

Some Remarks on FCSRs and Implications for FCSR-based Stream Ciphers

Simon Fischer¹ Willi Meier² **Dirk Stegemann**³

¹Siemens AG, Zug (Switzerland)

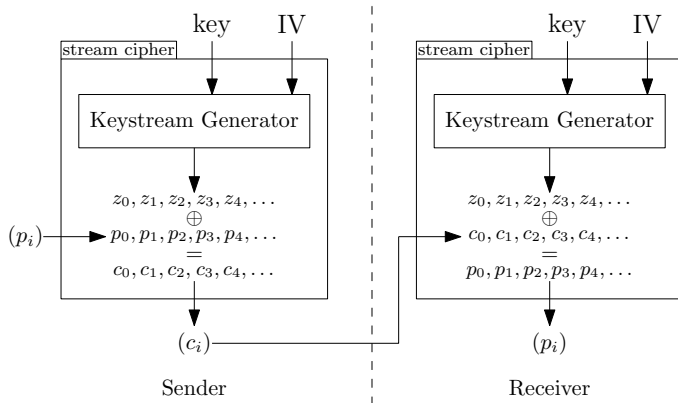
²FHNW, Windisch (Switzerland)

²University of Mannheim (Germany)

WMC 2008 - Second Workshop on Mathematical Cryptology
October 23–25, 2008
Santander, Spain

(Additive) Stream Ciphers — Basic Structure

Stream Ciphers are used for encrypting/decrypting data streams:



Main Application: hardware-constraint environments such as GSM, Bluetooth, Sensor Networks, ...

Attack Model

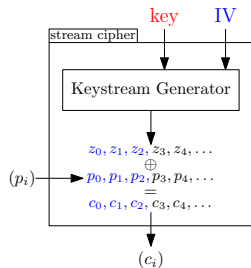
The (passive) attacker **knows**

- the definition of the cipher
- the IV
- the ciphertext stream (c_i)
- some pairs (p_i, c_i) , $0 \leq i \leq n_0$
 → corresponding keystream bits z_i

and wants to reconstruct the whole keystream (z_i) .

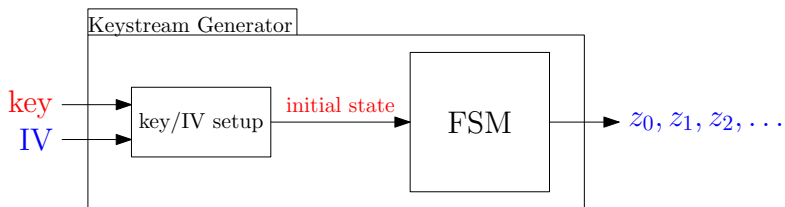
Generic strategy: Recover the secret **key**.

Generic countermeasure: Cipher should behave like a pseudo one-time pad, i.e., $(z_i)_{t \geq 0}$ should not be efficiently distinguishable from a truly random sequence.



The Keystream Generator

Many stream ciphers use an FSM-based keystream generator



to produce the keystream bits z_i .

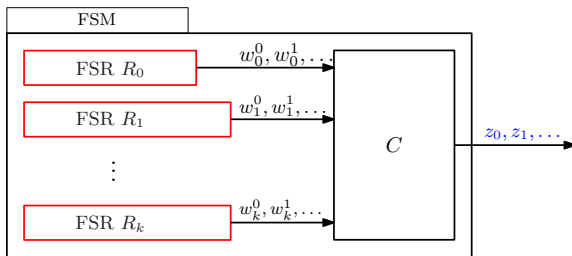
Observation: In order to reproduce the keystream, it is sufficient to recover the initial state of the FSM.

Popular hardware-oriented designs for the FSM:

- combination generators
- filter generators

based on Feedback Shift Registers (FSRs)

Combination Generators



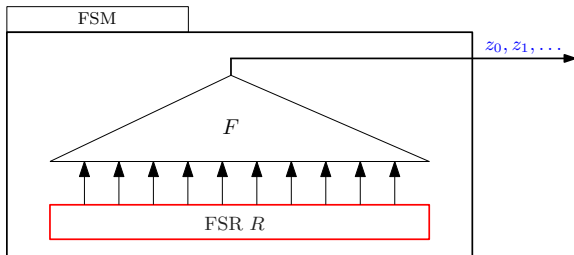
The FSM

- stores the state in Feedback Shift Registers (FSRs),
- produces keystream by combining the FSRs' output bits.

Examples:

- Bluetooth keystream generator E_0
- GSM keystream generator A5/1
- eSTREAM-recommended stream cipher Trivium

Filter Generators



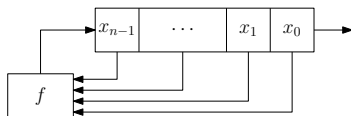
The FSM

- stores the state in a single FSR,
- produces keystream by filtering the current FSR content.

Examples:

- eSTREAM-recommended ciphers Grain and F-FCSR

Feedback Shift Registers (FSRs)



A Feedback Shift Register (FSR)

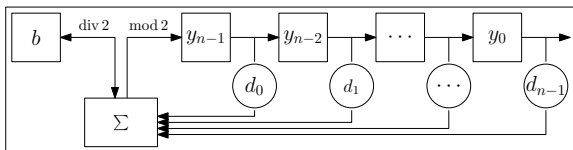
- consists of n register cells, $x_i \in \{0, 1\}$
- in each clock
 - outputs x_0
 - shifts the content one position to the right
 - updates x_{n-1} according to $f(x_0, \dots, x_{n-1})$

f linear \Rightarrow Call the register Linear Feedback Shift Register (LFSR).

f nonlinear \Rightarrow Call it Nonlinear Feedback Shift Register (NFSR).

Special NFSRs: Feedback with Carry Shift Registers (FCSRs)

FCSR in Fibonacci Architecture



In each clock cycle, $y_{n-1} := \sigma \bmod 2$
 $b := \sigma \operatorname{div} 2$
 with $\sigma := \sum_{i=0}^{n-1} y_i d_{n-i-1} + b$
 $y_i := y_{i+1}$ for $0 \leq i < n-1$

Identify the state (y, b) with the integer

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

Algebra behind FCSRs: Ring of 2-adic Integers

2-adic Integer = formal power series $\alpha = \sum_{i=0}^{\infty} u_i 2^i$

- Addition: addition mod 2 with carry
- Multiplication: multiplication mod 2 with carry
- Odd 2-adic integers q have multiplicative inverse q^{-1} .

→ Ring contains especially rational numbers $\frac{p}{q}$ with odd q .

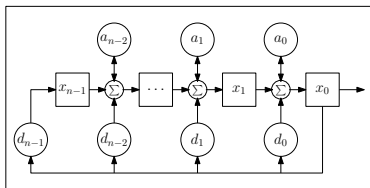
Observation

The output of an FCSR with connection integer $q = 1 - 2 \sum_{i=0}^{n-1} d_i 2^i$ and initial state corresponding to p is the 2-adic expansion of $\frac{p}{q}$.

For a periodic initial state corresponding to the integer $p(0)$,

- the state in time t corresponds to $p(t) = 2^{-t} p(0) \pmod{q}$
- the t -th output bit is $z(t) = p(t) \pmod{2}$

Sequences produced by individual Galois 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 $p_i(0) = F_i(x, a) \cdot q + M_i(q) \cdot p(0)$.

Proposition

For periodic states (x, a) , $p_i(0)$ can be simplified to $p_i(0) = p(s_i) \pmod q$ with $s_i = -\log_2(M_i(q))$.

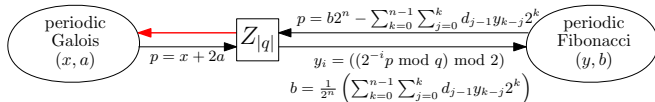
Implications:

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

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:

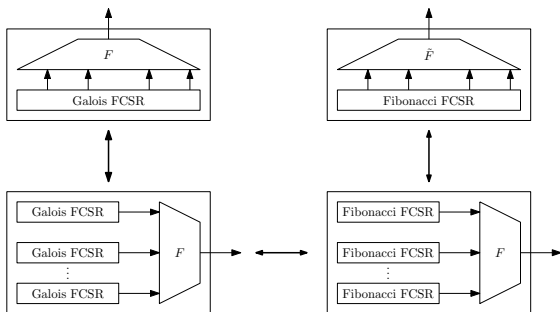


Proposition

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 $0 \leq i < n$
- $a' = \frac{p - x'}{2}$

FCSR-based Finite State Machines



A filtered Galois FCSR can be equivalently represented by

- a Galois/Fibonacci-based combination generator
- a filtered Fibonacci FCSR with modified filter function \tilde{F}

Remark: A Fibonacci FCSR with linear filter is insecure.

Properties of FCSRs and their Output Sequences

If the connection integer q is prime, 2 is a primitive root for q , and $0 < p_0 < |q|$, the FCSR produces so-called l -sequences with

- maximum period ($= |q| - 1$)
- low 2-adic complexity ($=$ size of the smallest FCSR generating the sequence)
- desirable statistical properties such as
 - equally many zeros and ones
 - high linear complexity
 - expected autocorrelation equal to zero

→ What about the autocorrelation for particular shifts?

Autocorrelation of l -sequences

In general, the autocorrelation $\theta_\tau(u)$ of a binary sequence $u = (u_i)_{i \geq 0}$ with shift τ is defined as

$$\theta_\tau(u) = \sum_{i \geq 0} (-1)^{u_i \oplus u_{i+\tau}} = |\{i : u_i \oplus u_{i+\tau} = 0\}| - |\{i : u_i \oplus u_{i+\tau} = 1\}| .$$

Proposition

For a shift $\tau > 0$, the autocorrelation of an l -sequence u is given by

$$\theta_\tau(u) = 4B(\tau, q) - (q - 1 \bmod 2^{\tau+1}) ,$$

where $B(\tau, q)$ denotes the number of $\beta \in \mathbb{Z}_{2^{\tau-1}}$ such that $2\beta q \bmod 2^{\tau+1} > -q \bmod 2^{\tau+1}$.

Open Question: How to compute $B(\tau, q)$ efficiently?

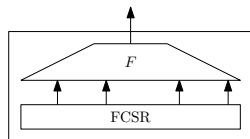
The F-FCSR Stream Cipher Family (Arnault et al.)

... is the first real-world FCSR-based stream cipher.

The FSM of the F-FCSR instances consists of

- a Galois 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]

... have been **broken** by Hell and Johansson (Asiacrypt 2008)

→ Galois FCSRs with linear filters are insecure!

Conclusion

Feedback with Carry Shift Registers

- have an underlying algebraic structure that facilitates their analysis (similarly to LFSRs and in contrast to general NFSRs)
- can be described explicitly in Galois and Fibonacci architecture
- can produce sequences with desirable pseudorandomness properties
- might be suitable for replacing LFSRs in stream cipher applications (if used carefully)

The End.

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