

# Equivalent Representations of the F-FCSR Keystream Generator

Simon Fischer<sup>1</sup>   Willi Meier<sup>1</sup>   **Dirk Stegemann<sup>2</sup>**

<sup>1</sup>FHNW, Windisch (Switzerland)

<sup>2</sup>University of Mannheim (Germany)

SASC 2008 - The State of the Art of Stream Ciphers  
February 13–14, 2008  
Lausanne, Switzerland

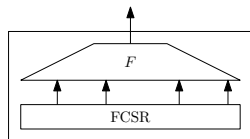
# The F-FCSR Stream Cipher Family (Arnault et al.)

The F-FCSR ciphers consist of

- a regularly clocked (Galois) Feedback with Carry Shift Register (FCSR) with  $n$  register cells

- a linear filter function

$$F : \{0,1\}^n \rightarrow \{0,1\}^k$$

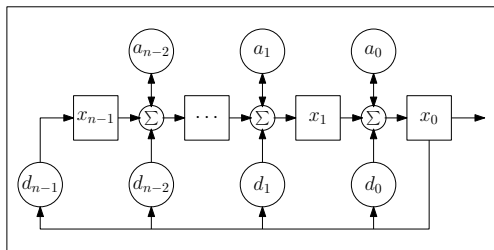


Proposed instances:

	$k$	$n$	keylength [bits]	IV length [bits]
F-FCSR-H	8	160	80	[32, 80]
F-FCSR-16	16	256	128	[0, 128]

We can assume the initial FCSR-state produced by key/IV-setup to be periodic.

# FCSR in Galois Architecture



In each clock cycle,  
 $x_i := \sigma_i \bmod 2$   
 $a_i := \sigma_i \operatorname{div} 2$   
 with  
 $\sigma_i := x_{i+1} + a_i d_i + x_0 d_i$

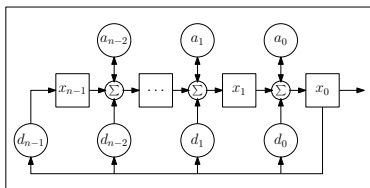
Identify the state  $(x, a)$  with  $p := x + 2a$  and assume that the connection integer  $q := 1 - 2d$  is prime.

At time  $t \geq 0$  we have

- current state  $p^t = 2^{-t} p^0 \bmod q$
- current output bit  $z^t = p^t \bmod 2$ .

for an initial state  $p^0 = p$ .

# Sequences produced by individual Register Cells



**Lemma** (Arnault et al.):

$(x_i^t)_{t \geq 0}$  is given by the output sequence of a Galois FCSR with connection integer  $q$  and initial state  $p_i = F_i(x, a) \cdot q + M_i(q) \cdot p$ .

## Observation

For periodic states  $(x, a)$ ,  $p_i$  can be simplified to  $p_i = p^{s_i} \pmod q$  with  $s_i = -\log_2(M_i(q))$ .

Implications:

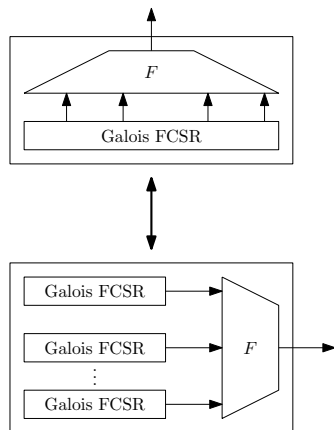
- $(x_i^t)_{t \geq 0}$  is a shifted version of  $(z_i^t)_{t \geq 0}$ .
- The phase shift  $s_i$  is independent of the initial state  $(x, a)$ .

# Equivalent F-FCSR Representation (1)

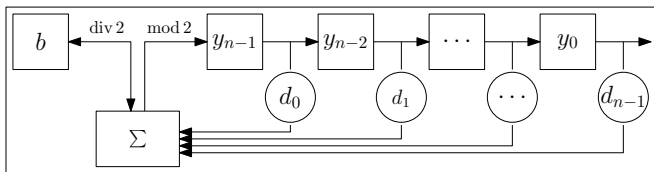
F-FCSR can be written as a combination generator with

- the original filter function  $F$
- $n$  Galois FCSRs with related initial states  $p_i = p^{s_i}$

**However:** Experiments for F-FCSR-H show that the shifts  $s_i$  are distributed over a large part of the period.



# FCSR in Fibonacci Architecture



Identify the state  $(y, b)$  with

$$p := b2^n - \sum_{k=0}^{n-1} \sum_{j=0}^k d_{j-1} y_{k-j} 2^k$$

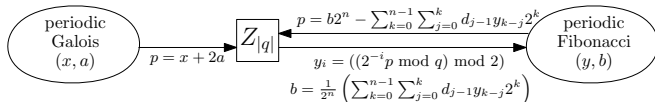
and assume that the connection integer  $q = 1 - 2d$  is prime. As in the Galois architecture, we have for  $t \geq 0$

- current state  $p^t = 2^{-t} p^0 \pmod{q}$
- current output bit  $z^t = p^t \pmod{2}$ .

# Mappings between Galois FCSRs and Fibonacci FCSRs

**Problem:** For a given periodic Galois state  $(x, a)$  find a periodic Fibonacci state  $(y, b)$  (and vice versa) such that the corresponding registers produce the same sequence.

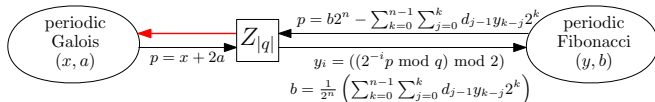
Known Mappings:



# Mappings between Galois FCSRs and Fibonacci FCSRs

**Problem:** For a given periodic Galois state  $(x, a)$  find a periodic Fibonacci state  $(y, b)$  (and vice versa) such that the corresponding registers produce the same sequence.

Known Mappings:



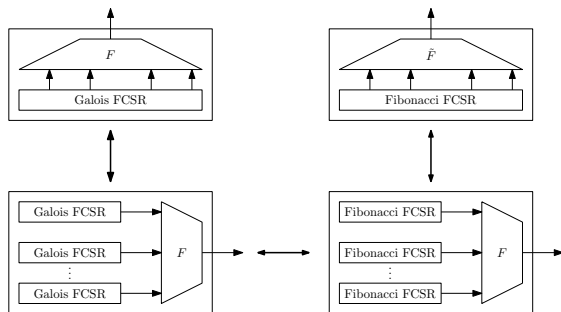
## Observation

For each  $0 \leq p < |q|$  and a prime connection integer  $q$ , the only periodic Galois initial state  $(x', a')$  with  $x' + 2a' = p$  is given by

- $x'_i = M_i \cdot p \bmod q$  for  $0 \leq i < n$
- $a' = \frac{p - x'}{2}$



## Equivalent Representation (2)



More equivalent representations:

- Fibonacci FCSRs in the combination generator
- Fibonacci FCSR and modified (non-linear) filter function  $\tilde{F}$  in the filter generator

**Remark:** Fibonacci FCSR with linear filter is insecure.

## Summary and Conclusion

We can transform the F-FCSR ciphers into equivalent

- combination or filter generators
- using Galois or Fibonacci FCSRs.

Currently, we see no efficient way to exploit these representations for cryptanalytic attacks,

... but maybe somebody else does?

# The End.

`simon.fischer@fhnw.ch`

`willi.meier@fhnw.ch`

`dstegema@th.informatik.uni-mannheim.de`