR has to be carefully chosen in that case
- further research on this subject is needed