

Synthesis (compilation) of shift register

Cédric Lauradoux

January 22, 2007

Linear Feedback Shift Registers

Theory

- ▶ Multiplication in a finite field: $s \times \alpha$
 - s is an arbitrary polynomial in $\mathbf{F}_q[X]$
 - α is a root of P in $\mathbf{F}_q[X]$
 - P is called the LFSR characteristic polynomial

Linear Feedback Shift Registers

Galois setup

► Polynomial basis:

$$\alpha s = (s_{m-1}a_{m-1} + s_{m-2})\alpha^{m-1} + \dots + (s_{m-1}a_0 + s_0)\alpha + s_{m-1}$$



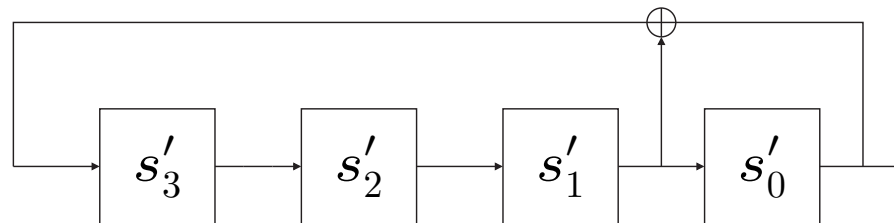
Linear Feedback Shift Registers

Fibonacci setup

► Dual basis:

$$(\alpha s)'_j = s'_{j+1}, j = 0, 1, \dots, m - 2$$

$$(\alpha s)'_{m-1} = \text{Tr}(s\alpha^m) = a_{m-1}s'_{m-1} + \dots + a_1s'_1 + s'_0$$



Linear Feedback Shift Registers

Parameters

$$P(X) = 1 + X^{d_1} + X^{d_2} + \dots + X^{d_{w-2}} + X^m$$

with $d_1 < d_2 < \dots < d_{w-1}$

► Critical Parameters:

- w number of monomials
- d_1 tail coefficient
- d_{w-2} head coefficient
- m degree of P

Linear Feedback Shift Registers

- ▶ Where are they used?
 - Encoder, scramblers, spread-spectrum
 - Build In Self Test
 - Stream ciphers
 - PRNG. . .

Outline

- ▶ Compilation
 - ▷ Bit Parallelism
 - ▷ Unrolling factor
- ▶ Non-Linear Feedback Shift Register
- ▶ Perspectives

Compilation

Why studying LFSRs software synthesis ?

Synthesis

IWYS

- ▶ Implement What You See (IWYS)
 - Compute one feedback
 - Shift by one bit
- ▶ Single bit manipulation
 - Easy for hardware
 - Inefficient in software

Synthesis

Throughput

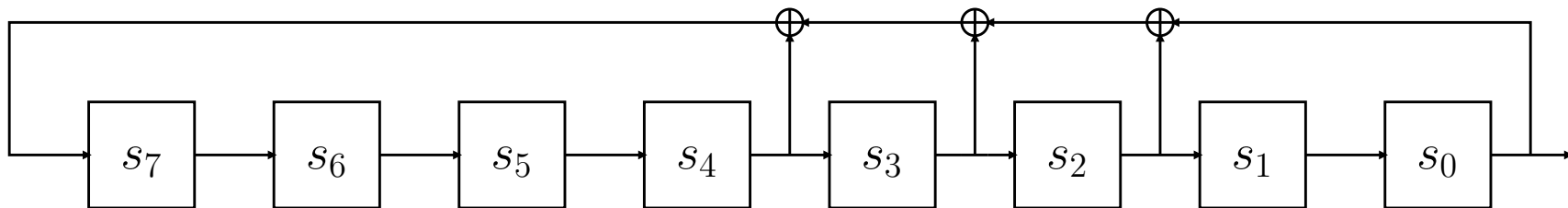
- ▶ How to improve ?

Compute more than one step in one clock cycle

Multiple step

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

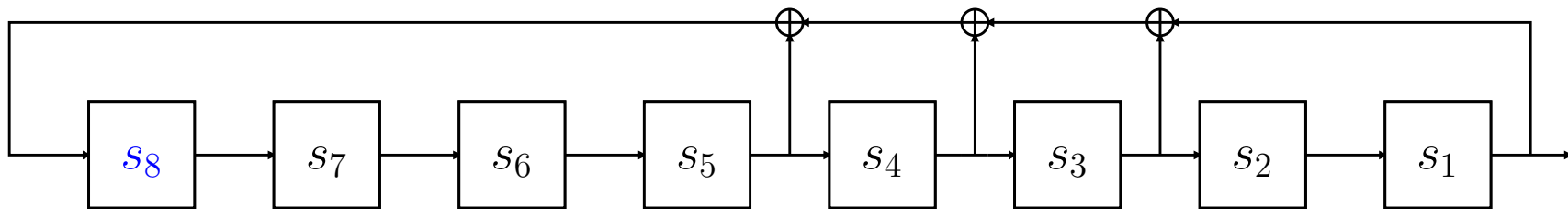
$T = 0$



Multiple step

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

$T = 1$

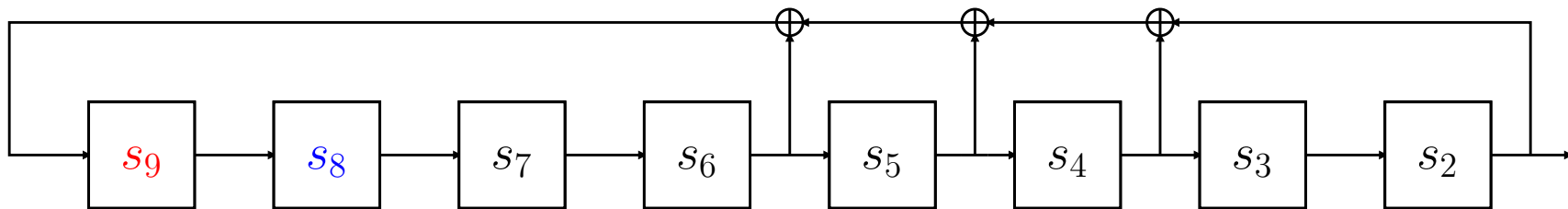


$$s_8 = s_0 \oplus s_2 \oplus s_3 \oplus s_4$$

Multiple step

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

$$T = 2$$

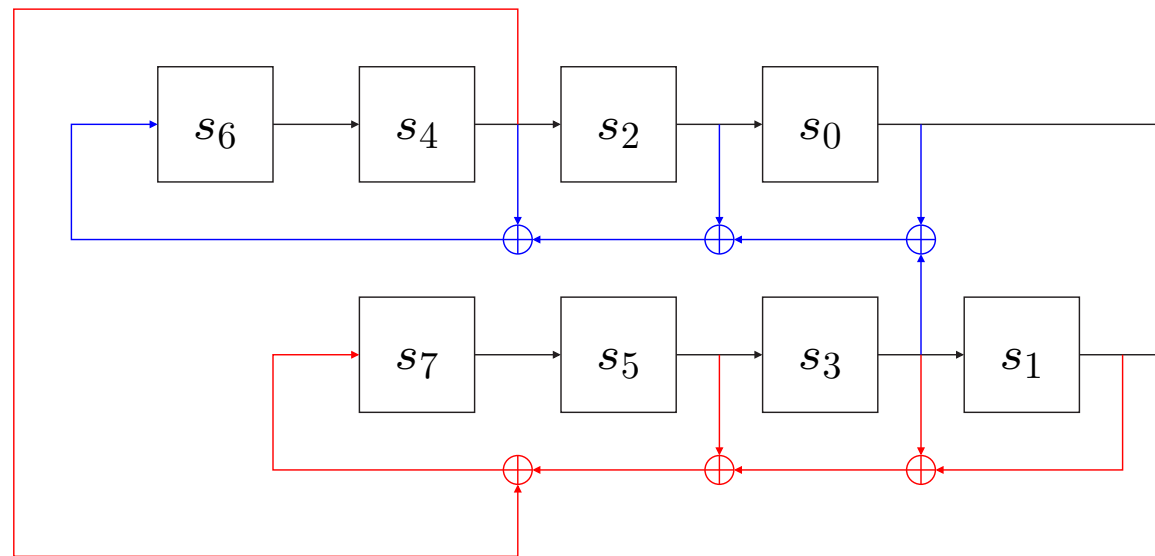


$$s_8 = s_0 \oplus s_2 \oplus s_3 \oplus s_4$$

$$s_9 = s_1 \oplus s_3 \oplus s_4 \oplus s_5$$

Multiple step

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$



$$s_8 = s_0 \oplus s_2 \oplus s_3 \oplus s_4$$

$$s_9 = s_1 \oplus s_3 \oplus s_4 \oplus s_5$$

Compilation

- ▶ New parameters:
 - r processor register width
 - k number of feedback computed
- Improve datapath usage (bit parallelism)
- Determine the best unrolling factor (k)

Compilation

Bit parallelism

Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

$$s_8 = s_4 \oplus s_3 \oplus s_2 \oplus s_0$$

Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

$$\begin{aligned} s_8 &= s_4 \oplus s_3 \oplus s_2 \oplus s_0 \\ s_9 &= s_5 \oplus s_4 \oplus s_3 \oplus s_1 \end{aligned}$$

Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

$$\begin{aligned} s_8 &= s_4 \oplus s_3 \oplus s_2 \oplus s_0 \\ s_9 &= s_5 \oplus s_4 \oplus s_3 \oplus s_1 \\ s_{10} &= s_6 \oplus s_5 \oplus s_4 \oplus s_2 \\ s_{11} &= s_7 \oplus s_6 \oplus s_5 \oplus s_3 \end{aligned}$$

Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

$$\begin{aligned} s_8 &= s_4 \oplus s_3 \oplus s_2 \oplus s_0 \\ s_9 &= s_5 \oplus s_4 \oplus s_3 \oplus s_1 \\ s_{10} &= s_6 \oplus s_5 \oplus s_4 \oplus s_2 \\ s_{11} &= s_7 \oplus s_6 \oplus s_5 \oplus s_3 \\ s_{12} &= s_8 \oplus s_7 \oplus s_6 \oplus s_4 \\ s_{13} &= s_9 \oplus s_8 \oplus s_7 \oplus s_5 \\ s_{14} &= s_{10} \oplus s_9 \oplus s_8 \oplus s_6 \\ s_{15} &= s_{11} \oplus s_{10} \oplus s_9 \oplus s_7 \end{aligned}$$

Compilation

Windows

- ▶ 4 kinds of windows:
 - Aligned windows: **nothing to do**
 - Unaligned windows: 1 shift
 - Overlapping windows: 2 shifts and 1 xor
 - Truncated windows: **it depends. . .**

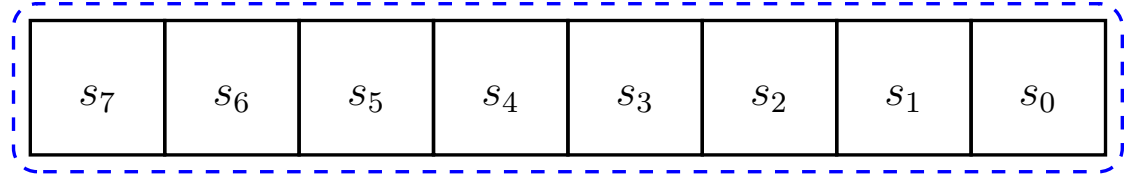
Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

s_7	s_6	s_5	s_4	s_3	s_2	s_1	s_0
-------	-------	-------	-------	-------	-------	-------	-------

Compilation

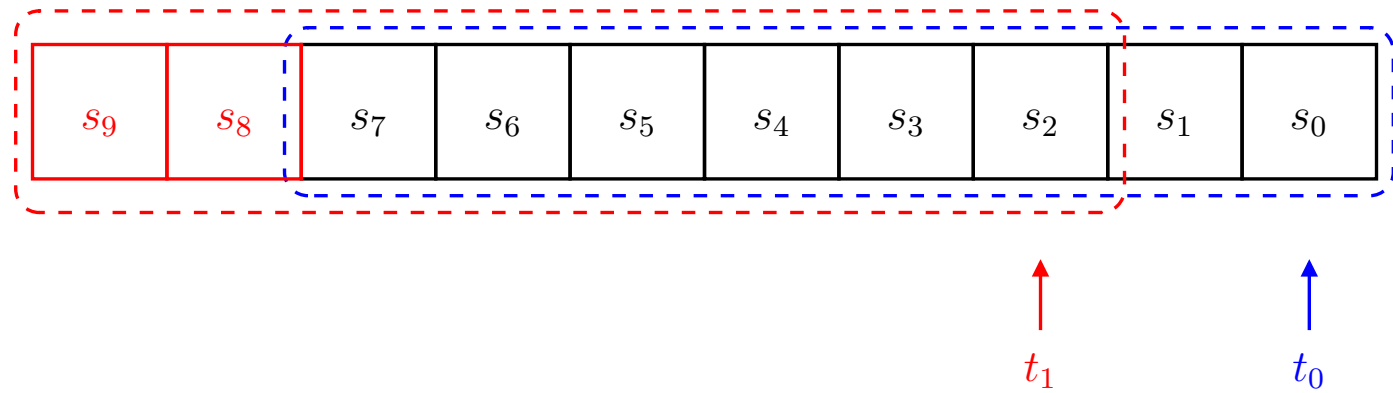
$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$



\uparrow
 t_0

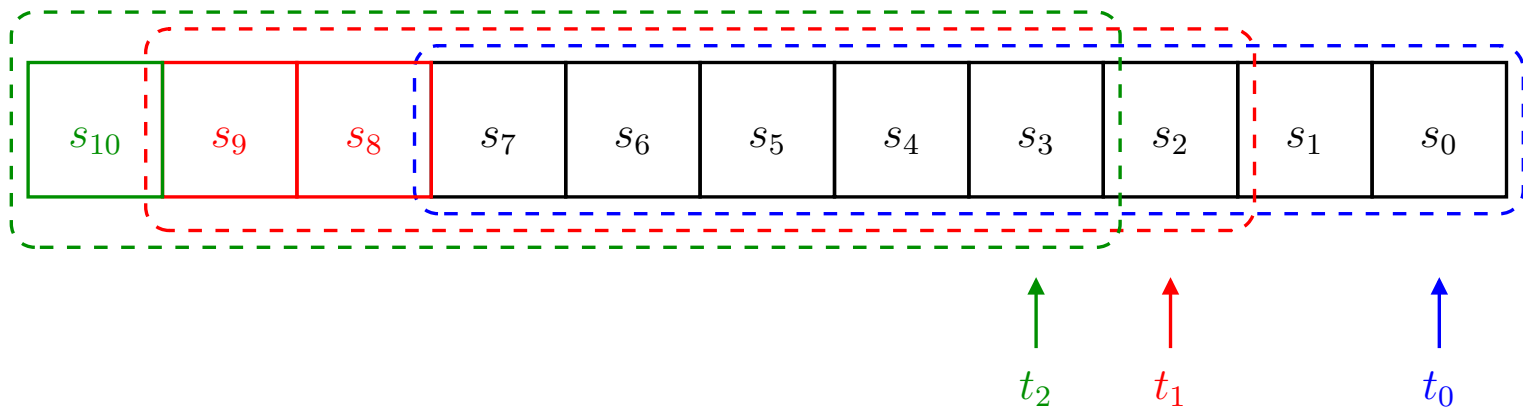
Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$



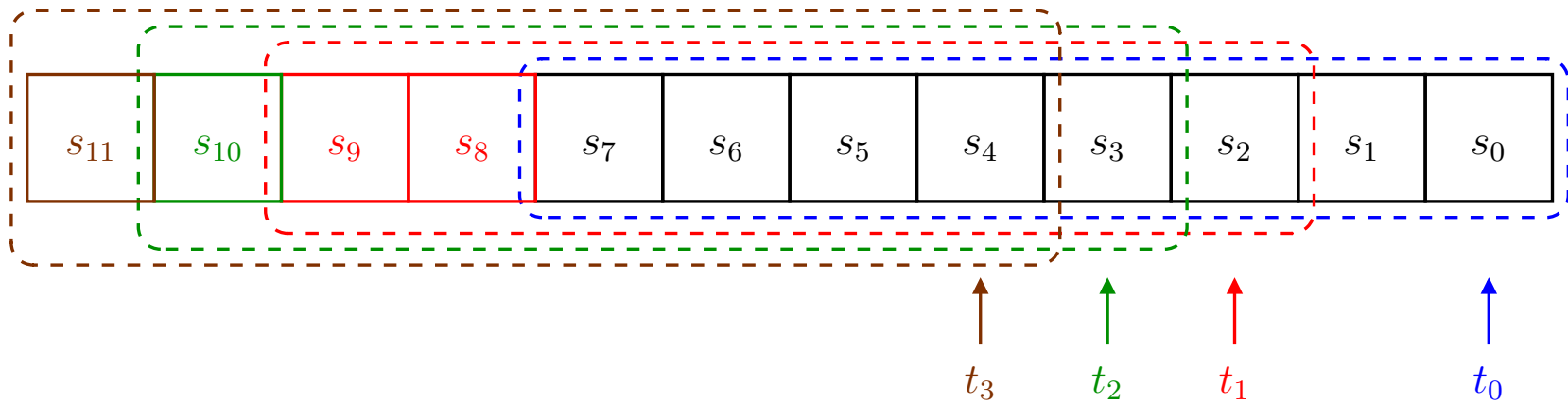
Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$



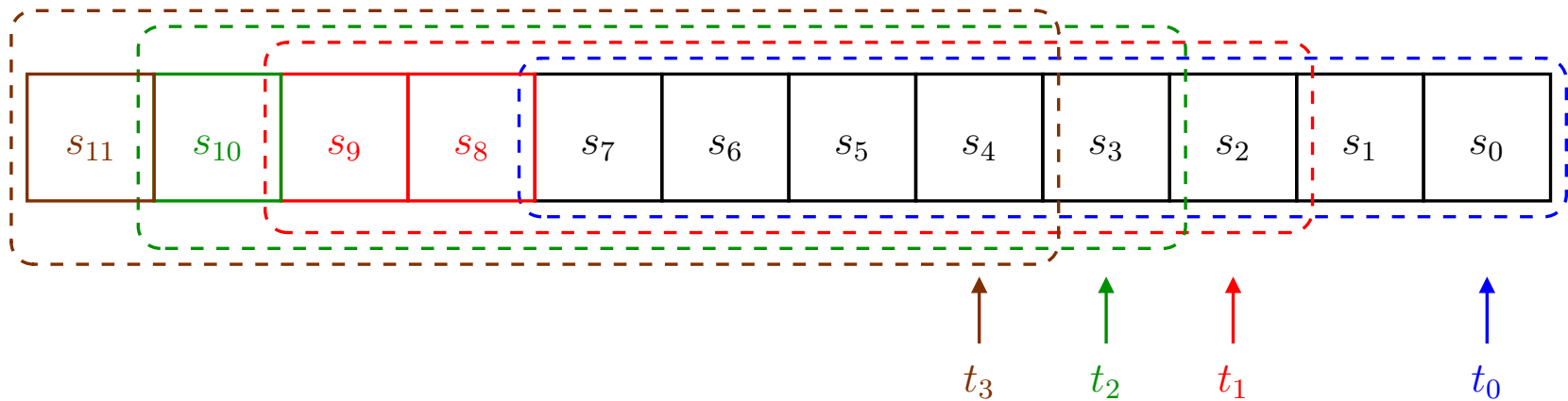
Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$



Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$



How to get s_8, s_9, s_{10}, s_{11} ?

Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

$$\begin{aligned} s_8 &= s_4 \oplus s_3 \oplus s_2 \oplus s_0 \\ s_9 &= s_5 \oplus s_4 \oplus s_3 \oplus s_1 \\ s_{10} &= s_6 \oplus s_5 \oplus s_4 \oplus s_2 \\ s_{11} &= s_7 \oplus s_6 \oplus s_5 \oplus s_3 \\ s_{12} &= s_8 \oplus s_7 \oplus s_6 \oplus s_4 \\ s_{13} &= s_9 \oplus s_8 \oplus s_7 \oplus s_5 \\ s_{14} &= s_{10} \oplus s_9 \oplus s_8 \oplus s_6 \\ s_{15} &= s_{11} \oplus s_{10} \oplus s_9 \oplus s_7 \end{aligned}$$

Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

$$\begin{aligned} s_8 &= s_4 \oplus s_3 \oplus s_2 \oplus s_0 \\ s_9 &= s_5 \oplus s_4 \oplus s_3 \oplus s_1 \\ s_{10} &= s_6 \oplus s_5 \oplus s_4 \oplus s_2 \\ s_{11} &= s_7 \oplus s_6 \oplus s_5 \oplus s_3 \\ p_0 &= 0 \oplus s_7 \oplus s_6 \oplus s_4 \\ p_1 &= 0 \oplus 0 \oplus s_7 \oplus s_5 \\ p_2 &= 0 \oplus 0 \oplus 0 \oplus s_6 \\ p_3 &= 0 \oplus 0 \oplus 0 \oplus s_7 \end{aligned}$$

Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

$$\begin{array}{l}
 s_8 = 0 \oplus 0 \oplus 0 \oplus s_8 = s_4 \oplus s_3 \oplus s_2 \oplus s_0 \\
 s_9 = 0 \oplus 0 \oplus 0 \oplus s_9 = s_5 \oplus s_4 \oplus s_3 \oplus s_1 \\
 s_{10} = 0 \oplus 0 \oplus 0 \oplus s_{10} = s_6 \oplus s_5 \oplus s_4 \oplus s_2 \\
 s_{11} = 0 \oplus 0 \oplus 0 \oplus s_{11} = s_7 \oplus s_6 \oplus s_5 \oplus s_3 \\
 s_{12} = s_8 \oplus 0 \oplus 0 \oplus p_0 = 0 \oplus s_7 \oplus s_6 \oplus s_4 \\
 s_{13} = s_9 \oplus s_8 \oplus 0 \oplus p_1 = 0 \oplus 0 \oplus s_7 \oplus s_5 \\
 s_{14} = s_{10} \oplus s_9 \oplus s_8 \oplus p_2 = 0 \oplus 0 \oplus 0 \oplus s_6 \\
 s_{15} = s_{11} \oplus s_{10} \oplus s_9 \oplus p_3 = 0 \oplus 0 \oplus 0 \oplus s_7
 \end{array}$$

Compilation

$$P(X) = X^8 + X^6 + X^5 + X^4 + 1$$

$$1: t_1 \leftarrow v_0 \ggg 2$$

t_1 alignment

$$2: t_2 \leftarrow v_0 \ggg 3$$

t_2 alignment

$$3: t_3 \leftarrow v_0 \ggg 4$$

t_3 alignment

$$4: t_4 \leftarrow v_0 \oplus t_1 \oplus t_2 \oplus t_3$$

partial t_4

$$5: t_4 \leftarrow t_4 \oplus (t_4 \lll 4)$$

t_3 completion

$$6: t_4 \leftarrow t_4 \oplus (t_4 \lll 5)$$

t_2 completion

$$7: t_4 \leftarrow t_4 \oplus (t_4 \lll 6)$$

t_1 completion

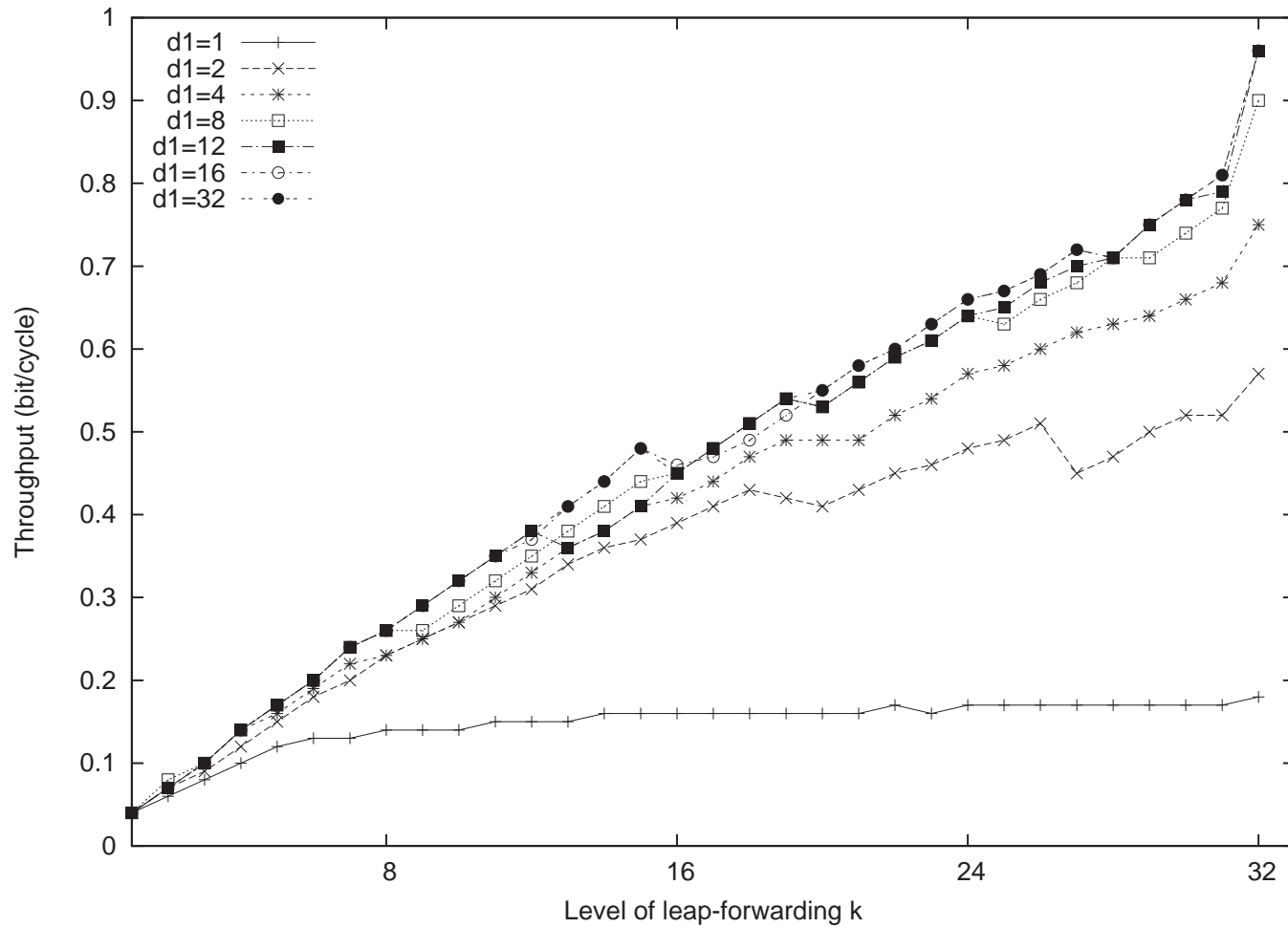
Compilation

Truncated windows

Cost per truncated windows				
Case	Shifts	Xors	And	Subtractions
$d_j \geq k/2$	2	1	0	0
$2 \leq d_j < k/2$	$\lfloor \frac{k-1}{d_j} \rfloor$	$\lfloor \frac{k-1}{d_j} \rfloor$	$\lfloor \frac{k-1}{d_j} \rfloor$	0
$d_1 = 1$	0	$k - 1$	$2(k - 1)$	$k - 1$

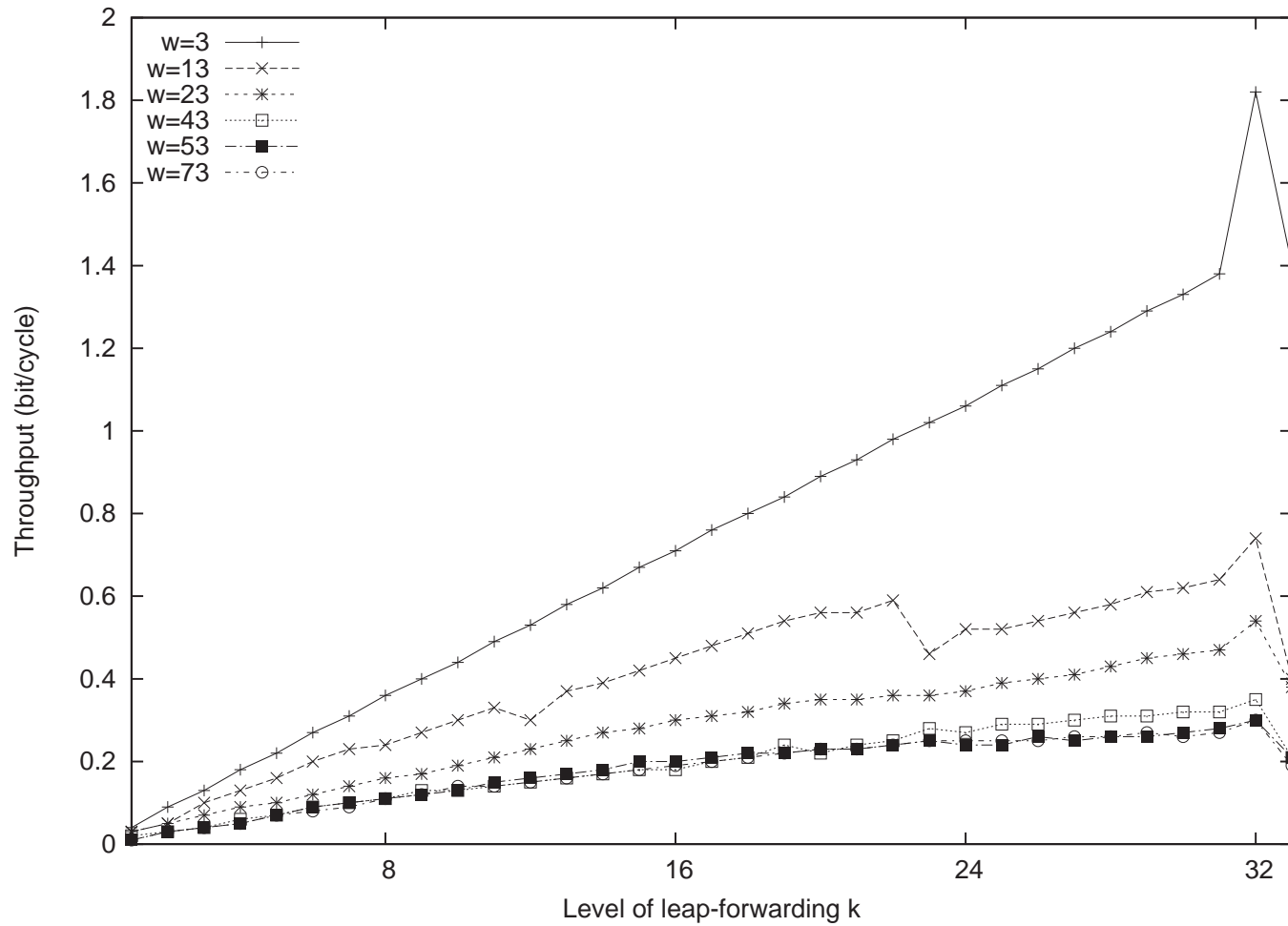
Compilation

$m = 128, w = 10$



Compilation

$m = 128, d_1 = 20$



Compilation

Simplification and subexpressions

$$F = F \oplus (s_0 \gg 4)$$

$$F = F \oplus (s_1 \gg 4)$$

$$F = F \oplus (s_1 \gg 7)$$

$$F = F \oplus (s_0 \gg 7)$$

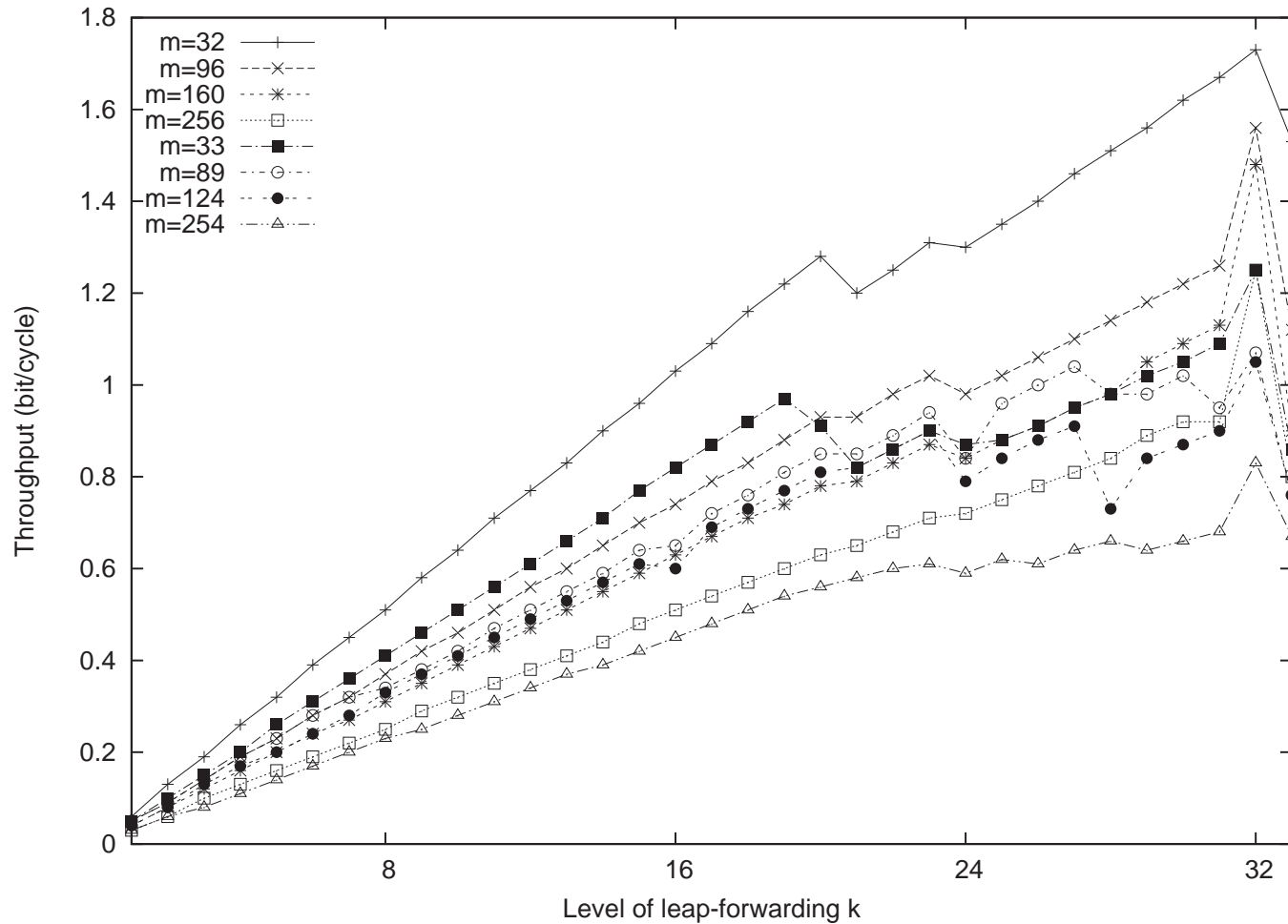
Compilation

Simplification and subexpressions

$$\begin{array}{l} F = F \oplus (s_0 \gg 4) \\ F = F \oplus (s_1 \gg 4) \\ F = F \oplus (s_1 \gg 7) \\ F = F \oplus (s_0 \gg 7) \end{array} \begin{array}{l} \longrightarrow \\ \longrightarrow \\ \longrightarrow \\ \longrightarrow \end{array} \begin{array}{l} F = F \oplus ((s_0 \oplus s_1) \gg 4) \\ F = F \oplus ((s_0 \oplus s_1) \gg 7) \end{array}$$

Compilation

$$d_1 = 20, w = 5$$

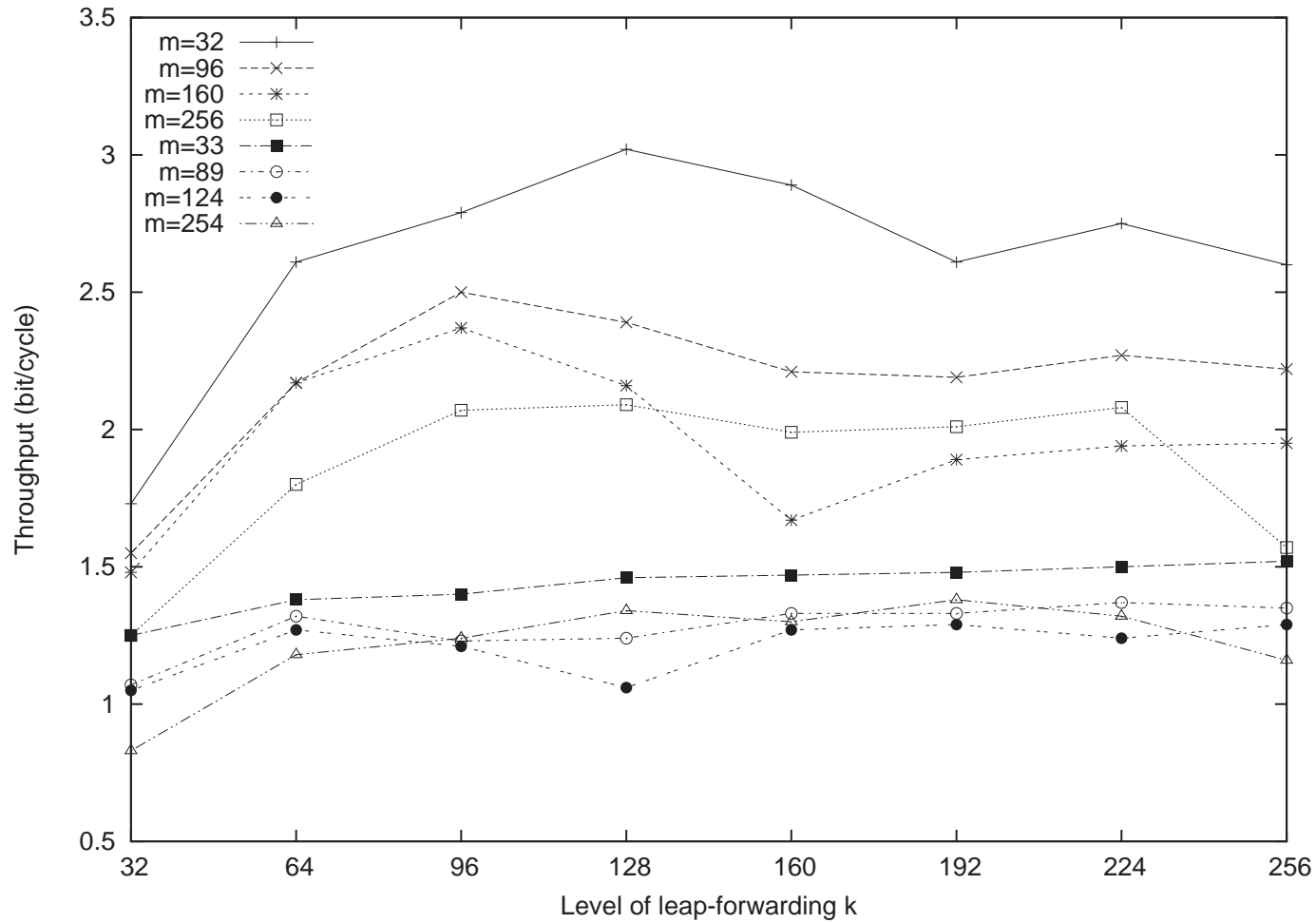


Compilation

Unrolling factor

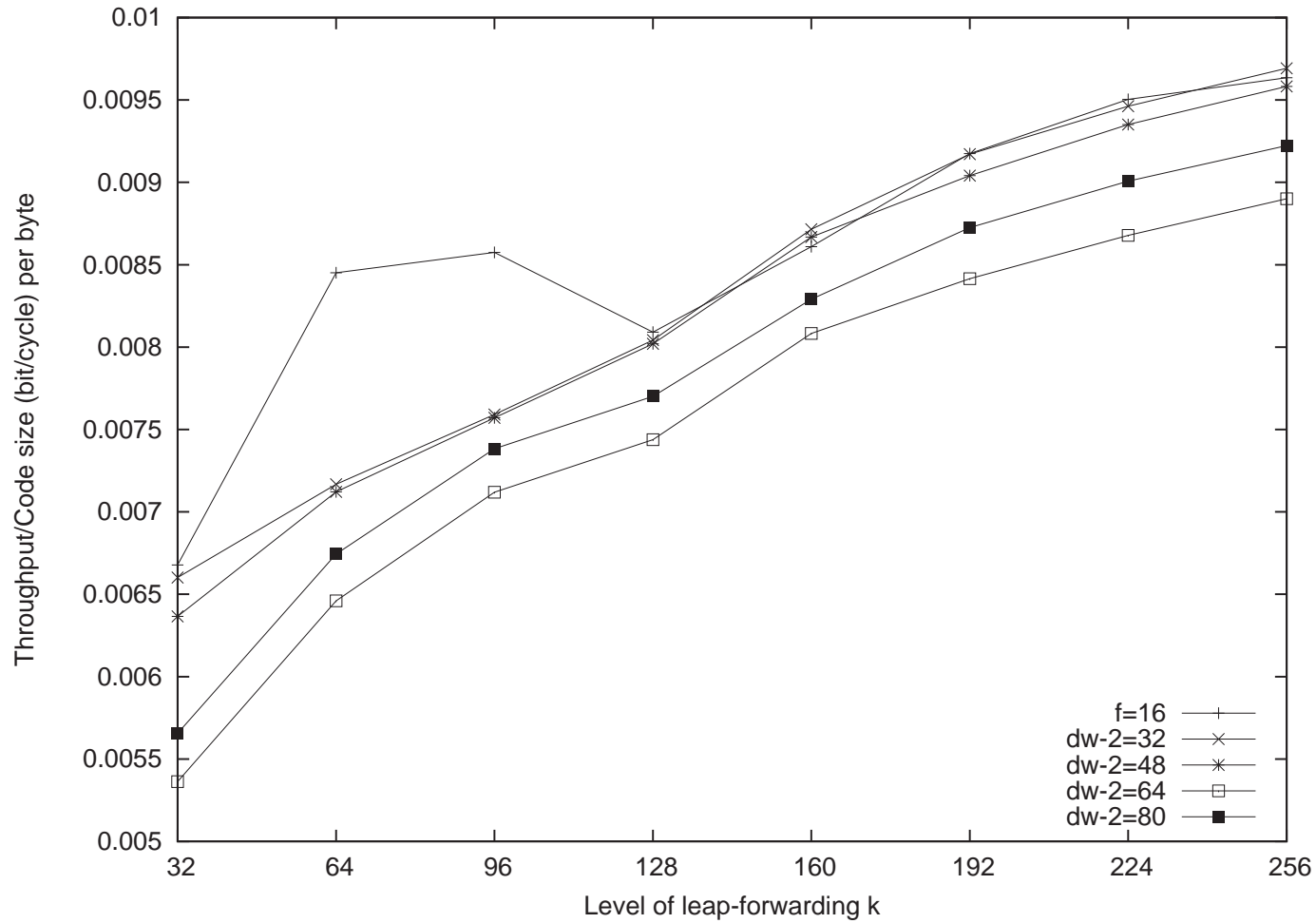
Compilation

$$d_1 = 20, w = 5$$



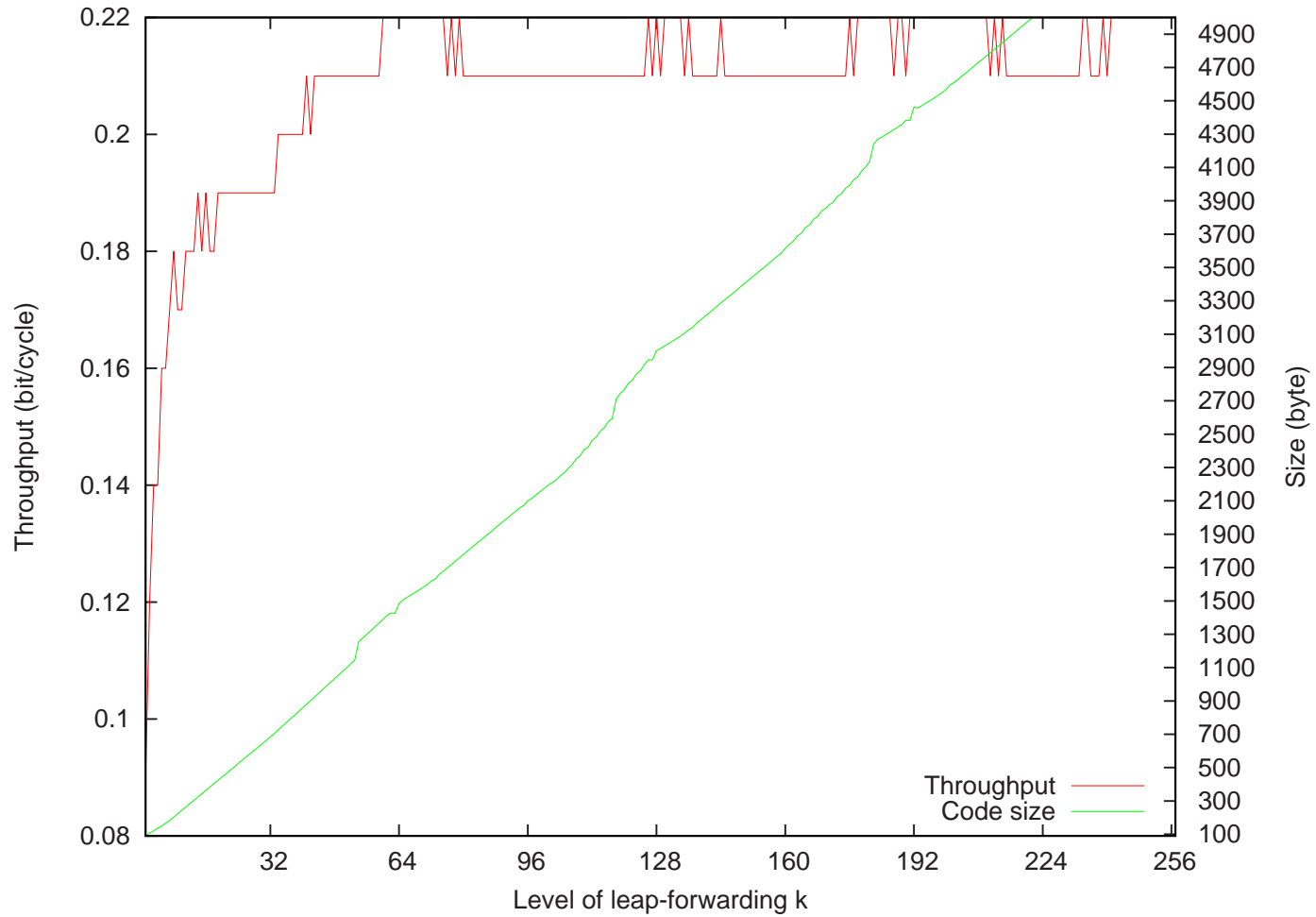
Compilation

$w = 20, d_1 = 10, m = 128$



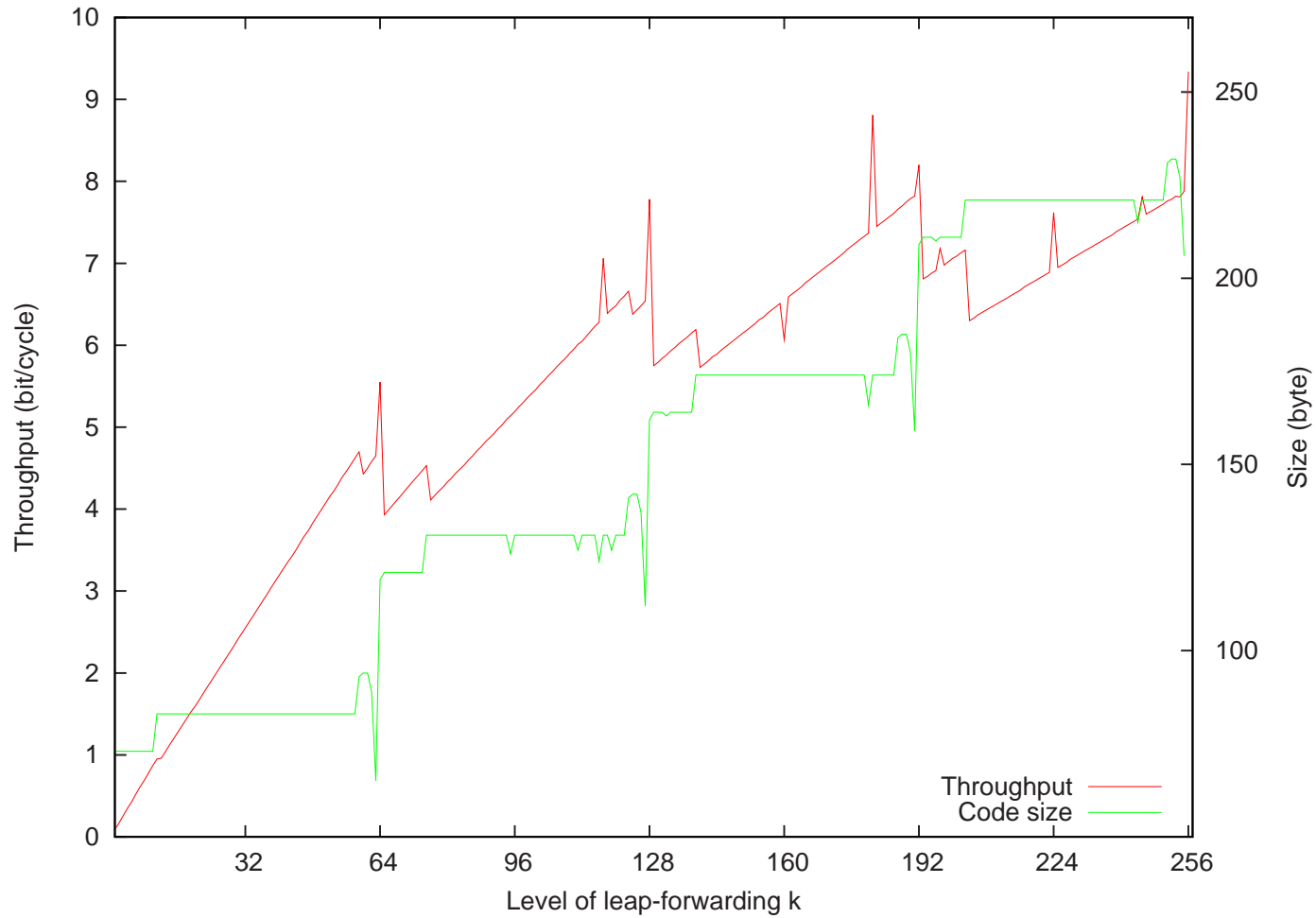
Compilation

$$1 + X + X^{53} + X^{63} + X^{128}$$



Compilation

$$1 + X^{64} + X^{78} + X^{123} + X^{128}$$



Compilation

$$P(X) = X^{128} + X^{32} + X^4 + X^3 + X^2 + X + 1$$

Polynomial	d_1	w	m
$P(X)$	1	7	128
$(1 + X) \times P(X)$	5	6	129
$(X^6 + X^5 + X + 1) \times P(X)$	10	10	134

Compilation

$$P(X) = X^{128} + X^{32} + X^4 + X^3 + X^2 + X + 1$$

Polynomial	best k	Throughput
$P(X)$	64	0.21
$(1 + X) \times P(X)$	512	1.54
$(X^6 + X^5 + X + 1) \times P(X)$	256	1.52

Compilation

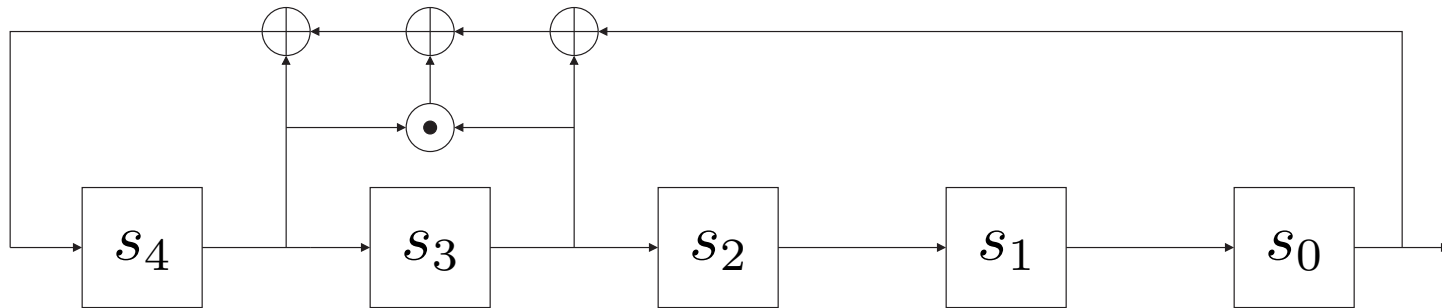
Primitive Polynomial

<http://www-rocq.inria.fr/codes/LFSR/doc/>

$P(X)$	Best k	Throughput
$1 \oplus X^{153} \oplus X^{217}$	576	16.66 bits/cycle
$1 \oplus X^{159} \oplus X^{223}$	576	16.66 bits/cycle

Non-Linear Feedback Shift Register

Truncated windows

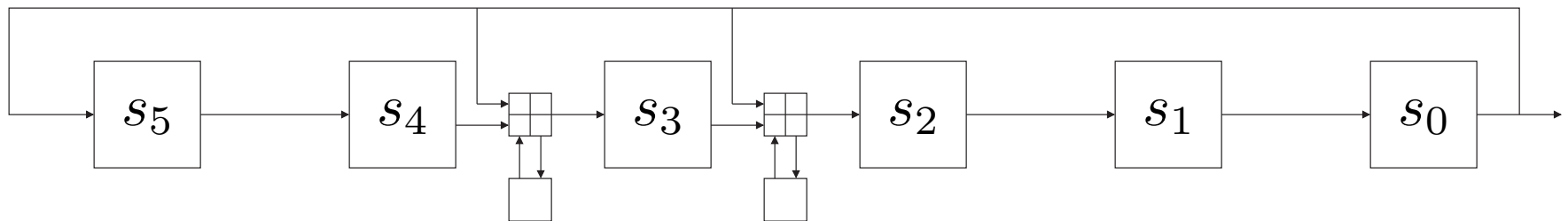


$$s_5 = s_0 \oplus s_3 \oplus s_3 s_4 \oplus s_4$$

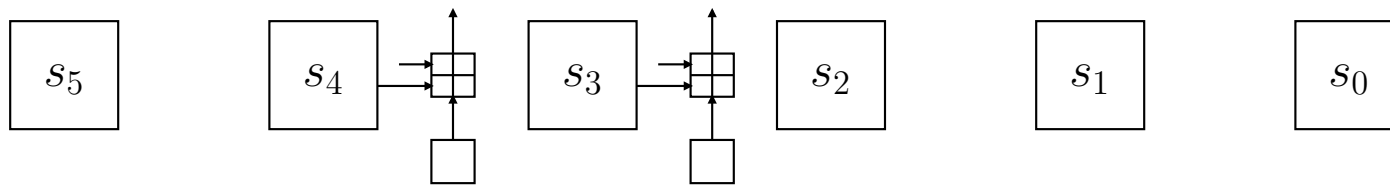
$$s_6 = s_1 \oplus s_4 \oplus s_4 s_5 \oplus s_5$$

Feedback with Carry Shift Registers

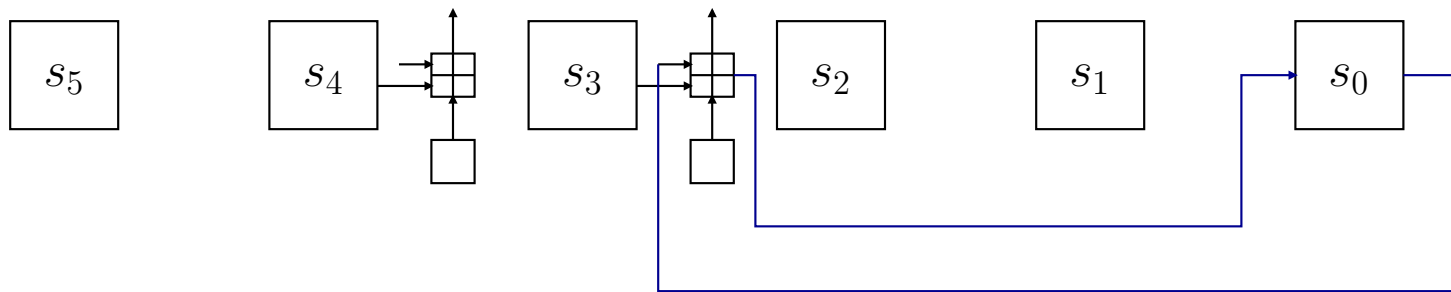
- ▶ Introduced by Klapper and Goresky in 1994
- ▶ Like LFSRs:
 - a variant of Berlekamp-Massey
 - a Galois and Fibonacci setup



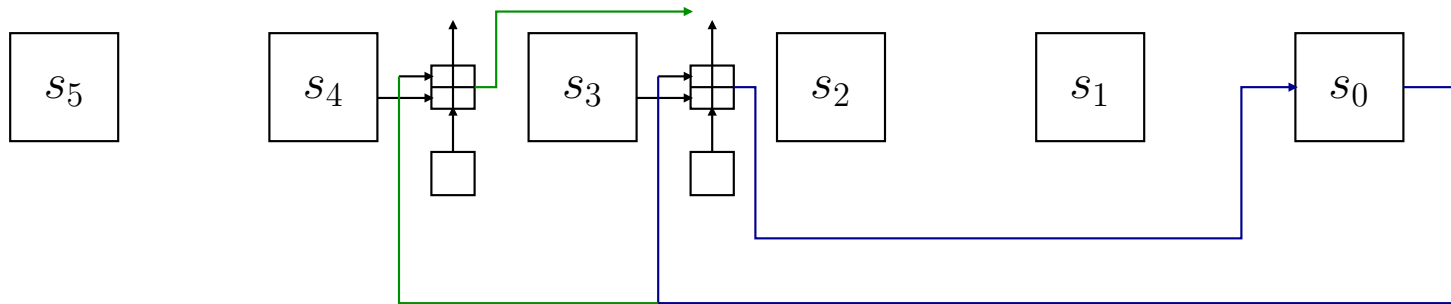
Feedback with Carry Shift Registers



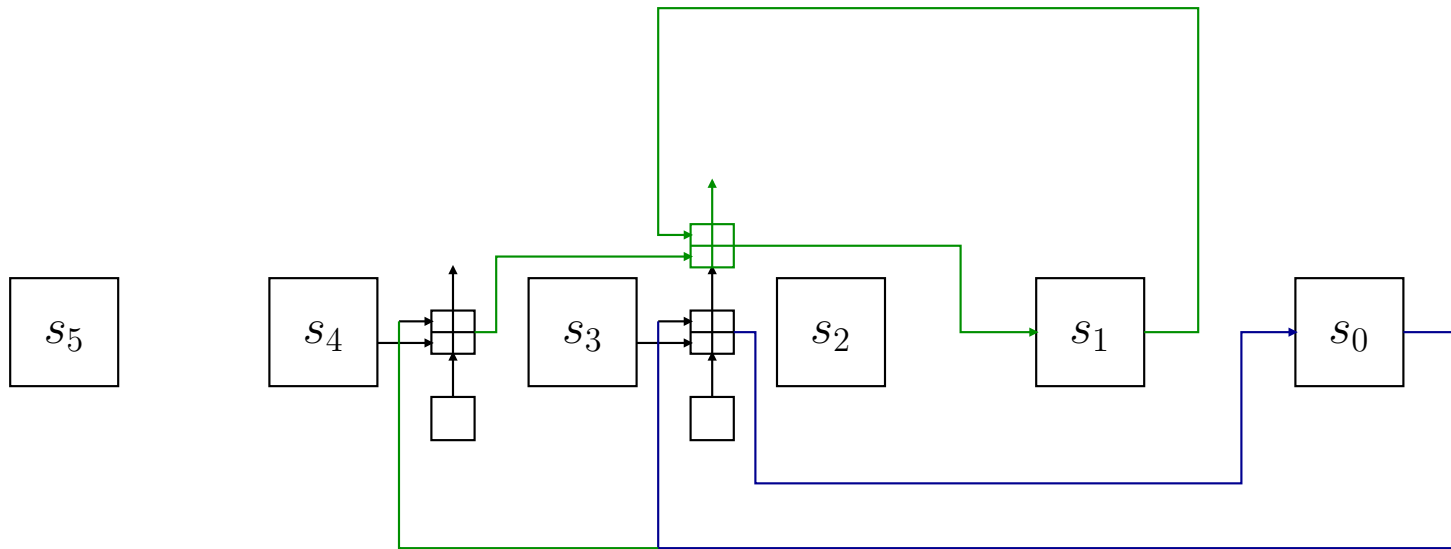
Feedback with Carry Shift Registers



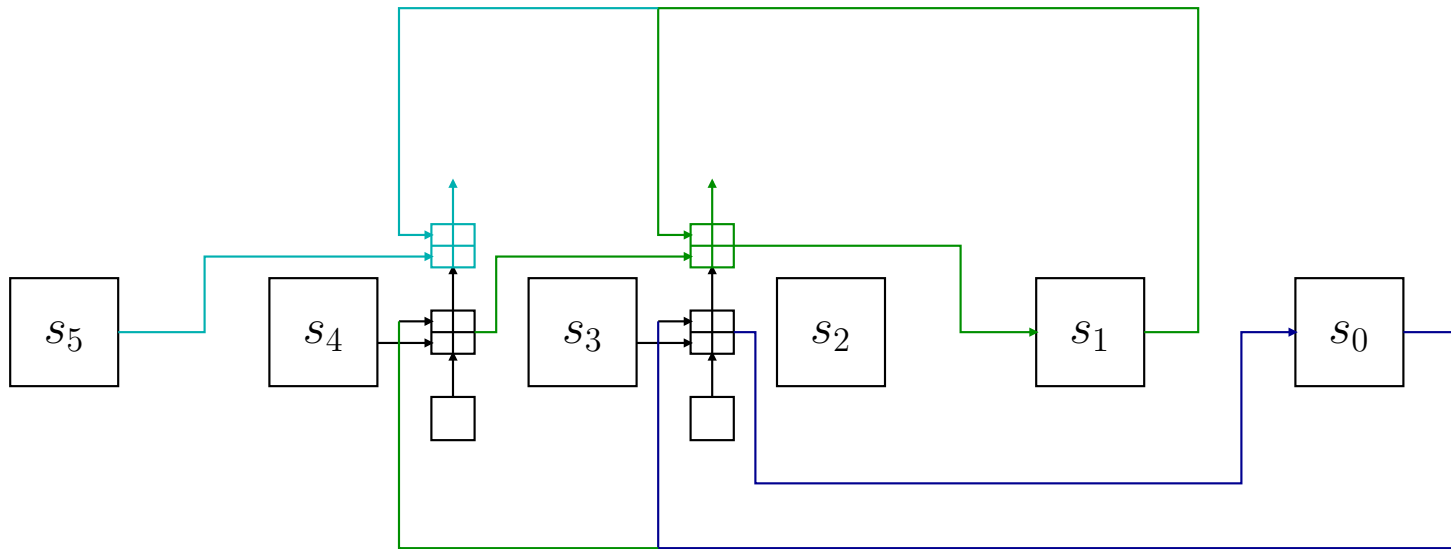
Feedback with Carry Shift Registers



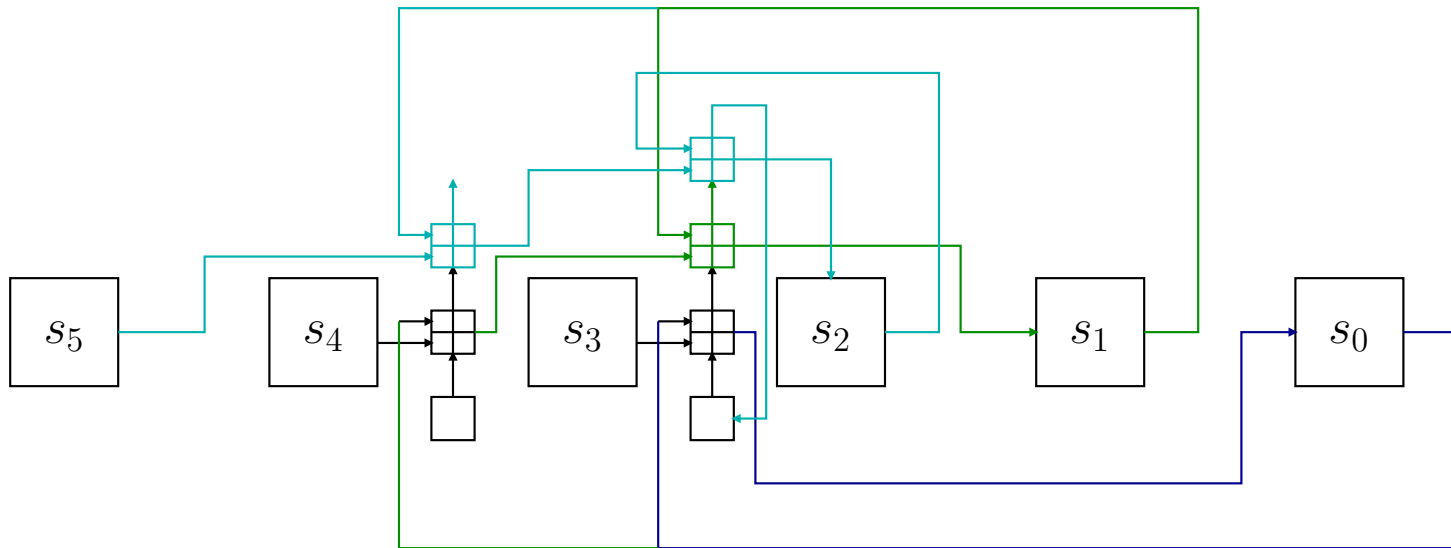
Feedback with Carry Shift Registers



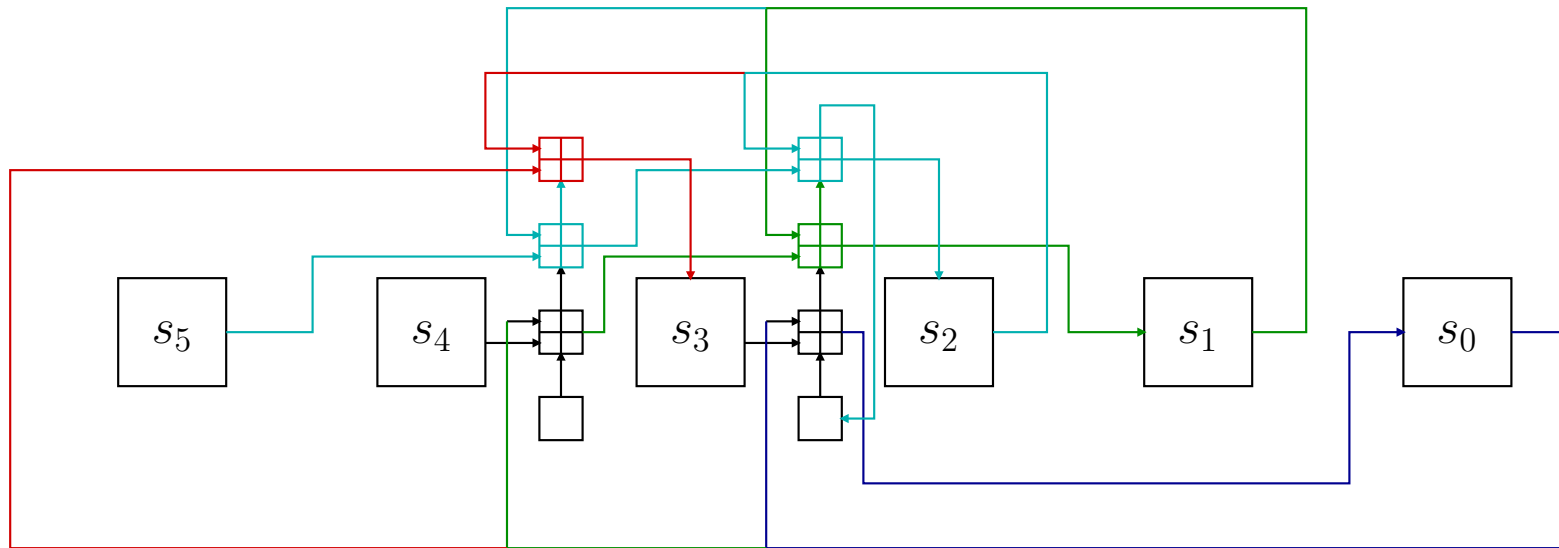
Feedback with Carry Shift Registers



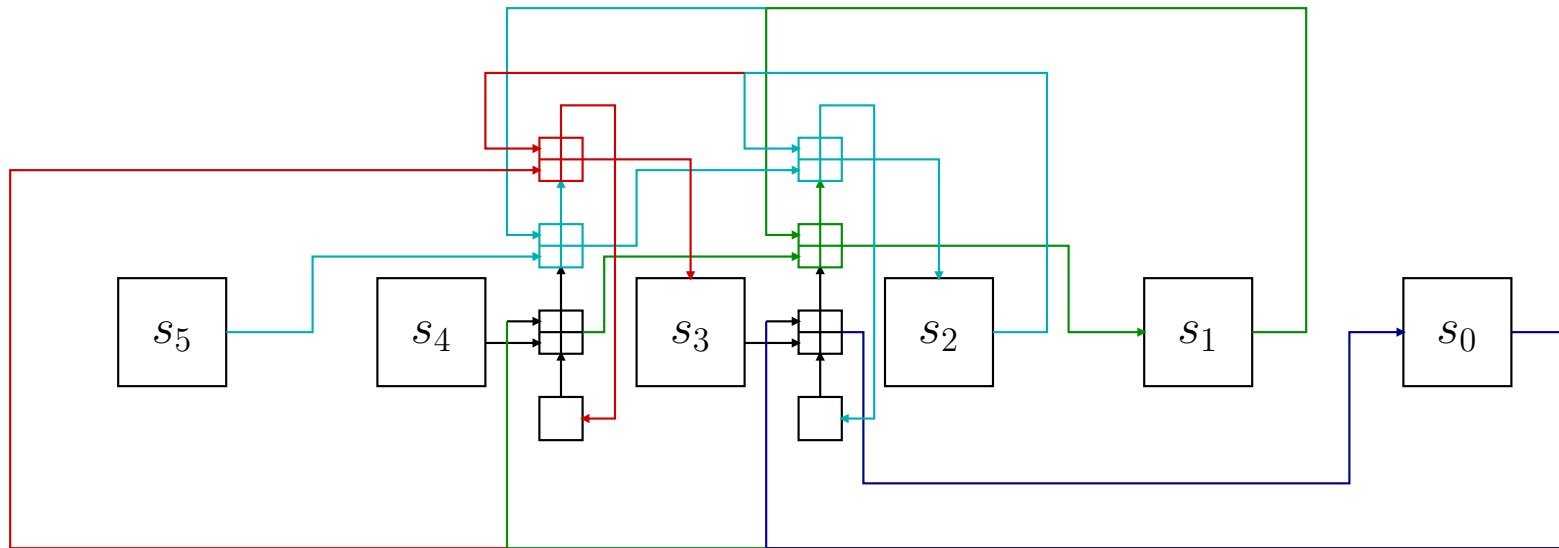
Feedback with Carry Shift Registers



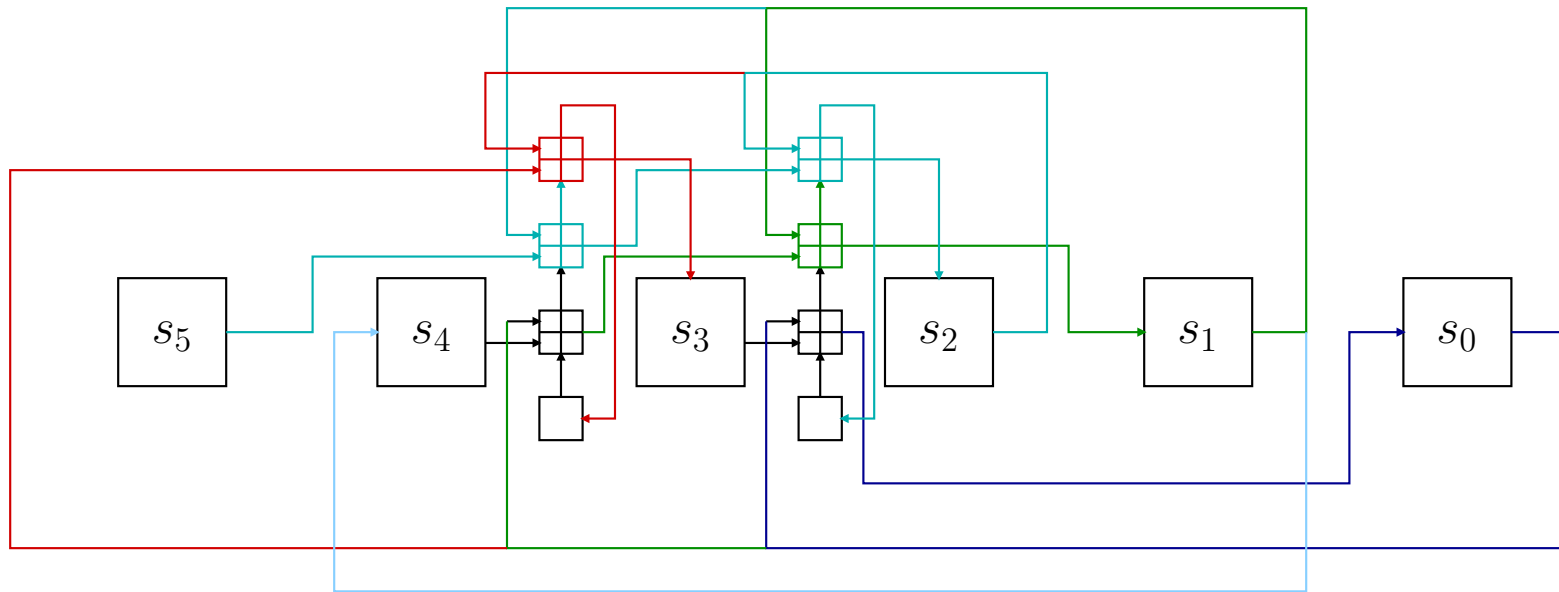
Feedback with Carry Shift Registers



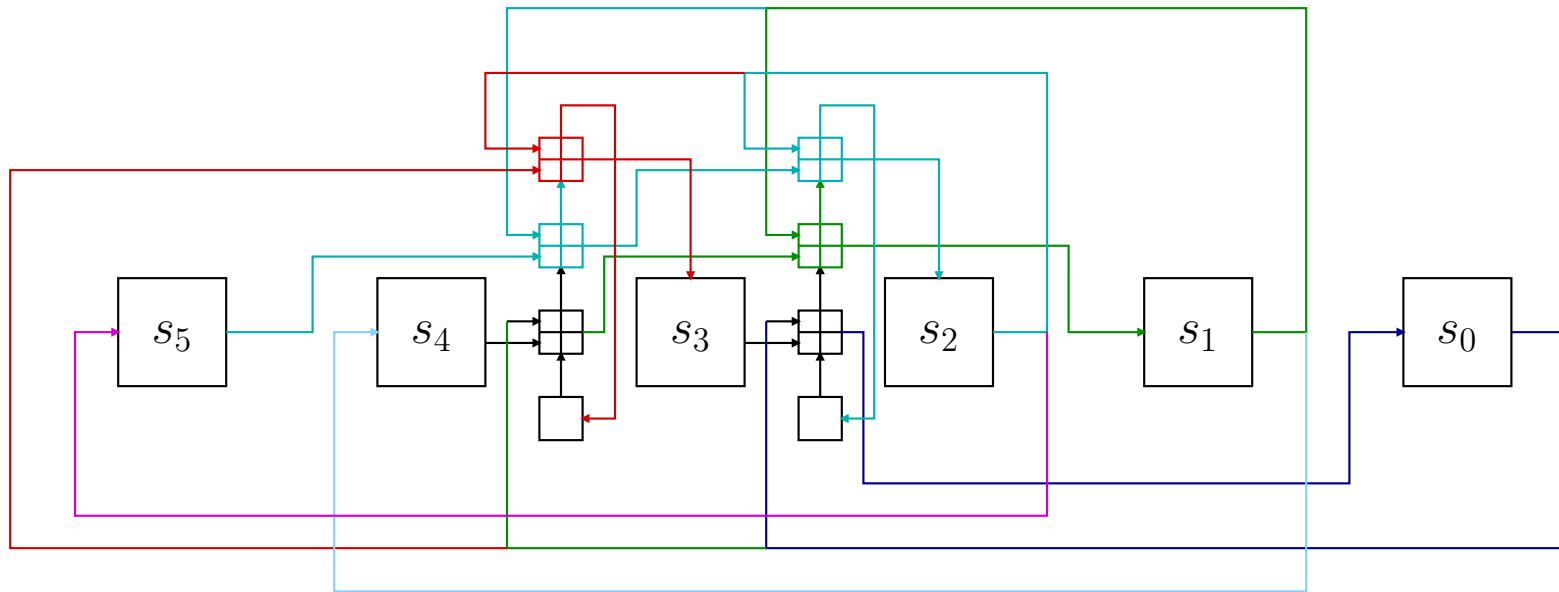
Feedback with Carry Shift Registers



Feedback with Carry Shift Registers



Feedback with Carry Shift Registers



Perspectives

- ▶ Online code generator:

<http://www-rocq.inria.fr/codes/LFSR/>

- ▶ Other fields: \mathbf{F}_3
- ▶ SIMD Instructions Set