Cryptanalysis of Pseudo-Random Generators based on Vectorial FCSRs

Thierry Berger[1] and **Marine Minier**[2]

[1]XLIM - Limoges University, France

[2]University of Lyon, INRIA, INSA Lyon, France

Indocrypt 2012

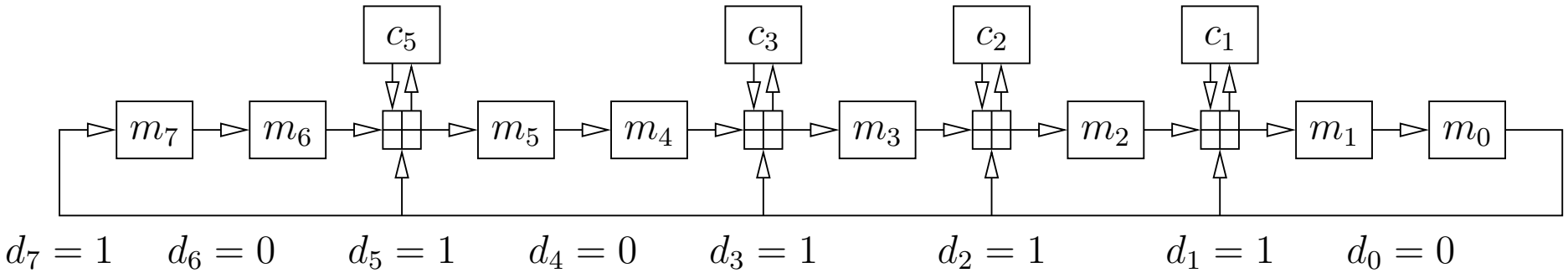
- **Stream ciphers: The FCSRs saga**
- **Vectorial FCSRs (V-FCSRs)**
- **Cryptanalysis of Q-SIFR, stream cipher based on V-FCSRs**
- **Conclusion**

Galois FCSRs [KG 09]

Main register: n binary cells $(m_0, \ldots, m_{n-1})$

Carry register: n binary cells $(c_0, \ldots, c_{n-1})$, $w_H(d)$ actives with $d = \dfrac{1-q}{2}$

Outputed sequences: $p/q \in \mathbb{Z}_2$ with $q = 1 - 2 \cdot \sum_{i=0}^{n-1} d_i 2^i$



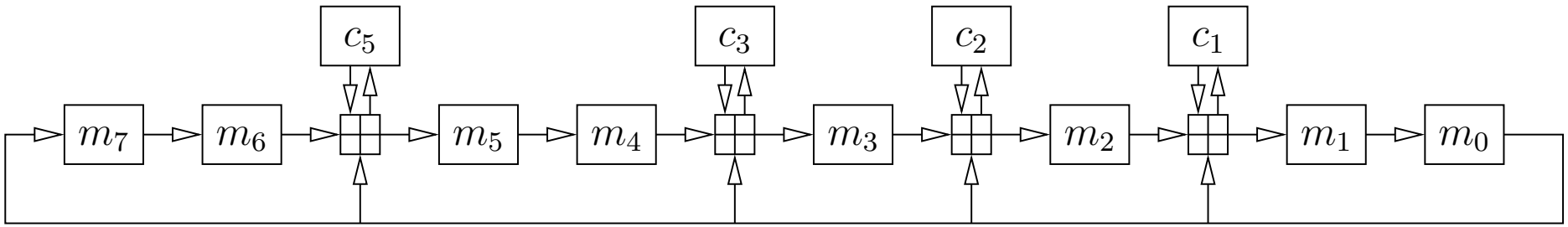
Matrix representation [ABLMP 09][1]

Update function: $T \in \mathcal{C}M_n(\{0,1\})$:

$$\begin{cases} m(t+1) &= Tm(t) + c(t) \bmod_2 \\ c(t+1) &= Tm(t) + c(t) \ \ \mathrm{div}_2 \end{cases}$$

Outputed sequences: p/q with $q = \det(I - 2 \cdot T)$

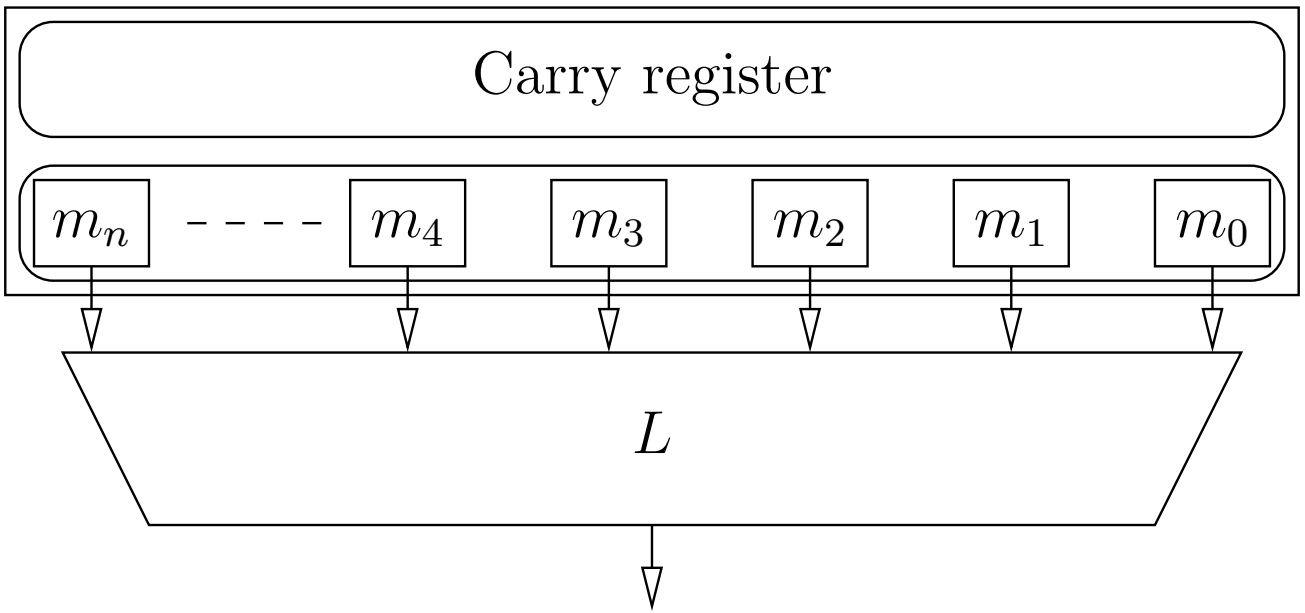
$$T_G = \begin{pmatrix} 0 & \mathbf{1} & & & & & \\ \mathbf{1} & & \mathbf{1} & & & (\mathbf{0}) & \\ \mathbf{1} & & & \mathbf{1} & & & \\ \mathbf{1} & & & & \mathbf{1} & & \\ 0 & & & & & \mathbf{1} & \\ \mathbf{1} & & & (\mathbf{0}) & & & \mathbf{1} \\ 0 & & & & & & \mathbf{1} \\ \mathbf{1} & & & & & & \end{pmatrix}$$



[1] F. Arnault, T. P. Berger, C. Lauradoux, M. Minier, B. Pousse. "A New Approach for FCSRs". In Selected Areas in Cryptography 2009, LNCS 5867.

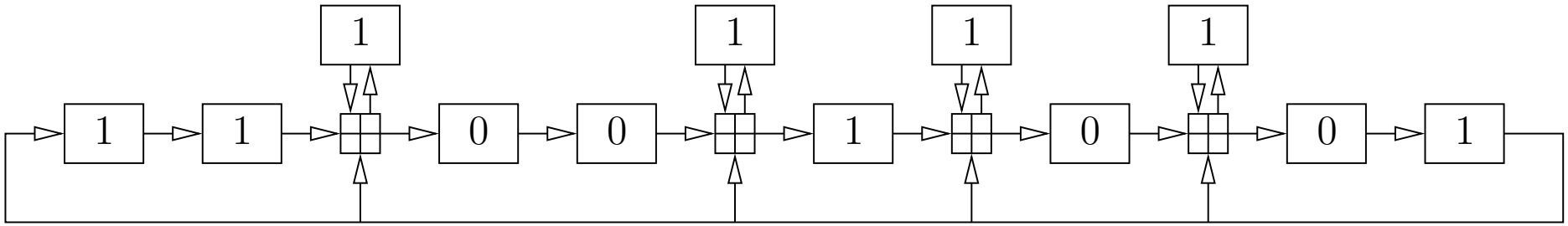
F-FCSR-H v2 proposal [ABL 05]

- eSTREAM finalist in hardware mode: Secret key/IV of 80 bits
- Use a Galois FCSR of size 160 bits filtered using a xor-linear function to output 1 byte per clock
- Good properties come from the 2-adic structure (known period, statistical property,...)



LFSRization of FCSRs [HJ 08]

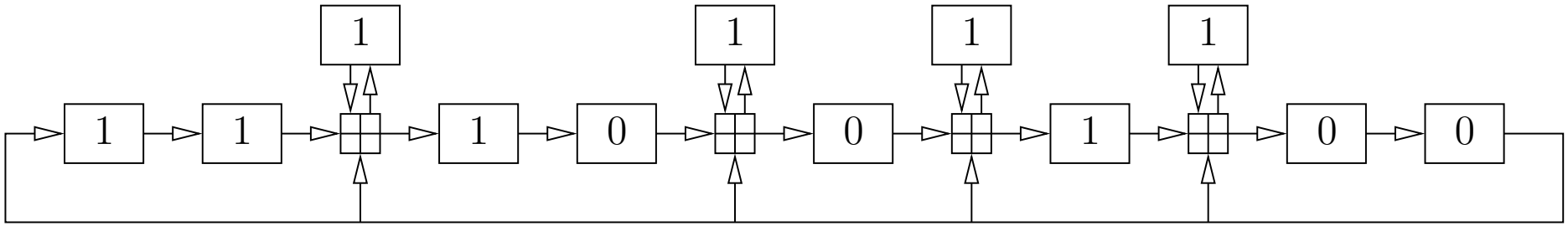
One cell controls all the feedback



A trail of 0 in m_0 leads to a known value for the carry register
$\Rightarrow$ Update function becomes affine

LFSRization of FCSRs [HJ 08]

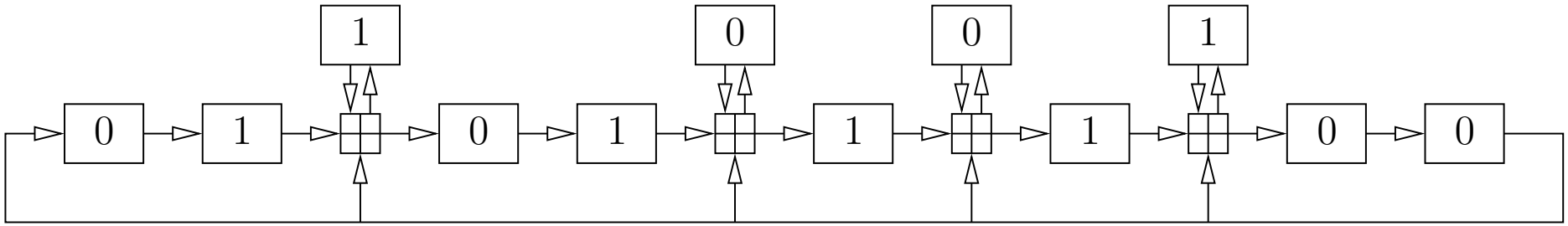
One cell controls all the feedback



A trail of 0 in m_0 leads to a known value for the carry register
$\Rightarrow$ Update function becomes affine

LFSRization of FCSRs [HJ 08]

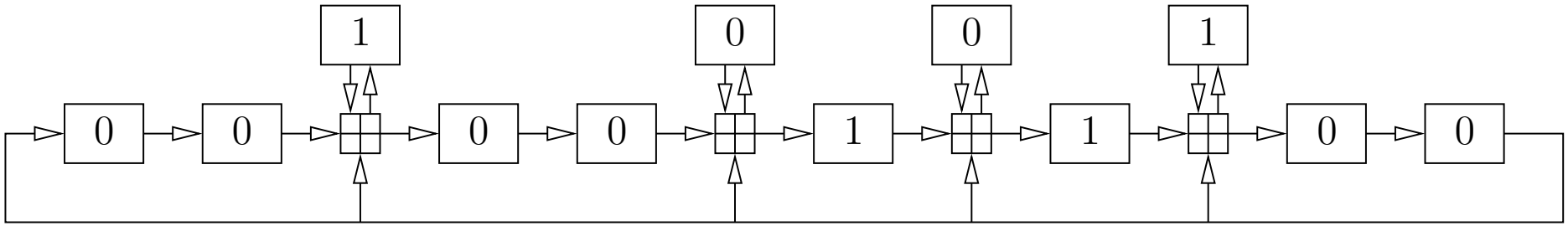
One cell controls all the feedback



A trail of 0 in m_0 leads to a known value for the carry register
$\Rightarrow$ Update function becomes affine

LFSRization of FCSRs [HJ 08]

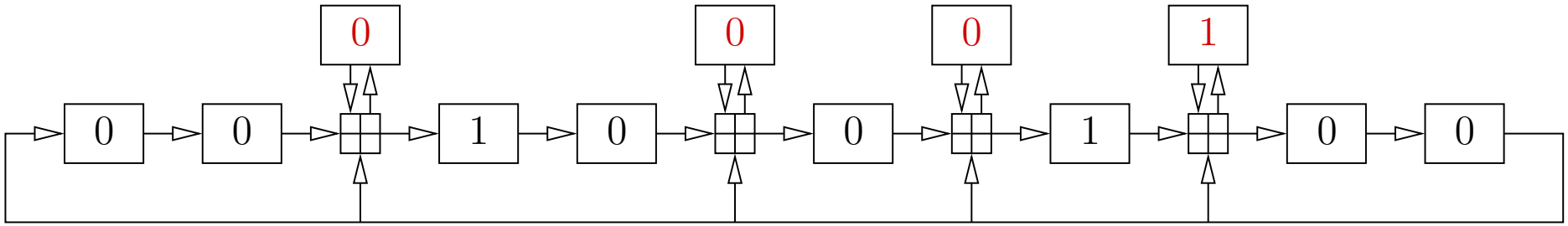
One cell controls all the feedback



A trail of 0 in m_0 leads to a known value for the carry register
$\Rightarrow$ Update function becomes affine

LFSRization of FCSRs [HJ 08]

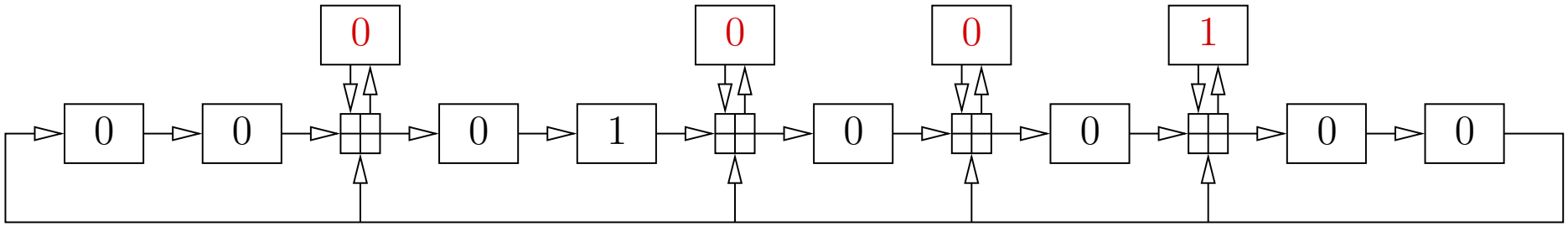
One cell controls all the feedback



A trail of 0 in m_0 leads to a known value for the carry register
$\Rightarrow$ Update function becomes affine

LFSRization of FCSRs [HJ 08]

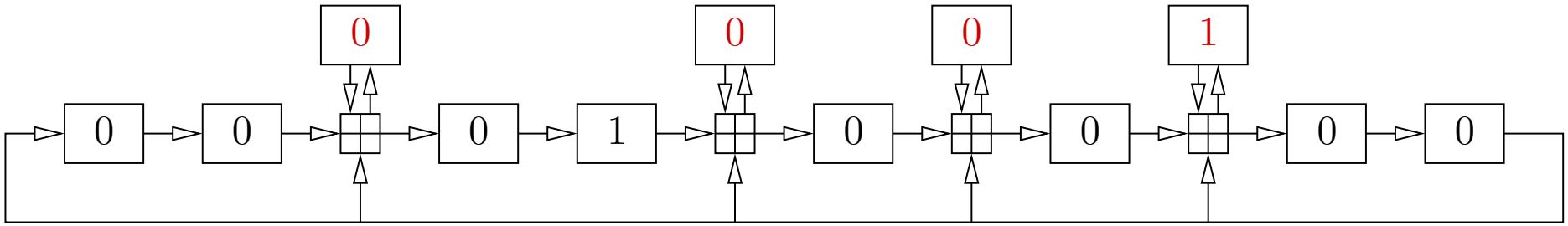
One cell controls all the feedback



A trail of 0 in m_0 leads to a known value for the carry register
$\Rightarrow$ Update function becomes affine

LFSRization of FCSRs [HJ 08]

One cell controls all the feedback

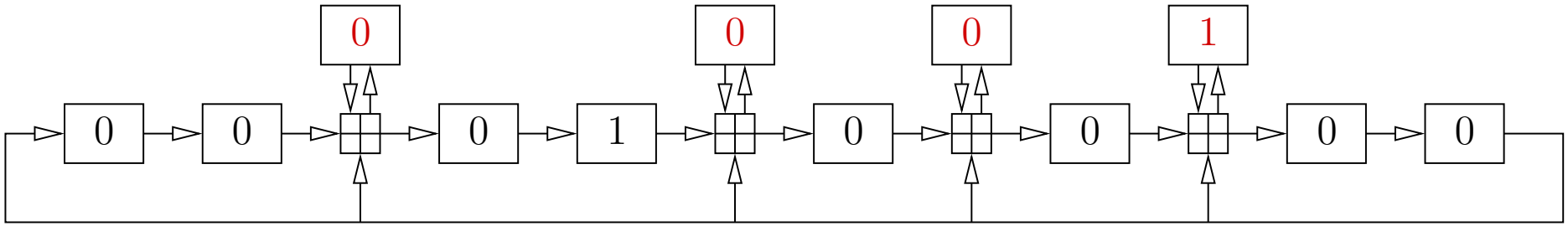


A trail of 0 in m_0 leads to a known value for the carry register
$\Rightarrow$ Update function becomes affine

$$Pr(m_0 = 0 \ during \ k \ clocks) \approx 2^{-k}$$

LFSRization of FCSRs [HJ 08]

One cell controls all the feedback



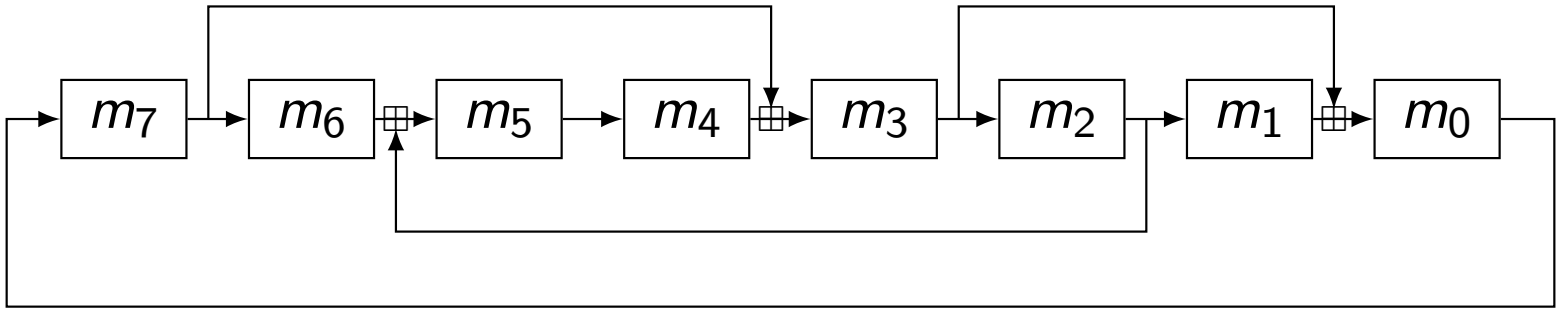
A trail of 0 in m_0 leads to a known value for the carry register
$\Rightarrow$ Update function becomes affine

$$Pr(m_0 = 0 \ during \ k \ clocks) \approx 2^{-k}$$

Against F-FCSR-H v2: $\mathcal{C}O(2^{25})$

Existing solutions to resist LFSRization attack

- [ABLMP 09]: Ring FCSRs (F-FCSR v3) still unbroken since 2009 !

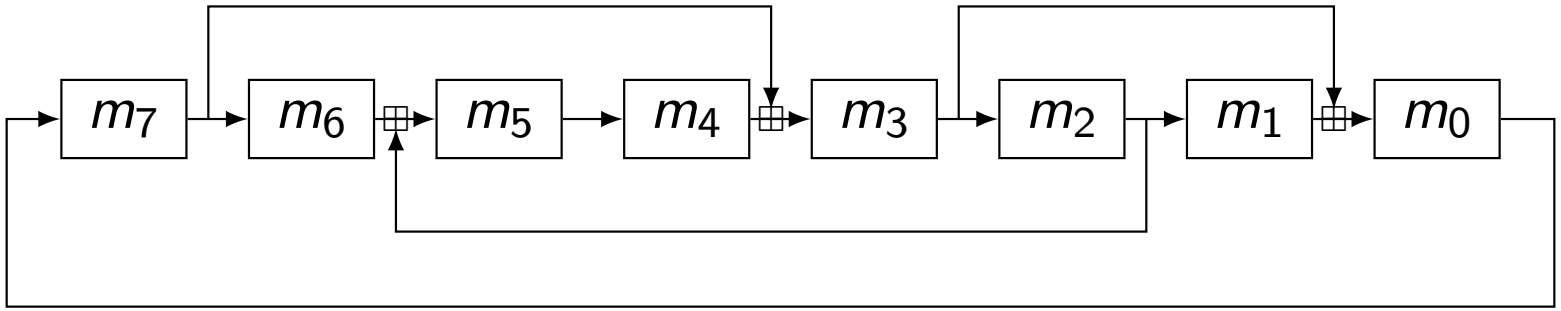


The transition matrix of this FCSR is

$$T_R = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Existing solutions to resist LFSRization attack

- [ABLMP 09]: Ring FCSRs (F-FCSR v3) still unbroken since 2009 !



The transition matrix of this FCSR is

$$T_R = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

- [AMM 10]: Q-SIFR based on Vectorial FCSRs (V-FCSRs)

Vectorial FCSRs: a simple example

- [AMM 10]: Vectorial FCSRs = particular AFSM on $\mathcal{A} = \mathbb{Z}[X]/(P(X))$ with $P(X) \in \mathbb{Z}[X]$, a monic irreducible polynomial of degree d

Vectorial FCSRs: a simple example

- [AMM 10]: Vectorial FCSRs = particular AFSM on $\mathcal{A} = \mathbb{Z}[X]/(P(X))$ with $P(X) \in \mathbb{Z}[X]$, a monic irreducible polynomial of degree d
- **Example:** $P(X) = X^2 - X - 1$, thus $d = 2$ and base of $\mathcal{A}$ $\mathcal{B} = \{0, 1, X, X + 1\}$
- Choose a polynomial $Q(X) = u + vX$, $u = -11$, $v = -10$
- set $d(X) = (1 - Q(X))/2$ and $d(X) = \sum_{i=0}^{3} d_i(X)2^i$ with $d_i \in \mathcal{B}$
- here, $d(X) = 12 + 5X = X \cdot 2^0 + (X + 1) \cdot 2^2 + 2^3$

Vectorial FCSRs: Matrix representation

Galois Matrix representation associated to $Q(X)$ is:

$$T = \begin{pmatrix} X & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1+X & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Vectorial FCSRs: Matrix representation

Galois Matrix representation associated to $Q(X)$ is:

$$T = \begin{pmatrix} X & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1+X & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

State Update: $T \in \mathcal{C}M_k(\mathcal{B})$ $(m(t), c(t)) \in \mathcal{B}^k \times \mathcal{B}^k$:

$$\begin{cases} z(t+1) &= Tm(t) + c(t) \\ m(t+1) &= \mathrm{mod}_2(z(t+1)) \\ c(t+1) &= \mathrm{div}_2(z(t+1)) \end{cases}$$

Vectorial FCSRs: Matrix representation

Galois Matrix representation associated to $Q(X)$ is:

$$T = \begin{pmatrix} X & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1+X & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

State Update: $T \in \mathcal{C}M_k(\mathcal{B})$ $(m(t), c(t)) \in \mathcal{B}^k \times \mathcal{B}^k$:

$$\begin{cases} z(t+1) &= Tm(t) + c(t) \\ m(t+1) &= \mathrm{mod}_2(z(t+1)) \\ c(t+1) &= \mathrm{div}_2(z(t+1)) \end{cases}$$

Relation: $\det(I - 2T) = Q(X)$, $Q(X)$ is the connection polynomial of the V-FCSR

Arithmetic on $\mathcal{A}$

- $\mathcal{A} = \mathbb{Z}[X]/(P(X)) \approx \mathbb{Z}^d$: $\sum_{i=0}^{d-1} r_i X^i$, $r_i \in \mathbb{Z} \rightarrow r = (r_0, ..., r_{d-1}) \in \mathbb{Z}^d$
- Multiplication in $\mathcal{A}$ by $r(X)$ $\mathbb{Z}$-linear and using a $d \times d$ matrix

Arithmetic on $\mathcal{A}$

- $\mathcal{A} = \mathbb{Z}[X]/(P(X)) \approx \mathbb{Z}^d$: $\sum_{i=0}^{d-1} r_i X^i$, $r_i \in \mathbb{Z} \rightarrow r = (r_0, ..., r_{d-1}) \in \mathbb{Z}^d$
- Multiplication in $\mathcal{A}$ by $r(X)$ $\mathbb{Z}$-linear and using a $d \times d$ matrix
- **Example:** Multiplication by X in $\mathcal{A} = M_X$ of $P(X)$ in $\mathbb{Z}^d$

$$M_X = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \\ -p_0 & -p_1 & \dots & \dots & -p_{d-1} \end{pmatrix}$$

Arithmetic on $\mathcal{A}$

- $\mathcal{A} = \mathbb{Z}[X]/(P(X)) \approx \mathbb{Z}^d$: $\sum_{i=0}^{d-1} r_i X^i$, $r_i \in \mathbb{Z} \rightarrow r = (r_0, ..., r_{d-1}) \in \mathbb{Z}^d$
- Multiplication in $\mathcal{A}$ by $r(X)$ $\mathbb{Z}$-linear and using a $d \times d$ matrix
- **Example:** Multiplication by X in $\mathcal{A} = M_X$ of $P(X)$ in $\mathbb{Z}^d$

$$M_X = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ \vdots & 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 1 \\ -p_0 & -p_1 & \dots & \dots & -p_{d-1} \end{pmatrix}$$

- **General case:** $r(X) = \sum_{i=0}^{d-1} r_i X^i$ in $\mathcal{A}$, $M_{r(X)} = \sum_{i=0}^{d-1} r_i M_X^i$ in $\mathbb{Z}^d$
- $\text{norm}(r(X)) = \det(M_{r(X)})$

Practical implementation (1/2)

- AFSM on $\mathcal{A}$ seen as d-tuples of $\mathbb{Z}$ elements; k-tuple of $\mathcal{A}$ elements becomes elements of $\mathbb{Z}^{kd}$
- $k \times k$ matrix T on $\mathcal{A} \Rightarrow kd \times kd$ matrix $\mathcal{T}$ on $\mathbb{Z}$ identifying $r(X)$ with $M_{r(X)}$

Practical implementation (1/2)

- AFSM on $\mathcal{A}$ seen as d-tuples of $\mathbb{Z}$ elements; k-tuple of $\mathcal{A}$ elements becomes elements of $\mathbb{Z}^{kd}$
- $k \times k$ matrix T on $\mathcal{A} \Rightarrow kd \times kd$ matrix $\mathcal{T}$ on $\mathbb{Z}$ identifying $r(X)$ with $M_{r(X)}$
- **Example:** with $P(X) = X^2 - X - 1$,

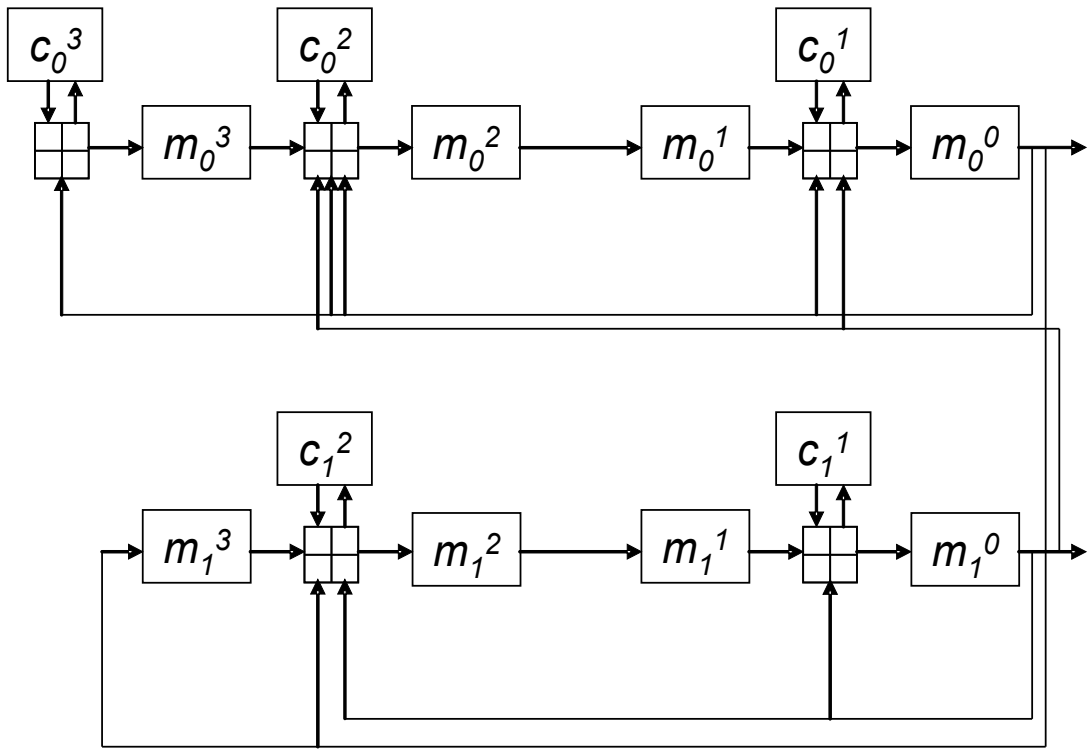
$$M_X = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad M_{1+X} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

- matrix $\mathcal{T}$ with $Q(X) = -11 - 10X$:

$$T = \begin{pmatrix} X & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1+X & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \Rightarrow \mathcal{T} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Practical implementation (2/2)

- Practical implementation with $Q(X) = -11 - 10X$ and $\mathcal{T}$ in Galois mode
- require simple carries, double carries and triple carries with two feedback bits $m_0^0(t)$ $m_1^0(t)$



Nice results

State Update:

- $(m, c) \in \mathbb{Z}^{kd} \times \mathbb{Z}^{kd}$
- A transition function given by a $k \times k$ matrix T. Let $\mathcal{T}$ be its corresponding $kd \times kd$ matrix over $\mathbb{Z}$:

If the automaton is in the state $(m(t), c(t))$ at time t, then

$$\begin{cases} z(t+1) &= \mathcal{T} m(t) + c(t) \\ m(t+1) &= z(t+1) \bmod 2 \\ c(t+1) &= z(t+1) \operatorname{div} 2 \end{cases}$$

Nice results

State Update:

- $(m, c) \in \mathbb{Z}^{kd} \times \mathbb{Z}^{kd}$
- A transition function given by a $k \times k$ matrix T. Let $\mathcal{T}$ be its corresponding $kd \times kd$ matrix over $\mathbb{Z}$:

If the automaton is in the state $(m(t), c(t))$ at time t, then

$$\begin{cases} z(t+1) &= \mathcal{T} m(t) + c(t) \\ m(t+1) &= z(t+1) \bmod 2 \\ c(t+1) &= z(t+1) \operatorname{div} 2 \end{cases}$$

Theorem

We have: $\det(\mathcal{T}) = \mathrm{norm}(\det(T))$ *and* $\tilde{q} = \det(I - 2 \cdot \mathcal{T})$

Nice results

State Update:

- $(m, c) \in \mathbb{Z}^{kd} \times \mathbb{Z}^{kd}$
- A transition function given by a $k \times k$ matrix T. Let $\mathcal{T}$ be its corresponding $kd \times kd$ matrix over $\mathbb{Z}$:

If the automaton is in the state $(m(t), c(t))$ at time t, then

$$\begin{cases} z(t+1) &= \mathcal{T} m(t) + c(t) \\ m(t+1) &= z(t+1) \bmod 2 \\ c(t+1) &= z(t+1) \operatorname{div} 2 \end{cases}$$

Theorem

We have: $\det(\mathcal{T}) = \mathrm{norm}(\det(T))$ *and* $\tilde{q} = \det(I - 2 \cdot \mathcal{T})$

- with $Q(X) = -11 - 10X$, $\tilde{q} = -131$.
- See complete theoretical treatment in the paper !

Description of Q-SIFR [AMM 10]

- Parameters of the V-FCSR: $n = 2$, $p(X) = X^2 - X - 1$, so $d = 2$ and

$$M_X = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

- Matrix of size $k = 160$ over $\mathcal{A}$. $q(X) = u + vX$ connection polynomial with

$$\begin{aligned} u &= -1993524591318275015328041611344215036460140087963 \\ v &= -1993524591318275015328041611344215036460140087860. \end{aligned}$$

Description of Q-SIFR [AMM 10]

- Parameters of the V-FCSR: $n = 2$, $p(X) = X^2 - X - 1$, so $d = 2$ and

$$M_X = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

- Matrix of size $k = 160$ over $\mathcal{A}$. $q(X) = u + vX$ connection polynomial with

$$\begin{aligned} u &= -1993524591318275015328041611344215036460140087963 \\ v &= -1993524591318275015328041611344215036460140087860. \end{aligned}$$

- Galois V-FCSR represented by a 320×320 matrix $\mathcal{T}$

$$\tilde{q} = \det(I - 2\mathcal{T}) = 39741402961906954206160047535539796042005214340820825272689327902761723128526374726419918065389 49$$

Description of Q-SIFR [AMM 10]

- Parameters of the V-FCSR: $n = 2$, $p(X) = X^2 - X - 1$, so $d = 2$ and

$$M_X = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

- Matrix of size $k = 160$ over $\mathcal{A}$. $q(X) = u + vX$ connection polynomial with

$$\begin{aligned} u &= -1993524591318275015328041611344215036460140087963 \\ v &= -1993524591318275015328041611344215036460140087860. \end{aligned}$$

- Galois V-FCSR represented by a 320×320 matrix $\mathcal{T}$

$$\tilde{q} = \det(I - 2\mathcal{T}) = 39741402961906954206160047535539796042005214340820825272689327902761723128526374726419918065389 49$$

- At each iteration, a linear filter extracts 16 bits of stream

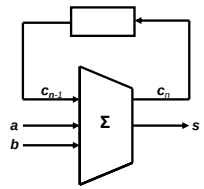
LFSRization attack against Q-SIFR (1/2)

- How many clocks to cancel the carry contents
- with 2 feedback bits: $m_0(t)$ and $m_1(t)$ and 3 kinds of carries?

LFSRization attack against Q-SIFR (1/2)

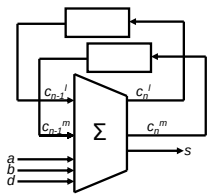
- How many clocks to cancel the carry contents
- with 2 feedback bits: $m_0(t)$ and $m_1(t)$ and 3 kinds of carries?

5 Classical carries:



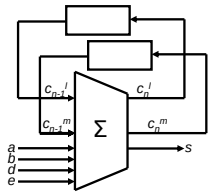
$$\begin{pmatrix} 1 & 0 \\ 1/2 & 1/2 \end{pmatrix}$$

82 Double carries:



$$\begin{pmatrix} 1 & 0 & 0 \\ 1/2 & 1/2 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

81 Triple carries:

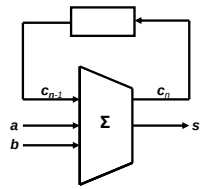


$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 \end{pmatrix}$$

LFSRization attack against Q-SIFR (1/2)

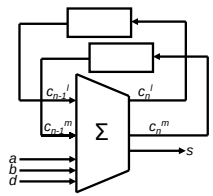
- How many clocks to cancel the carry contents
- with 2 feedback bits: $m_0(t)$ and $m_1(t)$ and 3 kinds of carries?

5 Classical carries:



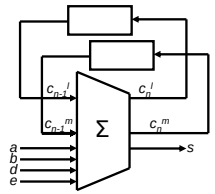
$$\begin{pmatrix} 1 & 0 \\ 1/2 & 1/2 \end{pmatrix}$$

82 Double carries:



$$\begin{pmatrix} 1 & 0 & 0 \\ 1/2 & 1/2 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

81 Triple carries:



$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1/2 & 1/2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1/2 & 1/2 & 0 \end{pmatrix}$$

$\Rightarrow$ In total, $\max(\log_2(5), \log_2(2 \times 82), \log_2(3 \times 81)) = 8$ clocks to cancel all the carry contents

$\Rightarrow$ Happens with $\Pr = 2^{-8\times 2} = 2^{-16}$ with $m_0(t) = 0$ AND $m_1(t) = 0$ during 8 clocks

LFSRization attack against Q-SIFR (2/2)

- To complete the attack, maintain during s clocks the state (0011000...000) in the carry register
- Enough to solve a system of 320 unknowns

LFSRization attack against Q-SIFR (2/2)

- To complete the attack, maintain during s clocks the state (0011000...000) in the carry register
- Enough to solve a system of 320 unknowns

$\Rightarrow$ True as soon as 19 clocks are performed

LFSRization attack against Q-SIFR (2/2)

- To complete the attack, maintain during s clocks the state (0011000...000) in the carry register
- Enough to solve a system of 320 unknowns

$\Rightarrow$ True as soon as 19 clocks are performed

- This happens with Proba $= 2^{-16} \times 2^{-19\times 2} = 2^{-54}$
- Gaussian elimination: $2^{54} \times (320)^{2.807} \approx 2^{77.35}$ operations

LFSRization attack against Q-SIFR (2/2)

- To complete the attack, maintain during s clocks the state (0011000...000) in the carry register
- Enough to solve a system of 320 unknowns

$\Rightarrow$ True as soon as 19 clocks are performed

- This happens with Proba $= 2^{-16} \times 2^{-19\times 2} = 2^{-54}$
- Gaussian elimination: $2^{54} \times (320)^{2.807} \approx 2^{77.35}$ operations
- Two improvements:
  - **System resolution improvement:** 16 subsystems of 20 linear equations due to the filter structure
    $\Rightarrow$ Resolution complexity $16 \times (20^{2.807}) \approx 2^{16.13}$ operations
    $\Rightarrow$ Overall complexity $2^{70.13}$ operations

LFSRization attack against Q-SIFR (2/2)

- To complete the attack, maintain during s clocks the state (0011000...000) in the carry register
- Enough to solve a system of 320 unknowns

$\Rightarrow$ True as soon as 19 clocks are performed

- This happens with Proba $= 2^{-16} \times 2^{-19\times 2} = 2^{-54}$
- Gaussian elimination: $2^{54} \times (320)^{2.807} \approx 2^{77.35}$ operations
- Two improvements:
  - **System resolution improvement:** 16 subsystems of 20 linear equations due to the filter structure
    $\Rightarrow$ Resolution complexity $16 \times (20^{2.807}) \approx 2^{16.13}$ operations
    $\Rightarrow$ Overall complexity $2^{70.13}$ operations
  - **Only 17 clocks are required:** the knowledge of the carry content at $t + 19$ is not necessary
    $\Rightarrow$ Overall complexity $2^{66.13}$ operations observing 2^{50} outputs

Conclusion

- **Test:** with a frequency 2^{-20}, carry register of Q-SIFR = (001100...00) during 11 consecutive clocks

Conclusion

- **Test:** with a frequency 2^{-20}, carry register of Q-SIFR = (001100...00) during 11 consecutive clocks

- **Hardware comparison:**
  - Done in the paper with a big advantage for F-FCSR-16 v3 !

Conclusion

- **Test:** with a frequency 2^{-20}, carry register of Q-SIFR = (001100...00) during 11 consecutive clocks
- **Hardware comparison:**
  - Done in the paper with a big advantage for F-FCSR-16 v3 !
- In summary, F-FCSR-16 more resistant to LFSRization attack than Q-SIFR and also with a better hardware implementation !

Conclusion

- **Test:** with a frequency 2^{-20}, carry register of Q-SIFR = (001100...00) during 11 consecutive clocks
- **Hardware comparison:**
  - Done in the paper with a big advantage for F-FCSR-16 v3 !
- In summary, F-FCSR-16 more resistant to LFSRization attack than Q-SIFR and also with a better hardware implementation !
- Please use F-FCSR-16 v3 rather than Q-SIFR !

Questions ?

Thank you for your attention !