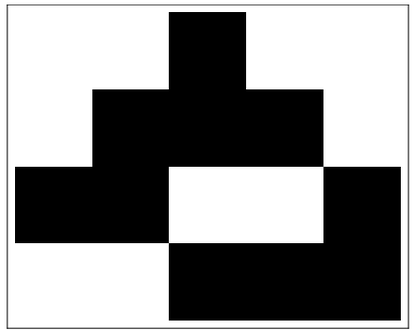
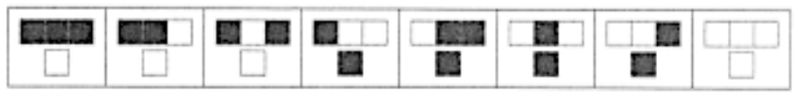
CA-based Random Number Generator

Bang-Ning Hsu
Darrell Gaspar
Yan-You Lin

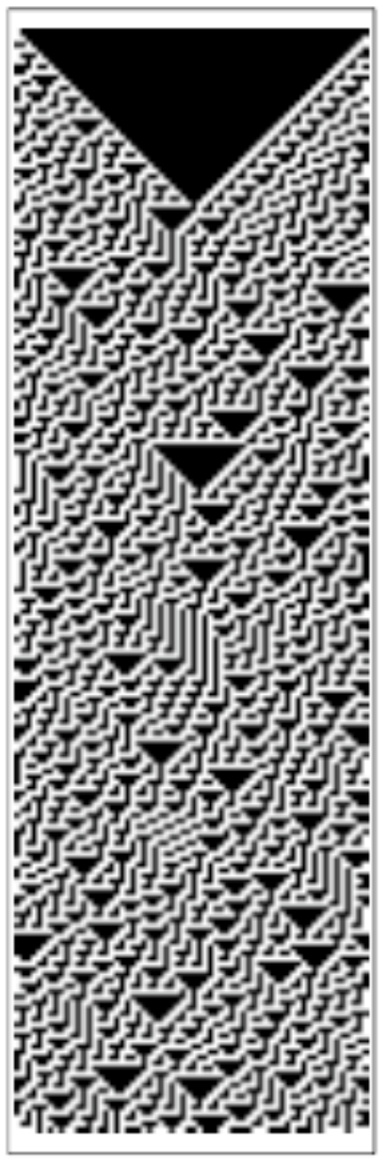
ECE261 Professor Morizio





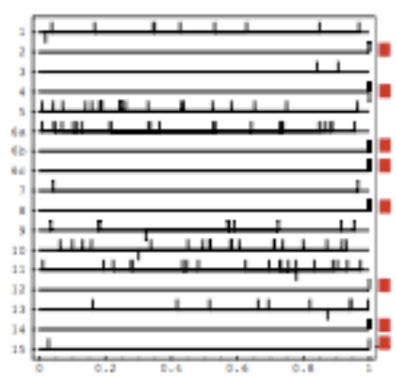
XOR[A, OR[B, C]]

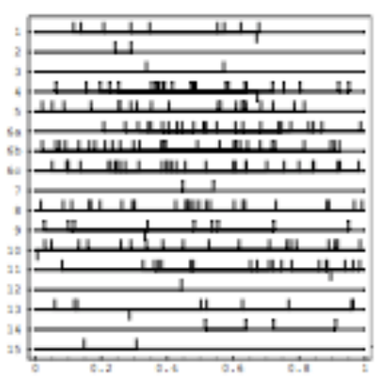
CA30
{-1, 0, 1}
1-d



CA38490
{-3, 0, 4, 9}
1-d

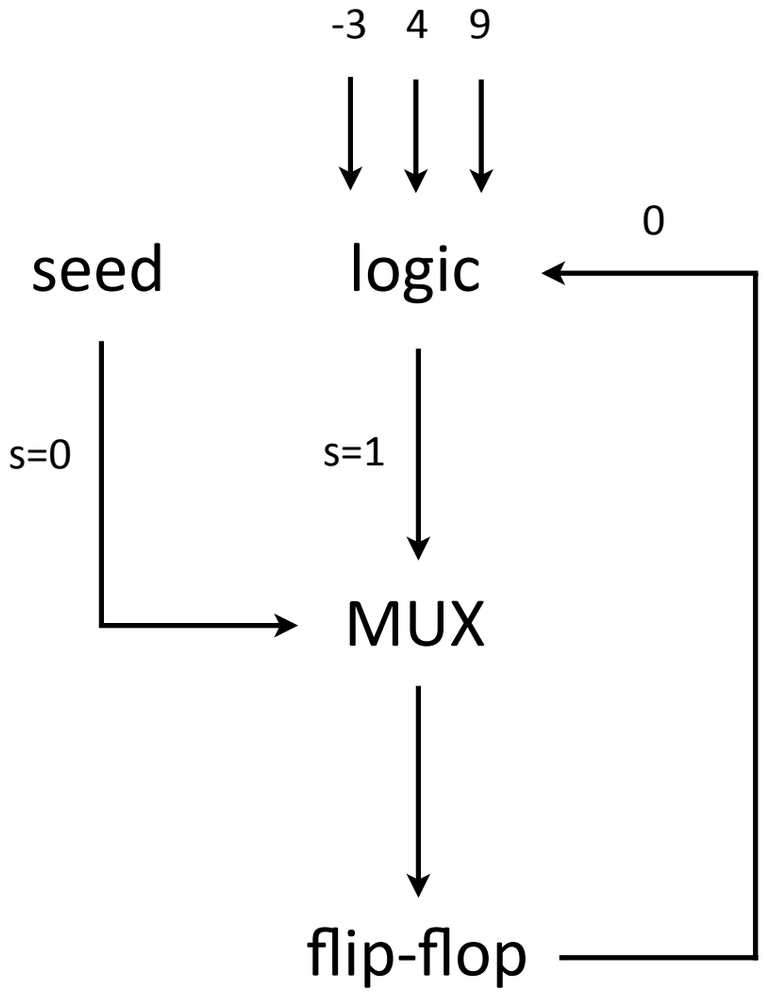
$\overline{AC}\,[B \text{ XOR } D] \quad A\overline{C}\,[B \text{ XOR } D]$

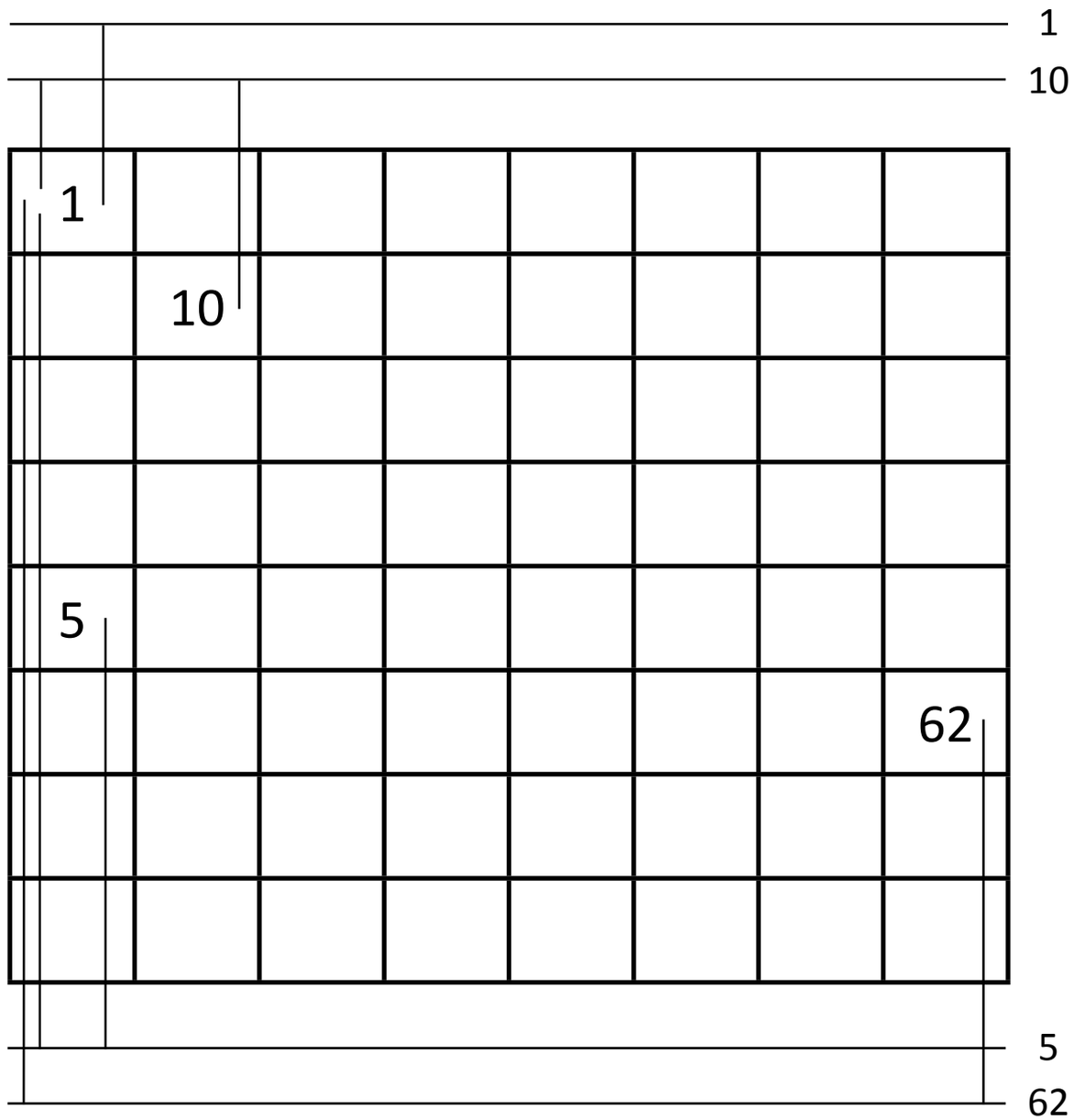


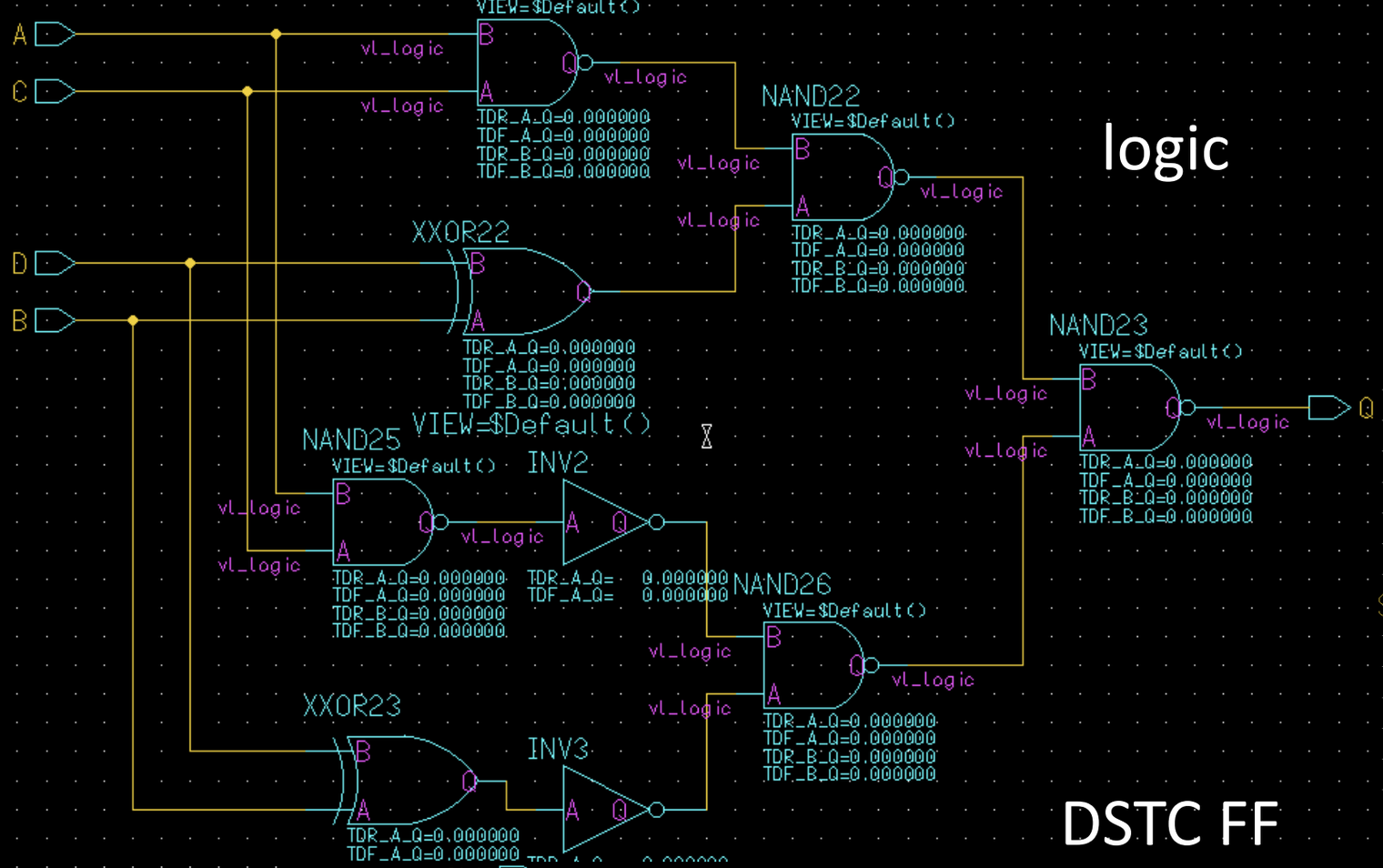


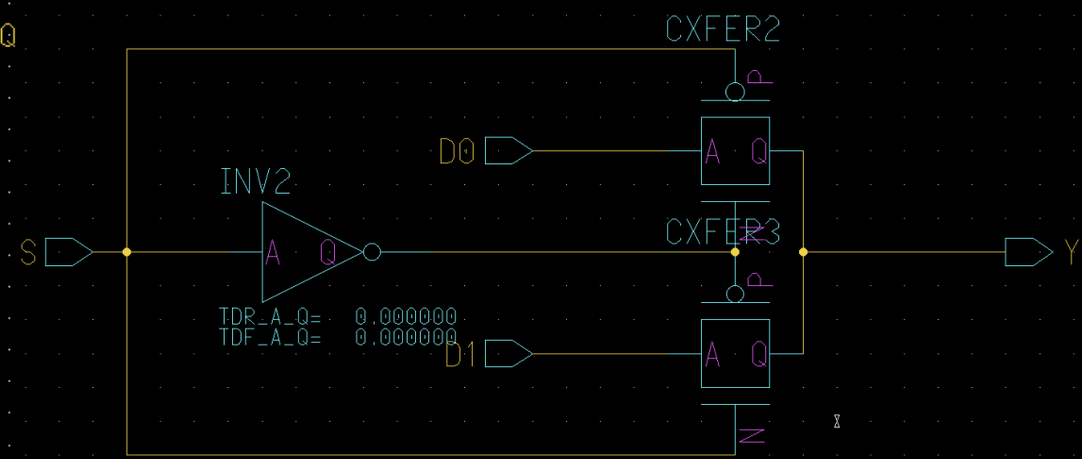
A New Kind of Science
S. Wolfram, 2002

FPGA implementation of neighborhood-of-four cellular automata random number generators
Shackleford *et al.*, 2002 ACM Symposium on FPGA, 106-112

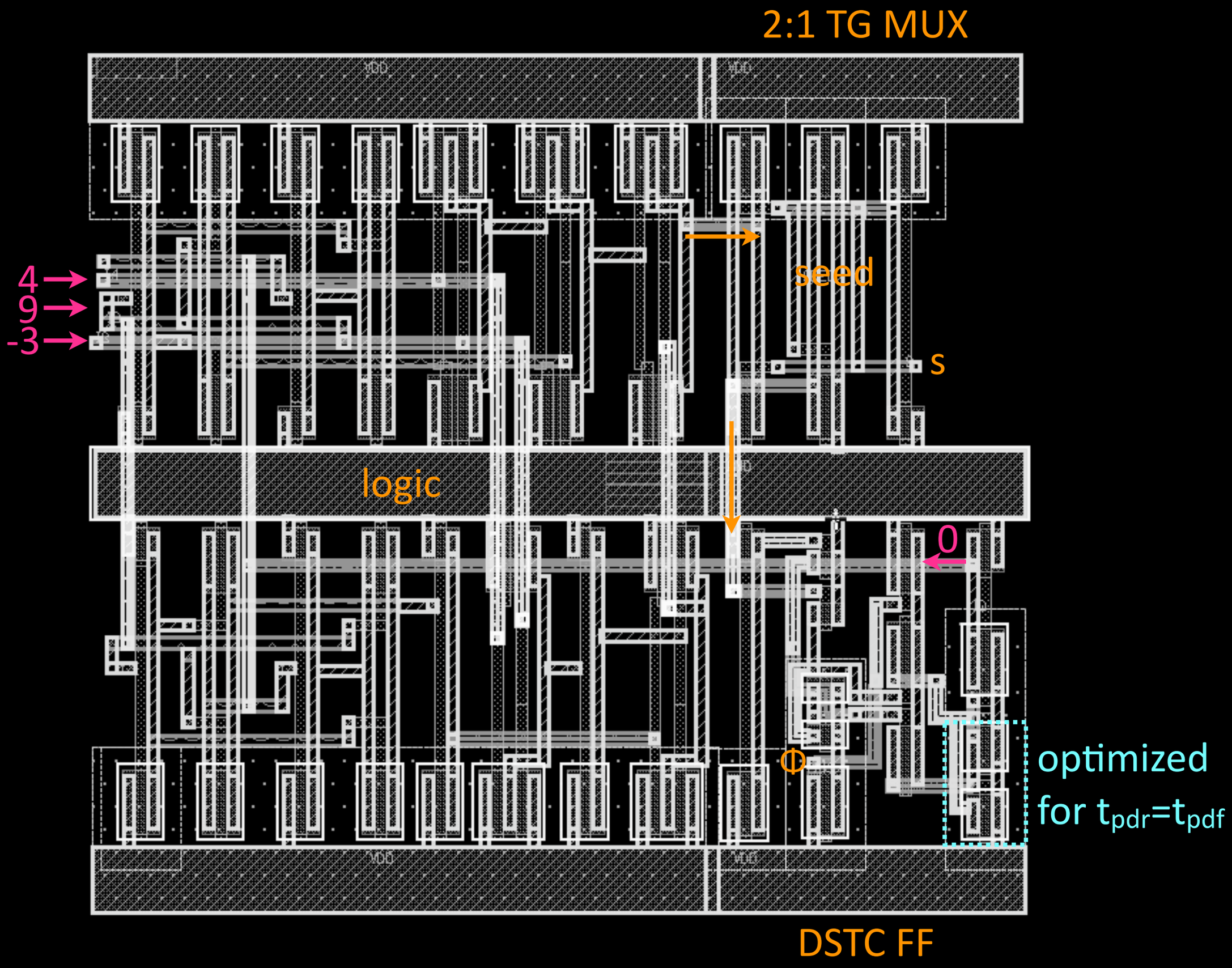

-3 4 9
seed
logic
0
s=0
s=1
MUX
flip-flop


1
10
1
10
5
62
5
62



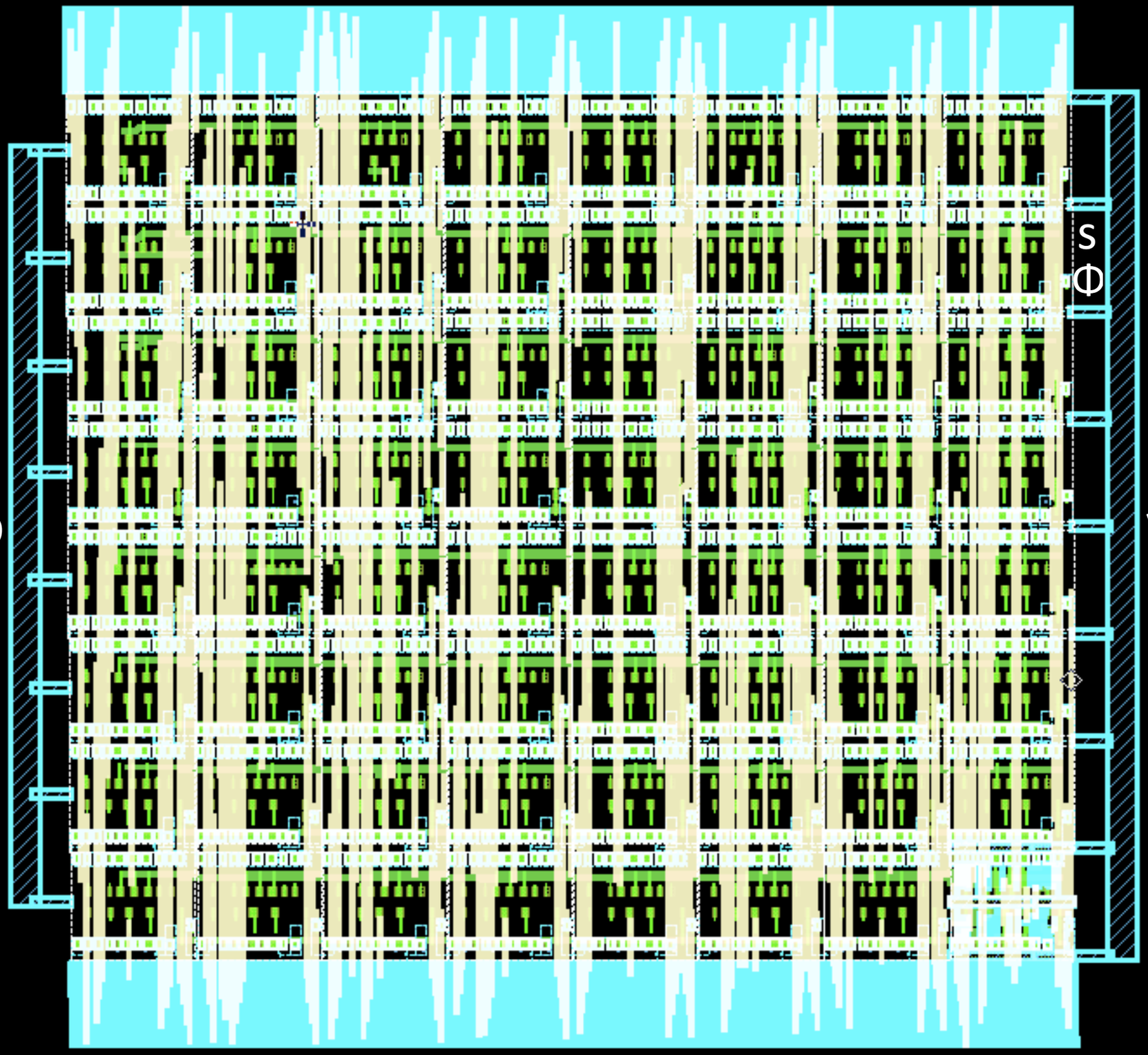


New TSPC Latches and Flipflops Minimizing Delay and Power
Yuen and Svensson, 1996 Symposium on VLSI Circuits Digest of Technical Papers


2:1 TG MUX
4
9
-3
seed
s
logic
0
Φ
optimized
for $t_{pdr}=t_{pdf}$
DSTC FF

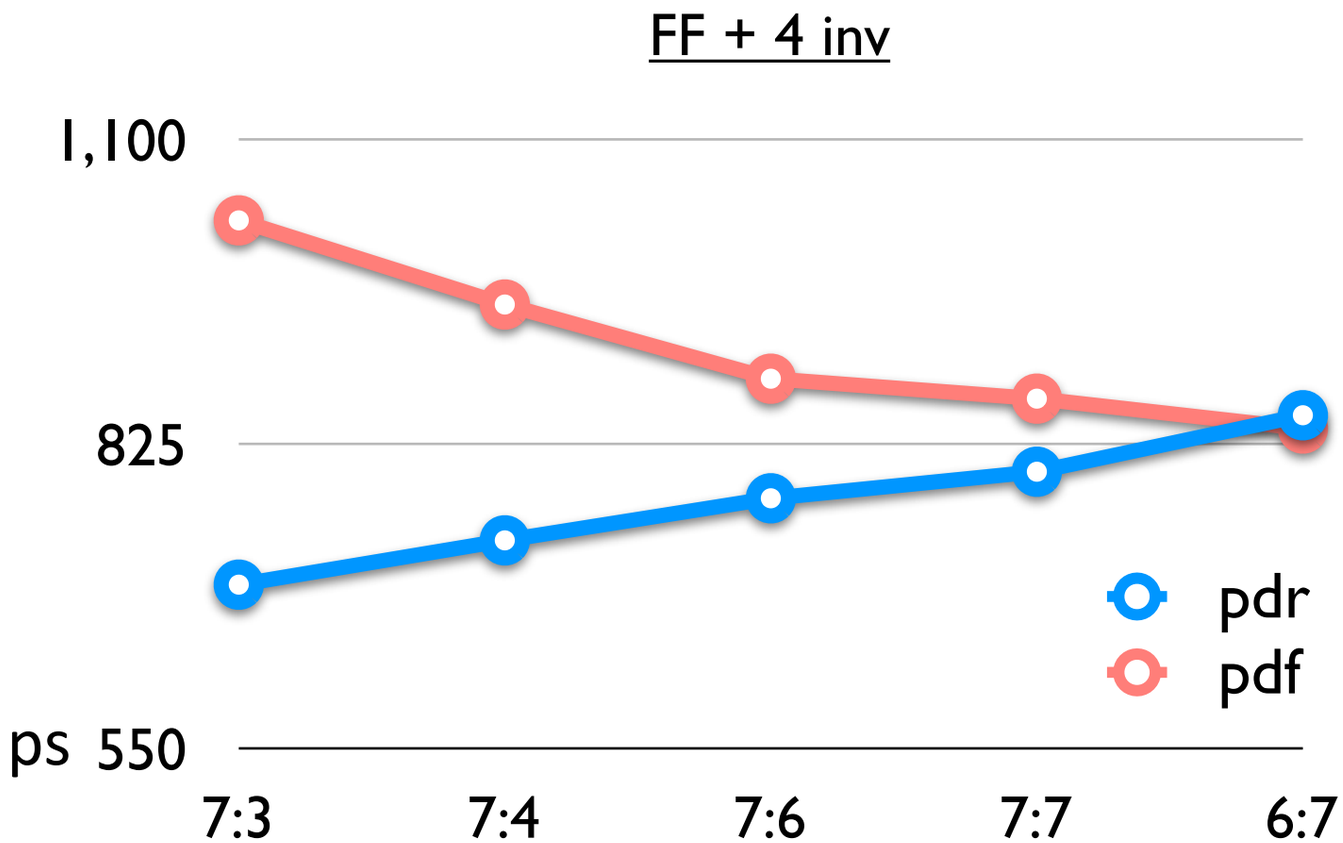
768.56 µm

outputs of the upper half of cells

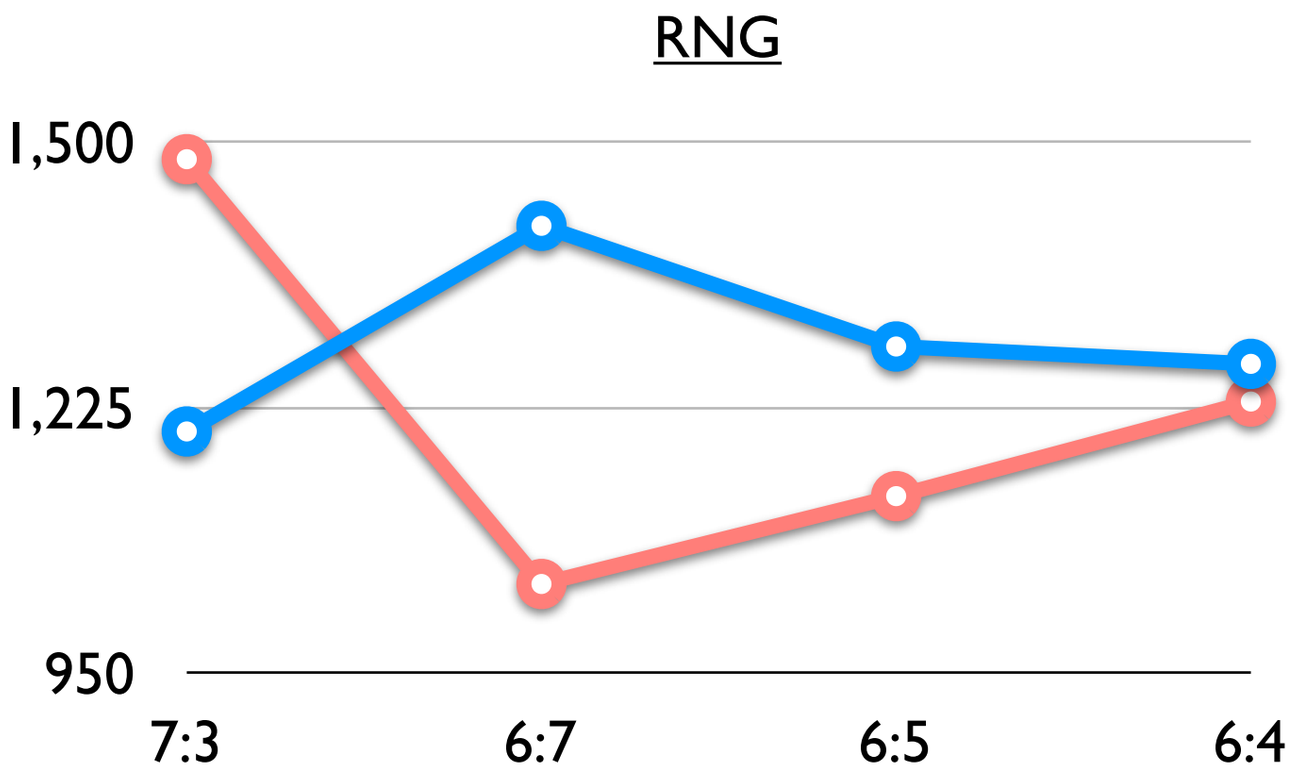


707.2 µm

outputs of the lower half of cells



optimization



loading seed into FF
(#64=1, else=0)

1st cycle

t_{pdr}, t_{pdf} =1.2 ns

Φ 10 ns

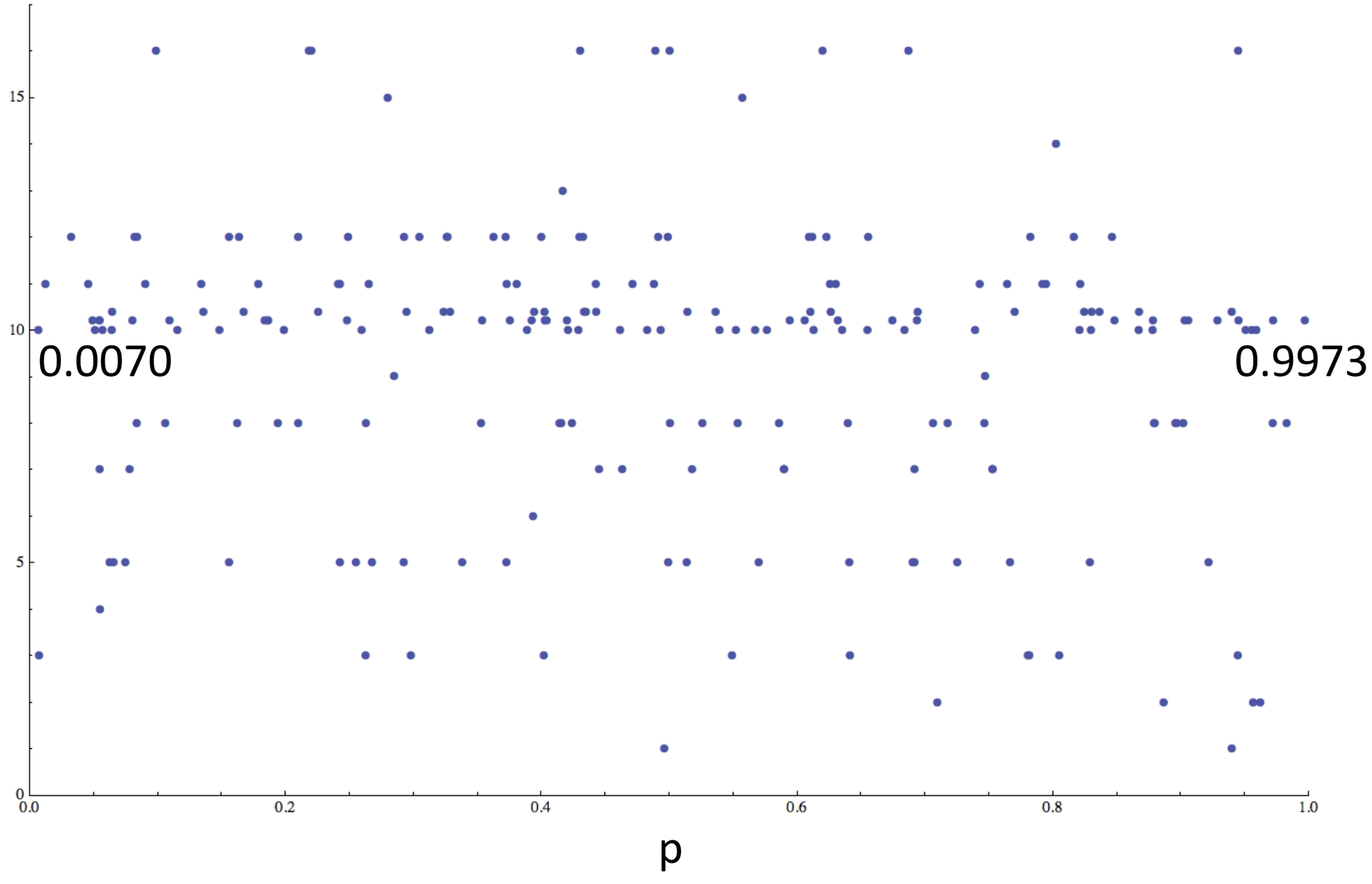
first 10 cycles
ELDO = VHDL
→ Java parser
→ 2.5 million numbers
→ DIEHARD

Φ 22 ns

DIEHARD

pass: 0.0000001 ~ 0.9999999

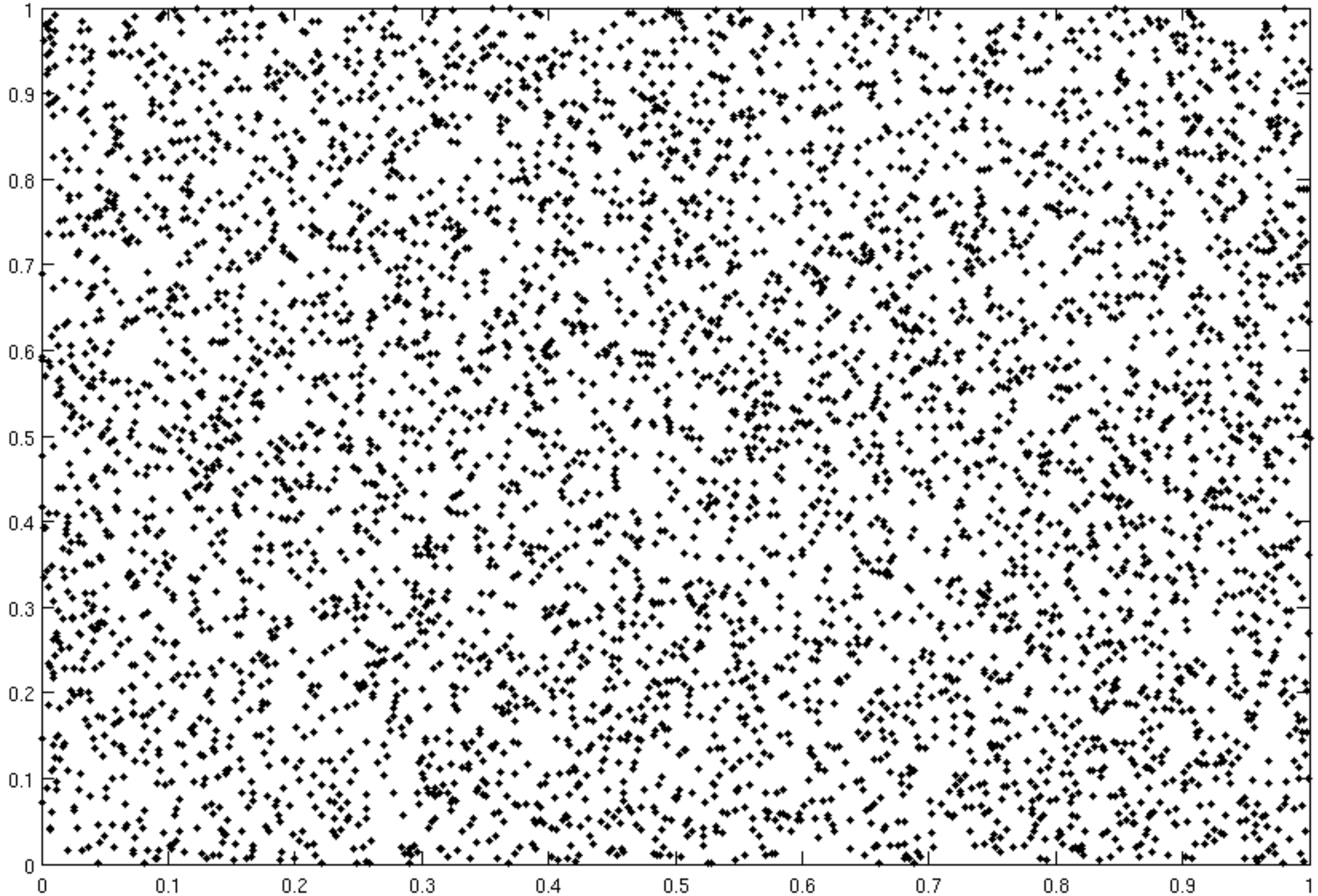
type of test



input: V_{DD} GND Φ S
output: 32-bit/10 ns cycle

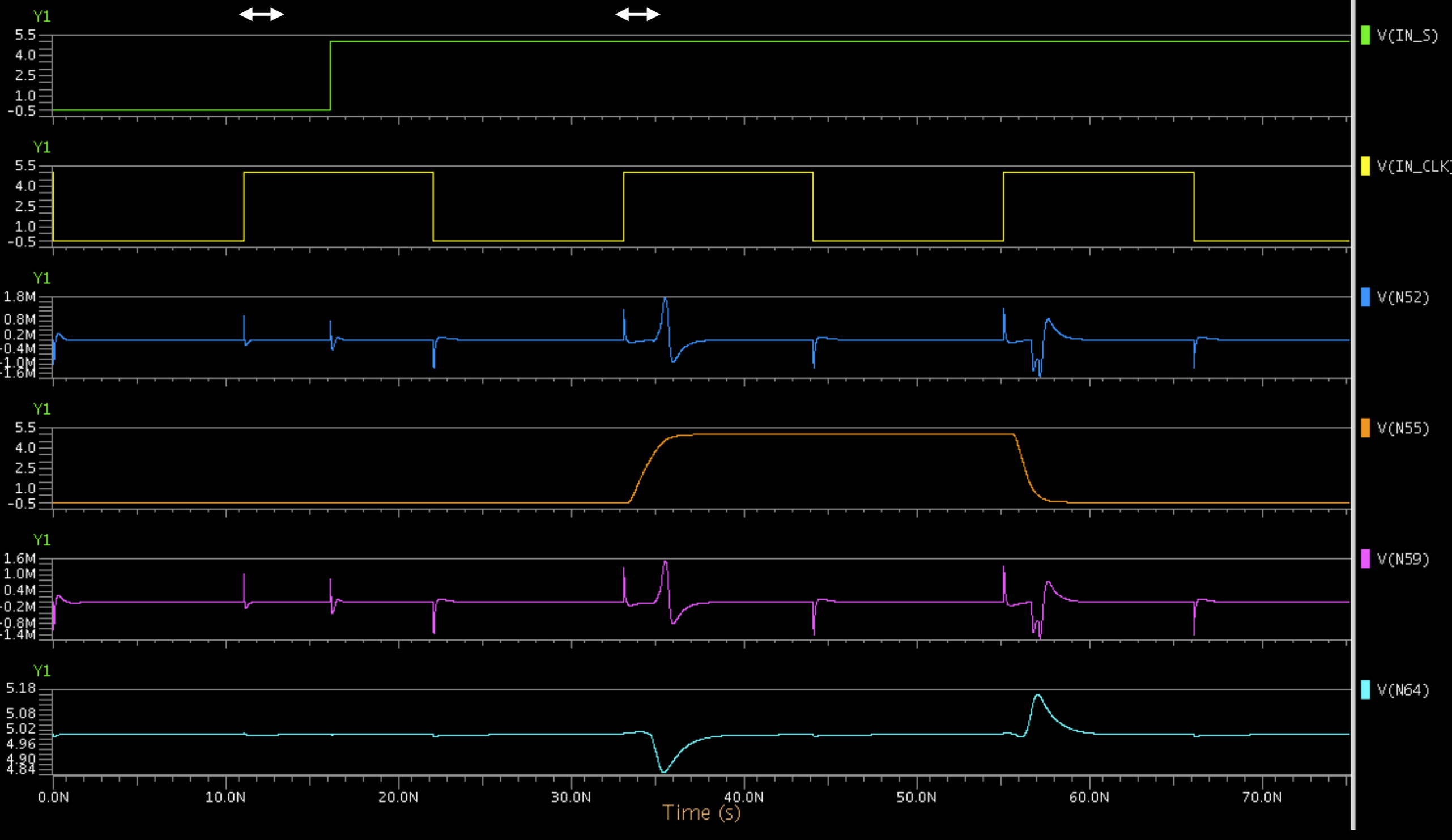
	technology	clock (MHz)	transistor	area (mm^2)	power
HP 2002	0.22μ FPGA 5-layer metal 2.5 V	219			
us	0.5μ 3-layer metal 5 V	100	3840 (logic 40+MUX 6+FF 14) x 64	0.54	86 nW
Hortensius 1989	3μ 1-layer metal	20		0.72	

Importance Sampling for Ising Computers Using One-Dimensional Cellular Automata
Hortensius *et al.* (1989) IEEE Transactions on Computers **38** 769


1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1

loading seed into FF
(#64=1, else=0)

1st cycle



Φ 22 ns