Design des automates algébriques pour les implémentations hardwares et softwares en cryptographie symétrique.

T. P. Berger

XLIM (UMR CNRS 7252), Université de Limoges

Codes et Cryptographie, Dinard, 7-12 Octobre 2012

This work was partially supported by the French National Agency of Research: ANR-06-SETI-013 and ANR-11-INS-011.

Common work with
François Arnault, Cédric Lauradoux, Marine Minier, Benjamin Pousse, Gaël Thomas, ...

Main publications:

- Arnault F., Berger T. P., Minier M., Pousse B.: Revisiting LFSRs for Cryptographic Applications, IEEE Transactions on Information Theory , 57(12), p.8095-8113 (2011)
- Arnault F., Berger T. P., Lauradoux C., Minier M., Pousse B. A New Approach for FCSRs, In Michael J. Jacobson Jr., Vincent Rijmen, Reihaneh Safavi-Naini editors, Selected Areas in Cryptography - SAC 2009,LNCS 5867: 433-448, Springer 2009.
- Arnault F., Berger T. P., Pousse B.: A matrix approach for FCSR automata, Cryptography and Communications, v.3 (2): p.109-139 (2011)

Autonomous LFSM

An Autonomous Linear Finite State Machine (LFSM) of length n, with ℓ outputs consists of:

- A set of n cells, $m = (m_0, \ldots, m_{n-1}) \in \mathbb{F}_2^n$, called the set of *states* of the automaton.
- A linear transition function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$.
- A linear extraction function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^\ell$.

T: $n \times n$ matrix of the transition function,
C: $n \times \ell$ matrix of the extraction function,

- Initialization: state $m(0) \in \mathbb{F}_2^n$ at time $t = 0$
- From the state $m(t)$ at time t, output: $v(t) = Cm(t)$
- Compute a new state $m(t+1) = Tm(t)$

An example: LFSR in Fibonnaci mode

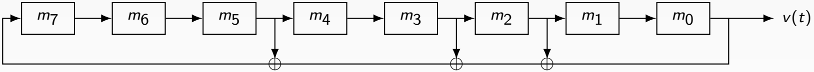
$$T_1 = \begin{pmatrix} & 1 & & & & & & \\ & & 1 & & & (0) & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & (0) & & & & 1 & \\ & & & & & & & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

An example: LFSR in Fibonnaci mode

$$T_1 = \begin{pmatrix} & 1 & & & & & & \\ & & 1 & & & (0) & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & (0) & & & & 1 & \\ & & & & & & & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$C_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$



Another example: LFSR in Galois mode

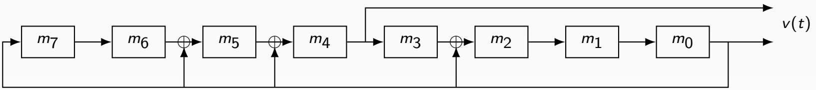
$$T_2 = \begin{pmatrix} 0 & 1 & & & & & & \\ 0 & & 1 & & & (0) & & \\ 1 & & & 1 & & & & \\ 0 & & & & 1 & & & \\ 1 & & & & & 1 & & \\ 1 & & (0) & & & & 1 & \\ 0 & & & & & & & 1 \\ 1 & & & & & & & \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

Another example: LFSR in Galois mode

$$T_2 = \begin{pmatrix} 0 & 1 & & & & & & \\ 0 & & 1 & & & (0) & & \\ 1 & & & 1 & & & & \\ 0 & & & & 1 & & & \\ 1 & & & & & 1 & & \\ 1 & & (0) & & & & 1 & \\ 0 & & & & & & & 1 \\ 1 & & & & & & & \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

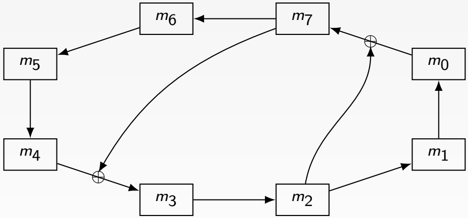


A third example: LFSR in Ring mode

$$T_3 = \begin{pmatrix} & 1 & & & & & & \\ & & 1 & & & (0) & & \\ & & & 1 & & & & \\ & & & & 1 & & & 1 \\ & & & & & 1 & & \\ & & (0) & & & & 1 & \\ & & & & & & & 1 \\ 1 & & 1 & & & & & \end{pmatrix}$$

A third example: LFSR in Ring mode

$$T_3 = \begin{pmatrix} & 1 & & & & & & \\ & & 1 & & & (0) & & \\ & & & 1 & & & & \\ & & & & 1 & & & 1 \\ & & & & & 1 & & \\ & & (0) & & & & 1 & \\ & & & & & & & 1 \\ 1 & & 1 & & & & & \end{pmatrix}$$



Output of LFSMs

$M_i(X) = \sum_{t=0}^{\infty} m_i(t)X^t$
$M = (M_0(X), ..., M_{n-1}(X))$

Theorem

If the initial state of a LFSM is $m = (m_0, ..., m_{n-1})$ *then*

$$^tM = \frac{Adj(I - XT)}{q(X)}\ ^tm$$

with $q(X) = \det(I - XT)$.

If $\det(T) \neq 0$ and $q(X)$ primitive, then

$M_i(X) = p_i(X)/q(X)$ m-sequences of period $2^n - 1$.

Examples continued

for $i = 0$, 2 or 3, $\quad q_i(X) = \det(I - XT_i) = X^8 + X^6 + X^5 + X^3 + 1$

$Adj(I - XT_3) =$

$$\begin{pmatrix}
x^6+x^3+1 & x^7+x^4+x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7+x^4 \\
x^7+x^4 & x^6+x^3+1 & x & x^2 & x^3 & x^4 & x^5 & x^6+x^3 \\
x^6+x^3 & x^7+x^4 & 1 & x & x^2 & x^3 & x^4 & x^5+x^2 \\
x^5+x^2 & x^6+x^3 & x^7+x^5+x^4+x^2 & 1 & x & x^2 & x^3 & x^4+x \\
x^4 & x^5 & x^6+x^4 & x^7+x^5 & x^5+x^3+1 & x^6+x^4+1 & x^7+x^5+x^2 & x^3 \\
x^3 & x^4 & x^5+x^3 & x^6+x^4 & x^7+x^5 & x^5+x^3+1 & x^6+x^4+x & x^2 \\
x^2 & x^3 & x^4+x^2 & x^5+x^3 & x^6+x^4 & x^7+x^5 & x^5+x^3+1 & x \\
x & x^2 & x^3+x & x^4+x^2 & x^5+x^3 & x^6+x^4 & x^7+x^5 & 1
\end{pmatrix}$$

LFSRs: for what purpose?

Non cryptographic context

- Simulation: hight speed for random numbers generation (Monte Carlo method...)
- Initialization tests of arithmetic circuits in computers
- Implementation of counters...

Cryptographic context

- basic building block for the design of automata in symmetric cryptography
- Good statistical properties
- Proved period...

Depending on the target, 2 types of outputs

- One bit output
- Block of bits output

Efficient implementations

Software applications

- Use the natural bloc structure (8, 16, 32, 64 bits) of the processor and assembly instructions
- Minimize the cycles: pipe-line optimizations, etc...

Hardware applications

- Power consumption
- Area of the circuit, number of gates
- Minimize path, fan-out...

A new concept: diffusion delay

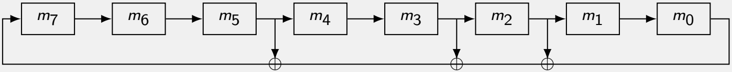
The diffusion delay is the smallest number d, such that there exist two cells m_i and m_j with the following property: the successive values $m_j(0)$, ..., $m_j(d-1)$ are independent of the value $m_i(0)$.

Definition

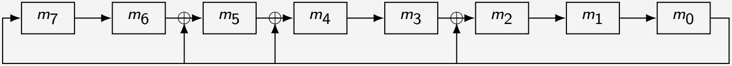
Diffusion delay = Diameter of the graph of connection of the cells

One bit output: hardware implementations

- Fibonnaci



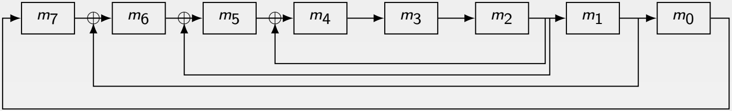
- Galois



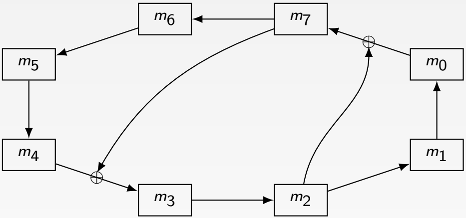
	Critical path	Fan-out	Cost	Diffusion delay
Galois	1	$\approx n/2$	$\approx n/2$	$n-1$
Fibonacci	$\approx n/2$	2	$\approx n/2$	$n-1$

One bit output: hardware implementations

- G. Mrugalski, J. Rajski, and J. Tyszer, 2004



- Ring



	Critical path	Fan-out	Cost	Diffusion delay
Mrugalski & all	2	3	$\approx n/2$	$\approx n/2$
Optimal Ring	1	2	$\approx n/2$	$\approx n/4$

Words oriented software implementations

- Twisted Generalized Feedback Shifts Registers
  Matsumoto & Kurita 1992, Matsumoto & Nishurima 1998

$$A = \begin{pmatrix} 0 & I_w & & & & \\ & 0 & I_w & & (0) & \\ & & 0 & I_w & & \\ & (0) & & \ddots & \ddots & \\ & & & & 0 & I_w \\ I_w & 0 & \cdots & L & 0 & 0 \end{pmatrix}$$

I_w: $w \times w$ identity matrix, L: a $w \times w$ binary matrix.

Words oriented software implementations

- Multiple-Recursive Matrix Method H. Niederreiter 1995, see also Marsaglia 2003 (Xorshift PRNG)

$$A = \begin{pmatrix} 0 & I_w & & & & \\ & 0 & I_w & & (0) & \\ & & 0 & I_w & & \\ & (0) & & \ddots & \ddots & \\ & & & & 0 & I_w \\ A_r & A_{r-1} & A_{r-2} & \dots & A_2 & A_1 \end{pmatrix}$$

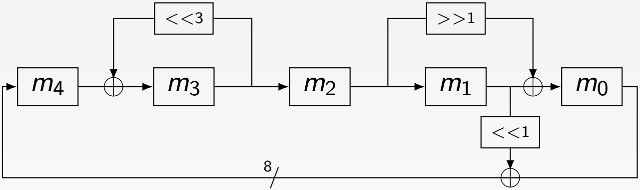
I_w: $w \times w$ identity matrix, A_i: software efficient transformations (right or left shifts, word rotations).

$$q(X) = \det(I - XA) = \det\left(I + \sum_{j=1}^{r} X^j A_j\right)$$

Word-oriented ring LFSRs

- F. Arnault, T.P. B., M. Minier, P. Pousse, 2011

A small example: $A = \begin{pmatrix} & I_8 & R^1 & & \\ & & I_8 & & \\ & & & I_8 & \\ & & & L^3 & I_8 \\ I_8 & L^1 & & & \end{pmatrix}$



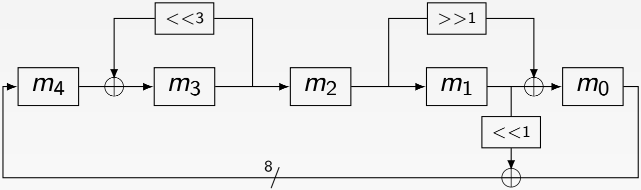
Optimal, both in hardware and software.

Problem How to construct good word-ring LFSRs ?

Word-oriented ring LFSRs

- F. Arnault, T.P. B., M. Minier, P. Pousse, 2011

A small example: $A = \begin{pmatrix} & I_8 & R^1 & & \\ & & I_8 & & \\ & & & I_8 & \\ & & & L^3 & I_8 \\ I_8 & L^1 & & & \end{pmatrix}$



Optimal, both in hardware and software.

Problem How to construct good word-ring LFSRs ?

l-adic topology

$\mathcal{A}$:unitary commutative ring. $\mathcal{I} = < \pi >$ such that

- π is not a 0 divisor.
- $\bigcap_{n \in \mathbb{N}} \mathcal{I}^n = \{0\}$

Ultrametric distance:

$$d(x,y) = \begin{cases} 2^{-k} & \textit{if} \quad x \neq y \\ 0 & \textit{if} \quad x = y \end{cases} \quad \text{with } k = \max\{n \in \mathbb{N},\ x - y \in \mathcal{I}^n\}$$

Associated l-adic (π-adic) topology.

Topologic completion of $\mathcal{A}$: $\mathcal{A}_{\mathcal{I}}$ (or $\mathcal{A}_{\pi}$).

I-adic topology

$\mathcal{A}$:unitary commutative ring. $\mathcal{I} =< \pi >$ such that

- π is not a 0 divisor.
- $\bigcap_{n\in\mathbb{N}} \mathcal{I}^n = \{0\}$

Ultrametric distance:

$$d(x,y) = \begin{cases} 2^{-k} & if \quad x \neq y \\ 0 & if \quad x = y \end{cases} \quad \text{with } k = \max\{n \in \mathbb{N},\ x - y \in \mathcal{I}^n\}$$

Associated I-adic (π-adic) topology.

Topologic completion of $\mathcal{A}$: $\mathcal{A}_{\mathcal{I}}$ (or $\mathcal{A}_\pi$).

l-adic topology

$\mathcal{A}$:unitary commutative ring. $\mathcal{I} =< \pi >$ such that

- π is not a 0 divisor.
- $\bigcap_{n\in\mathbb{N}} \mathcal{I}^n = \{0\}$

Ultrametric distance:

$$d(x,y) = \begin{cases} 2^{-k} & \textit{if} \quad x \neq y \quad \text{with } k = \max\{n \in \mathbb{N},\ x-y \in \mathcal{I}^n\} \\ 0 & \textit{if} \quad x = y \end{cases}$$

Associated I-adic (π-adic) topology.

Topologic completion of $\mathcal{A}$: $\mathcal{A}_{\mathcal{I}}$ (or $\mathcal{A}_\pi$).

mod_π **function**

Suppose that there exist 2 functions

$$\mathrm{mod}_\pi : \mathcal{A} \longrightarrow \mathcal{S} \subseteq \mathcal{A} \qquad \mathrm{div}_\pi : \mathcal{A} \longrightarrow \mathcal{A}$$

such that

$$a = \pi\, \mathrm{div}_\pi(a) + \mathrm{mod}_\pi(a) \text{ for all } a$$

Set $\mathcal{S} = \mathrm{mod}_\pi(\mathcal{A})$.

More requirement:

- $\mathcal{S}$ is a set of representatives of $\mathcal{A}/(\pi)$
- $0, 1 \in \mathcal{S}$.

mod_π function

Suppose that there exist 2 functions

$$\text{mod}_\pi : \mathcal{A} \longrightarrow \mathcal{S} \subseteq \mathcal{A} \qquad\qquad \text{div}_\pi : \mathcal{A} \longrightarrow \mathcal{A}$$

such that

$$a = \pi \,\text{div}_\pi(a) + \text{mod}_\pi(a) \text{ for all } a$$

Set $\mathcal{S} = \text{mod}_\pi(\mathcal{A})$.

More requirement:

- $\mathcal{S}$ is a set of representatives of $\mathcal{A}/(\pi)$
- $0, 1 \in \mathcal{S}$.

Convergence

For $a \in \mathcal{A}$, set $\mathrm{seq}_\pi(a) = (s_n)_{n\in\mathbb{N}}$ with

$$s_n = \mathrm{mod}_\pi(\mathrm{div}_\pi{}^n(a)).$$

Theorem

Set $a \in \mathcal{A}$ and $s = \mathrm{seq}_\pi(a)$. The series $\sum_{n\in\mathbb{N}} s_n\pi^n \in \mathcal{A}_\pi$ is convergent in $\mathcal{A}_\pi$, moreover $a = \sum_{n\in\mathbb{N}} s_n\pi^n$.

“Integers”

Integers

$$\mathcal{F} = \{a \in \mathcal{A}_\pi \mid \exists n \in \mathbb{N}^*, {\mathrm{div}_\pi}^n(a) = 0\}.$$

Signed integers

$$\mathcal{Z} = \{a - b \mid a, b \in \mathcal{F}\}.$$

arithmetic

If $\mathcal{S}$ is finite, elements of $\mathcal{Z}$ are representable on computers

If $s + t$ and st are in $\mathcal{Z}$ and known, it is possible to provide an effective arithmetic on $\mathcal{Z}$.

Periodic elements

Set $\mathcal{P}$ the set of periodic elements of $\mathcal{A}_\pi$, i.e. such that $\mathrm{seq}_\pi(a)$ is ultimately periodic.

Lemma

$$\mathcal{P} = \{p = a' p(T) + a''\}$$

with a', $a'' \in \mathcal{Z}$ *and* $p(T) = \sum_{i=0}^{\infty} p^{iT}$ $(= 1/(1 - p^T))$.

Proposition

$$\mathcal{Z} \subseteq \mathcal{P}.$$

Rational elements

Set $\mathcal{Q} = \{u/v \mid u,\ v \in \mathcal{Z},\ v \text{ invertible in } \mathcal{Z}_\pi\}$.

Lemma

$a \in \mathcal{Z}$ is invertible in $\mathcal{Z}_\pi$

$$\Leftrightarrow$$

$s_0 = \mathrm{mod}_\pi(a)$ is invertible in $\mathcal{Z}$.

Proposition

$$\mathcal{Q} = \{u/(1+\pi v) \mid u,\ v \in \mathcal{Z}\}$$

Proposition

$$\mathcal{P} \subseteq \mathcal{Q}.$$

AFSM automata

Definition

An algebraic automata on $\mathcal{Z}$ of size $n \in \mathbb{N}^*$ is constituted of

- a set of states $(m, c) \in \mathcal{S}^n \times \mathcal{A}_\pi^n$
- a transition function given by a $n \times n$ matrix T with coefficients in $\mathcal{A}_\pi$.

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

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

AFSM automata

$M(t) = (M_0(t), ..., M_{n-1}(t))$ is the n-tuple of π-adic integers observed in the cells m_0, m_{n-1} from time t.

Proposition

$$M(t+1) = TM(t) + c(t).$$

Theorem

If the automaton is in state (m, c) at time t_0, then

$$M(t_0) = \frac{\mathrm{adj}(I - \pi T)}{\det(I - \pi T)} \cdot (m(t_0) + \pi c(t_0))$$

Problem: an algebraic automaton is not necessary finite.

AFSM automata

$M(t) = (M_0(t), \ldots, M_{n-1}(t))$ is the n-tuple of π-adic integers observed in the cells m_0, m_{n-1} from time t.

Proposition

$$M(t+1) = TM(t) + c(t).$$

Theorem

If the automaton is in state (m, c) at time t_0, then

$$M(t_0) = \frac{\operatorname{adj}(I - \pi T)}{\det(I - \pi T)} \cdot (m(t_0) + \pi c(t_0))$$

Problem: an algebraic automaton is not necessary finite.

AFSM automata

$M(t) = (M_0(t), \dots, M_{n-1}(t))$ is the n-tuple of π-adic integers observed in the cells m_0, m_{n-1} from time t.

Proposition

$$M(t+1) = TM(t) + c(t).$$

Theorem

If the automaton is in state (m, c) at time t_0, then

$$M(t_0) = \frac{\text{adj}(I - \pi T)}{\det(I - \pi T)} \cdot (m(t_0) + \pi c(t_0))$$

Problem: an algebraic automaton is not necessary finite.

Example: $\mathcal{A} = \mathbb{F}_2[x]$

- $\mathcal{A} = \mathbb{F}_2[x]$, $\pi = x$, T with coefficients in $\mathbb{F}_2$

  $\Rightarrow$ classical binary LFSRs (or LFSMs).

- $\mathcal{A} = \mathbb{F}_2[x]$, $\pi = x^d$, T with coefficients $t_{i,j}(x)$, $deg(t_{i,j}) < d$

  $\Rightarrow$ d-parallelized binary LFSRs .

- $\mathcal{A} = \mathbb{F}_2[x]$, $\pi = x$ and T with rational coefficients

  $\Rightarrow$ Global definition of binary LFSRs .

An example of global description

$$T = \begin{pmatrix} 0 & P_1(X)/Q_1(X) & 0 \\ 0 & 0 & P_2(X)/Q_2(X) \\ P_3(X)/Q_3(X) & 0 & 0 \end{pmatrix}$$

$$\det(I - XT) = \frac{Q_1(X)Q_2(X)Q_3(X) + X^3 P_1(X)P_2(X)P_3(X)}{Q_1(X)Q_2(X)Q_3(X)}$$

An example of global description

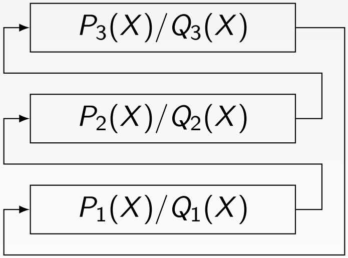
$$T = \begin{pmatrix} 0 & P_1(X)/Q_1(X) & 0 \\ 0 & 0 & P_2(X)/Q_2(X) \\ P_3(X)/Q_3(X) & 0 & 0 \end{pmatrix}$$

$$\det(I - XT) = \frac{Q_1(X)Q_2(X)Q_3(X) + X^3 P_1(X)P_2(X)P_3(X)}{Q_1(X)Q_2(X)Q_3(X)}$$

An example of global description

$$T = \begin{pmatrix} 0 & P_1(X)/Q_1(X) & 0 \\ 0 & 0 & P_2(X)/Q_2(X) \\ P_3(X)/Q_3(X) & 0 & 0 \end{pmatrix}$$

$$\det(I - XT) = \frac{Q_1(X)Q_2(X)Q_3(X) + X^3 P_1(X)P_2(X)P_3(X)}{Q_1(X)Q_2(X)Q_3(X)}$$



Example: $\mathcal{A} = \mathbb{Z}$

- $\pi = 2$, T binary

  $\Rightarrow$ 2-adic integers, classical FCSRs (Feedback with Carry Shift Registers).

- $\pi = 2$, T with coefficients in $\mathbb{Z}$: a more general framework
  can be always realized with binary FCSRs

All the software or hardware oriented design of LFSRs can be directly applied to FCSRs!

Example: $\mathcal{A} = \mathbb{Z}$

- $\pi = 2$, T binary

  $\Rightarrow$ 2-adic integers, classical FCSRs (Feedback with Carry Shift Registers).

- $\pi = 2$, T with coefficients in $\mathbb{Z}$: a more general framework can be always realized with binary FCSRs

All the software or hardware oriented design of LFSRs can be directly applied to FCSRs!

Example: $\mathcal{A} = \mathbb{Z}$

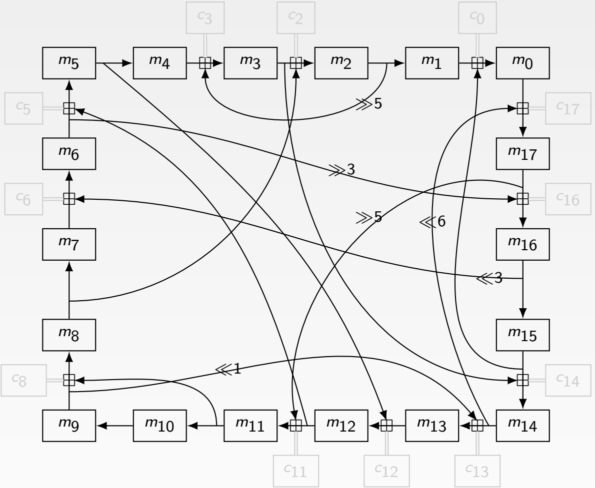
- $\pi = 2$, T binary

  $\Rightarrow$ 2-adic integers, classical FCSRs (Feedback with Carry Shift Registers).

- $\pi = 2$, T with coefficients in $\mathbb{Z}$: a more general framework can be always realized with binary FCSRs

All the software or hardware oriented design of LFSRs can be directly applied to FCSRs!

FCSR automaton for GLUON 64

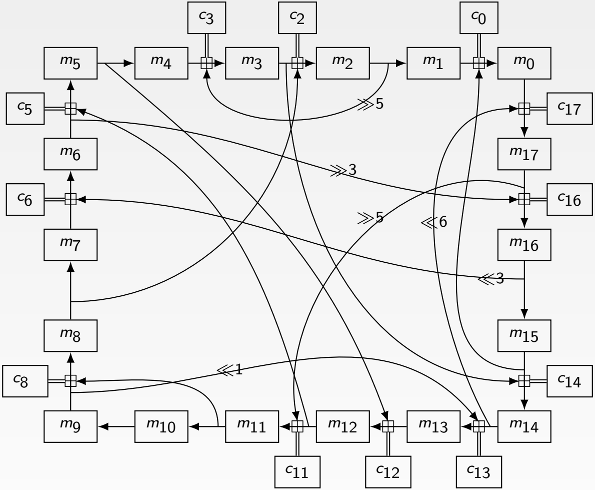


18 blocs of 8 bits

FCSR of 144 bits

+ 73 bits of carries

FCSR automaton for GLUON 64



18 blocs of 8 bits

FCSR of 144 bits

+ 73 bits of carries

Corresponding matrix

$$T = \begin{pmatrix}
0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 \\
0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & I & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & SR^5 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & SL^3 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & SR^5 \\
0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & SL^1 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 \\
0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & SR^3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I \\
I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & SL^6 & 0 & 0 & 0
\end{pmatrix}$$

Example: $\mathcal{A} = \mathbb{Z}[x]/p(x)$, $p(x)$ unitary

- $p(x) = x^d - \sum_{i=0}^{d-1} \epsilon_i x^i$, $\epsilon_i \in \{0, 1\}$, $\pi = 2$.

  $\Rightarrow$ V-FCSRs introduced by Allailou, Marjane and Mokrane for Galois and Fibonnaci mode.
  Can be generalized to any mode.
  In fact, the practical implementation of V-FCSRs is nothing else than non-optimal binary FCSRs. [1]

- $p(x) = x^d - n$, $\pi = x$.

  $\Rightarrow$ $\mathcal{A} = \mathbb{Z}[\sqrt[d]{n}]$ and $\pi = \sqrt[d]{n}$. Generalization introduced by Klapper et Goresky.
  Decimation of sequences leads to classical FCSRs.

[1] Berger T.P., Minier M., Cryptanalysis of Pseudo-random Generators Based on Vectorial FCSRs, Indocrypt 2012, Kolkata.

Example: $\mathcal{A} = \mathbb{Z}[x]/p(x)$, $p(x)$ unitary

- $p(x) = x^d - \sum_{i=0}^{d-1} \epsilon_i x^i$, $\epsilon_i \in \{0,1\}$, $\pi = 2$.

  $\Rightarrow$ V-FCSRs introduced by Allailou, Marjane and Mokrane for Galois and Fibonnaci mode.
  Can be generalized to any mode.
  In fact, the practical implementation of V-FCSRs is nothing else than non-optimal binary FCSRs. [1]

- $p(x) = x^d - n$, $\pi = x$.

  $\Rightarrow$ $\mathcal{A} = \mathbb{Z}[\sqrt[d]{n}]$ and $\pi = \sqrt[d]{n}$. Generalization introduced by Klapper et Goresky.
  Decimation of sequences leads to classical FCSRs.

[1] Berger T.P., Minier M., Cryptanalysis of Pseudo-random Generators Based on Vectorial FCSRs, Indocrypt 2012, Kolkata.

Example: $\mathcal{A} = \mathbb{Z}[x]/p(x)$, $p(x)$ unitary

- $p(x) = x^d - \sum_{i=0}^{d-1} \epsilon_i x^i$, $\epsilon_i \in \{0, 1\}$, $\pi = 2$.

  $\Rightarrow$ V-FCSRs introduced by Allailou, Marjane and Mokrane for Galois and Fibonnaci mode.
  Can be generalized to any mode.
  In fact, the practical implementation of V-FCSRs is nothing else than non-optimal binary FCSRs. [1]

- $p(x) = x^d - n$, $\pi = x$.

  $\Rightarrow$ $\mathcal{A} = \mathbb{Z}[\sqrt[d]{n}]$ and $\pi = \sqrt[d]{n}$. Generalization introduced by Klapper et Goresky.
  Decimation of sequences leads to classical FCSRs.

[1] Berger T.P., Minier M., Cryptanalysis of Pseudo-random Generators Based on Vectorial FCSRs, Indocrypt 2012, Kolkata.

Example: $\mathcal{A} = \mathbb{Z}[x]/p(x)$, $p(x)$ unitary

- $p(x) = x^d - \sum_{i=0}^{d-1} \epsilon_i x^i$, $\epsilon_i \in \{0, 1\}$, $\pi = 2$.

  $\Rightarrow$ V-FCSRs introduced by Allailou, Marjane and Mokrane for Galois and Fibonnaci mode.
  Can be generalized to any mode.
  In fact, the practical implementation of V-FCSRs is nothing else than non-optimal binary FCSRs. [1]

- $p(x) = x^d - n$, $\pi = x$.

  $\Rightarrow$ $\mathcal{A} = \mathbb{Z}[\sqrt[d]{n}]$ and $\pi = \sqrt[d]{n}$. Generalization introduced by Klapper et Goresky.
  Decimation of sequences leads to classical FCSRs.

[1] Berger T.P., Minier M., Cryptanalysis of Pseudo-random Generators Based on Vectorial FCSRs, Indocrypt 2012, Kolkata.

A new example?

$\mathcal{A} = \mathbb{Z}[x]/p(x)$, $p(x) = \pi(X)^d - N$ unitary

- In this case, AFSM are finite automata
- It seems that they cannot be reduced to classical FCSRs.
- Reconstruction algorithms for such sequences?