Institut des Nanotechnologies de Lyon UMR 5270

System architectures and new computing paradigms

FeFET opportunities for Secure and reconfigurable processor

Cédric Marchand

Agenda

- Introduction
  - Context
  - Objectives
  - Methodology

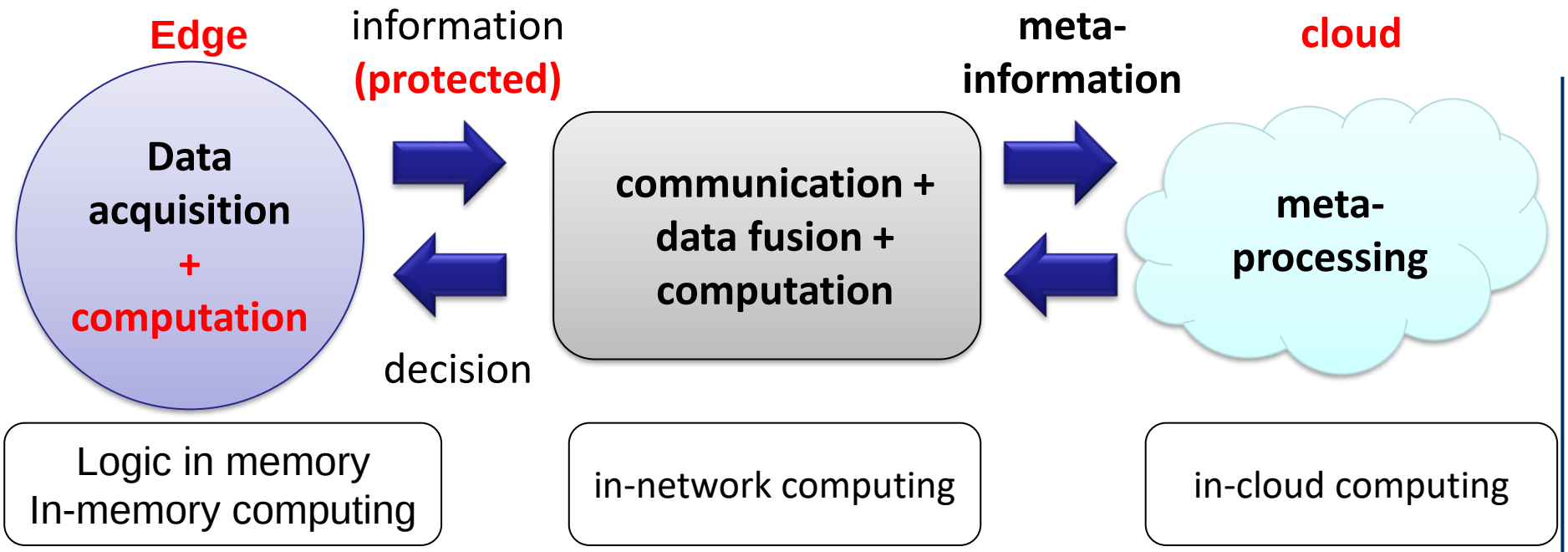
- FeFET: Fine grain Logic in Memory
  - Custom Logic Gate
  - Generic Logic Gate
  - TCAM/RAM

Agenda

- Introduction
  - Context
  - Objectives
  - Methodology

- FeFET : Fine grain Logic in Memory
  - Custom Logic Gate
  - Generic Logic Gate
  - TCAM/RAM

Context


Edge
information
(protected)
meta-
information
cloud
Data
acquisition
+
computation
communication +
data fusion +
computation
meta-
processing
decision
Logic in memory
In-memory computing
in-network computing
in-cloud computing

Context

Edge

Data acquisition + computation

information (protected)

decision

communication + data fusion + computation

meta-information

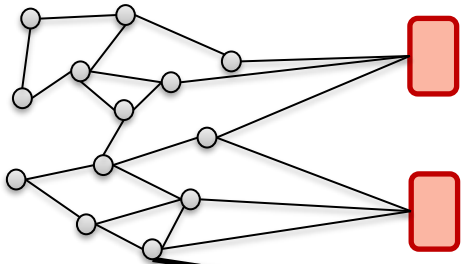
cloud

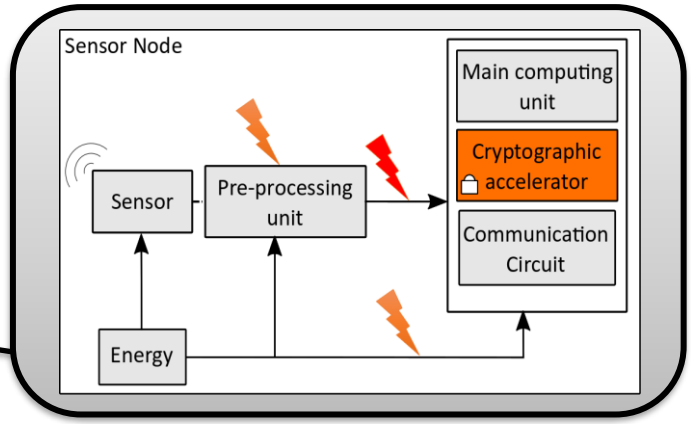
meta-processing

Logic in memory
In-memory computing

in-network computing

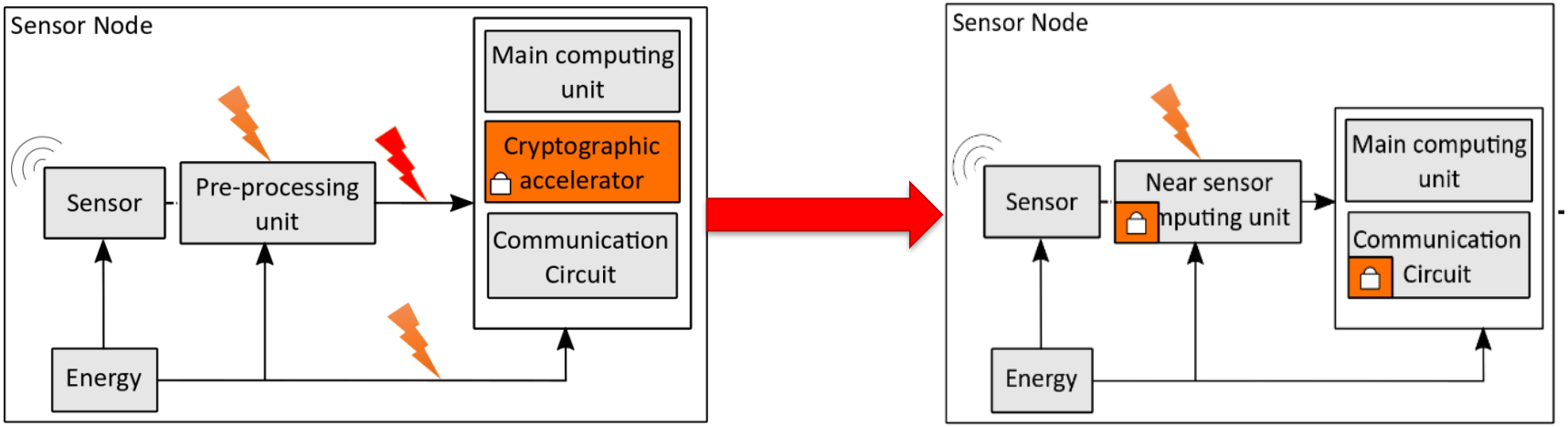
in-cloud computing



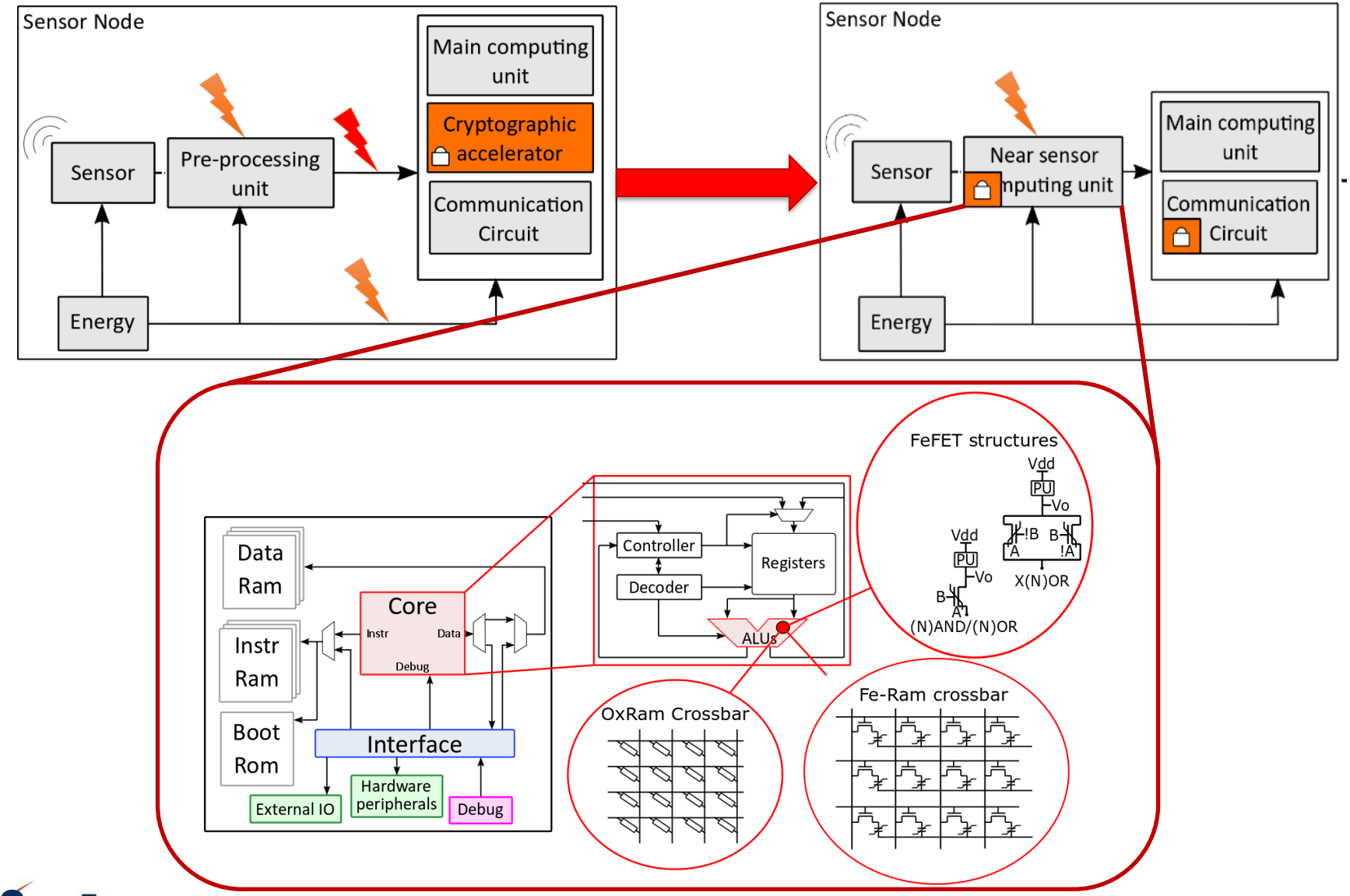


Need for a Secure and Highly energy efficient Computing platform

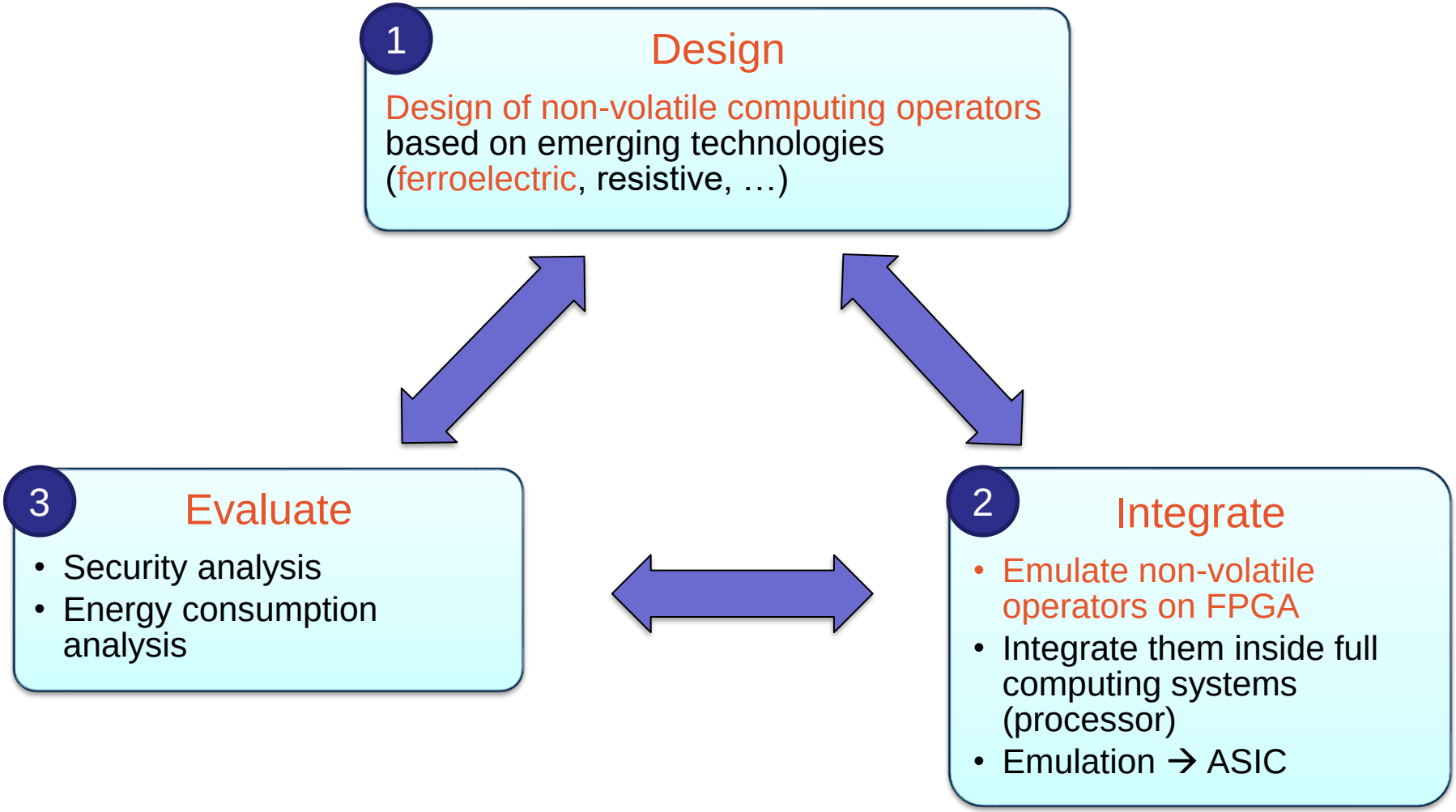
Objectives


Sensor Node
Sensor
Pre-processing unit
Main computing unit
Cryptographic accelerator
Communication Circuit
Energy
Sensor Node
Sensor
Near sensor mputing unit
Main computing unit
Communication Circuit
Energy

Objectives


Sensor Node
Sensor
Pre-processing unit
Main computing unit
Cryptographic accelerator
Communication Circuit
Energy
Sensor Node
Sensor
Near sensor mputing unit
Main computing unit
Communication Circuit
Energy
Data Ram
Instr Ram
Boot Rom
Core
Instr
Data
Debug
Interface
External IO
Hardware peripherals
Debug
Controller
Registers
Decoder
ALUs
FeFET structures
Vdd
PU
Vo
!B
B
A
!A
X(N)OR
(N)AND/(N)OR
OxRam Crossbar
Fe-Ram crossbar

Methodology



Agenda

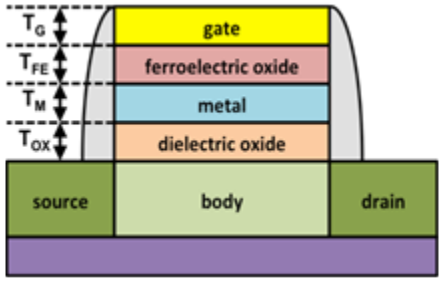
- Introduction
  - Context
  - Objectives
  - Methodology

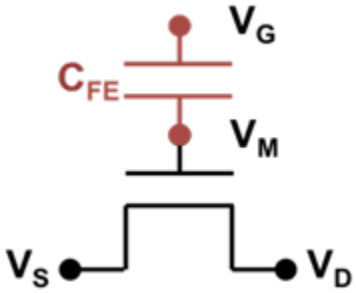
- FeFET: Fine grain Logic in Memory
  - Custom Logic Gate
  - Generic Logic Gate
  - TCAM/RAM

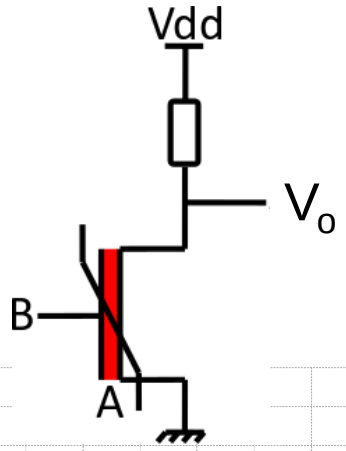
FeFET : single transistor characteristics

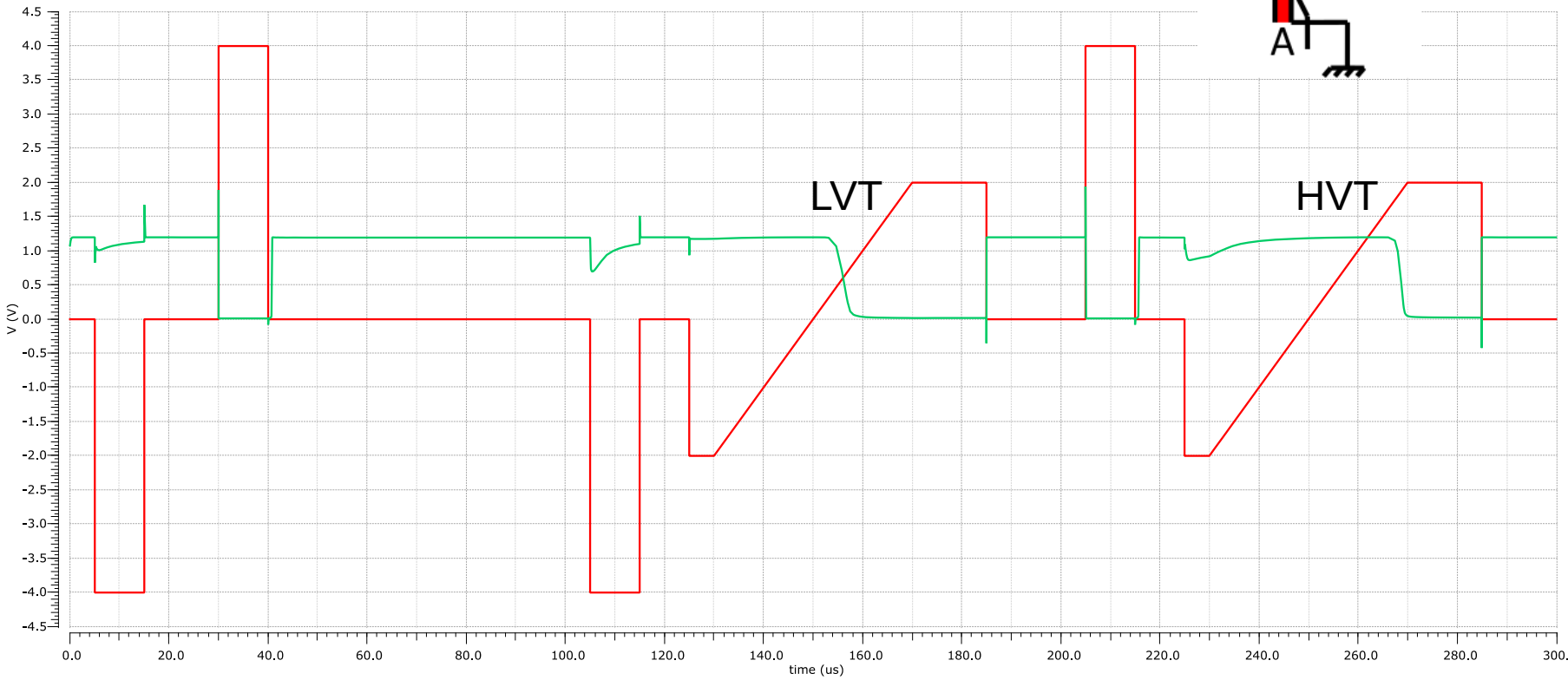
V_o

V_B





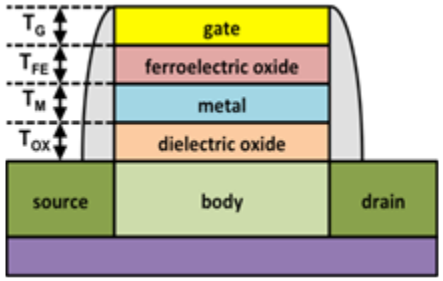


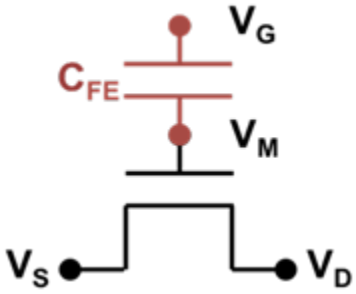


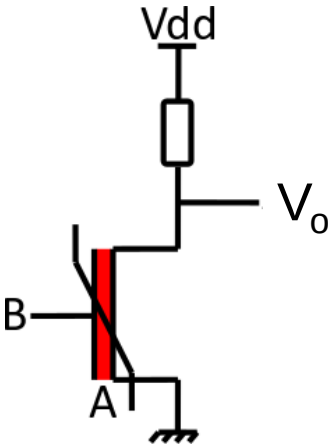
FeFET : single transistor characteristics

V_o

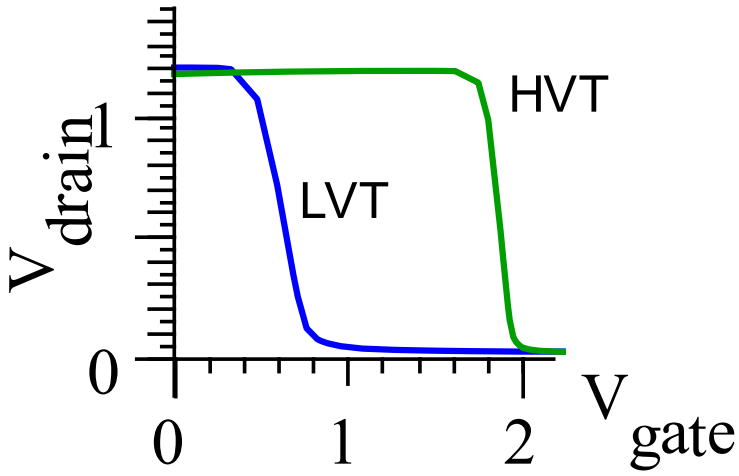
V_B







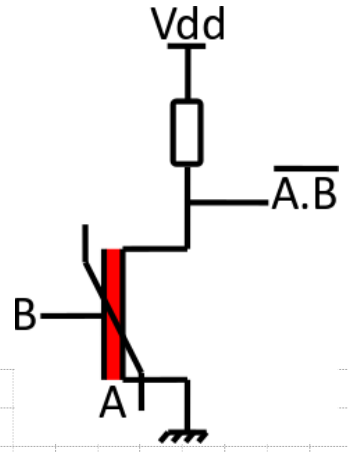
Voltage characteristic



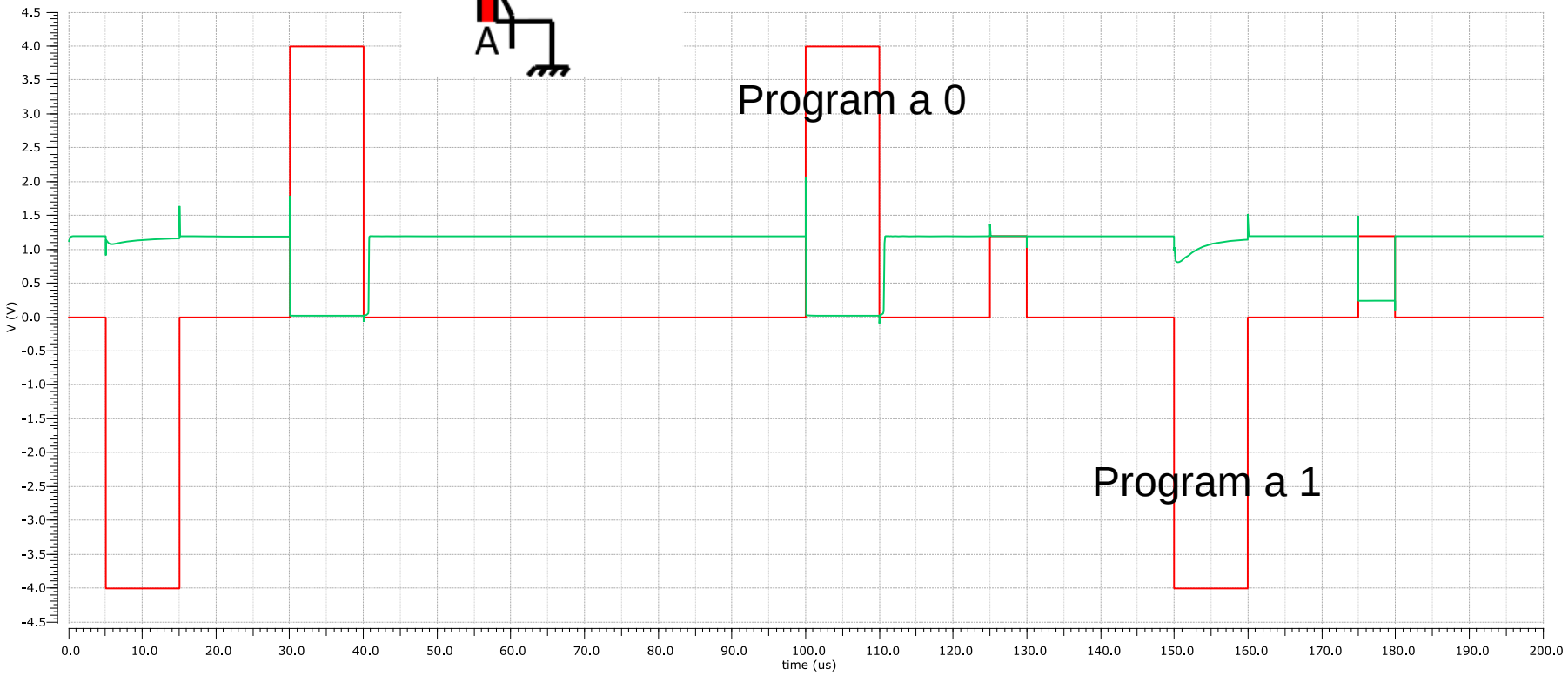
Custom Logic Gate

V_o

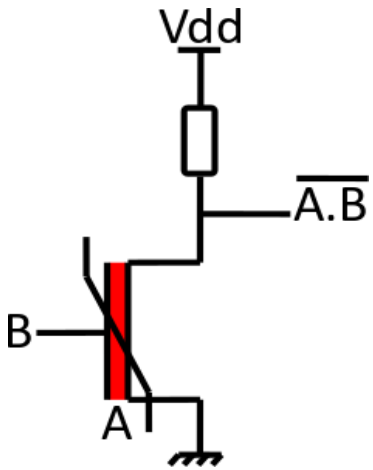
V_B

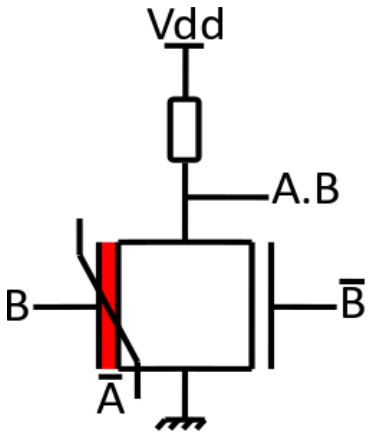


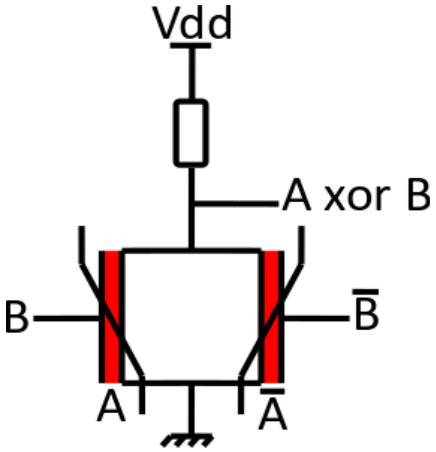
Logical Operation

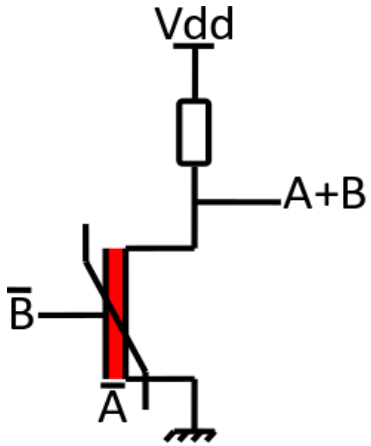


Custom Logic Gate

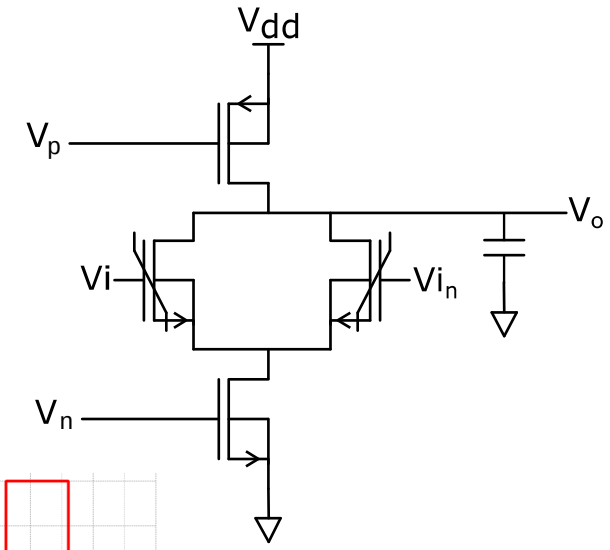


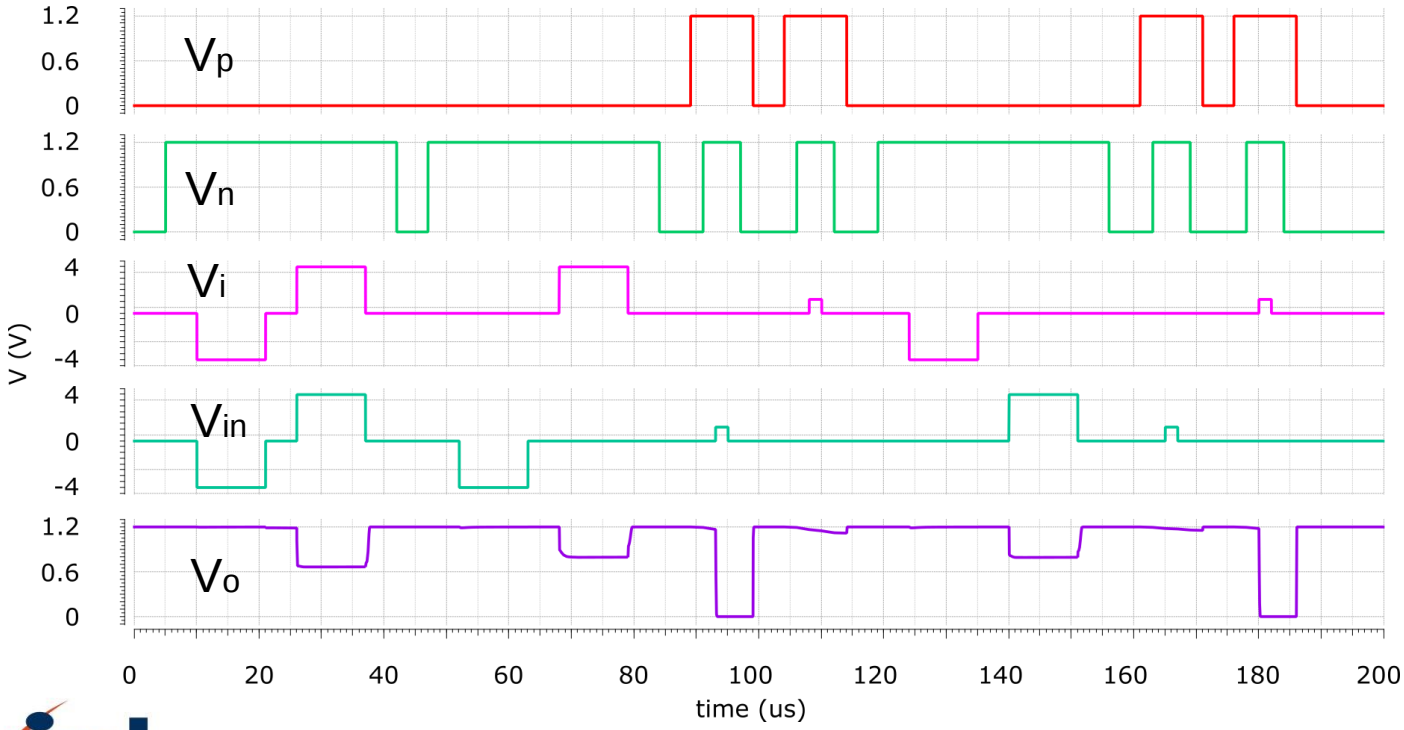




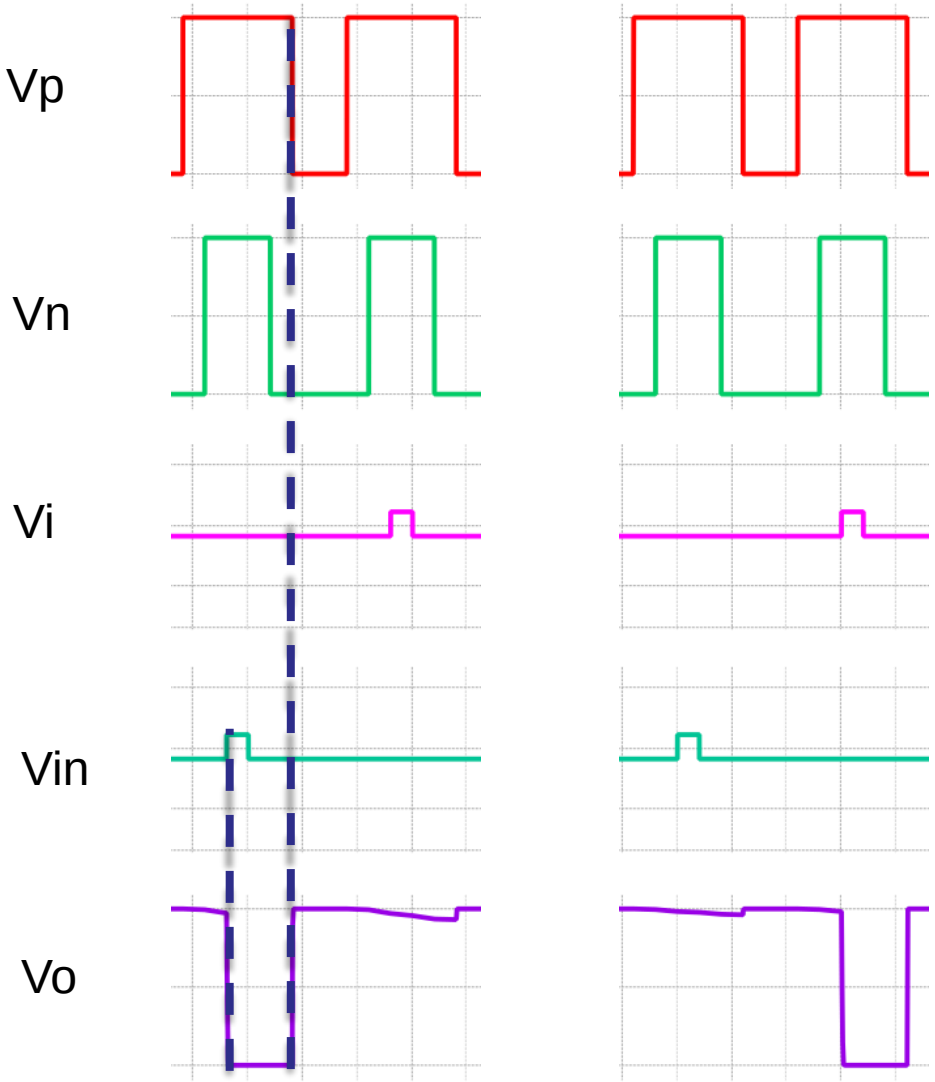


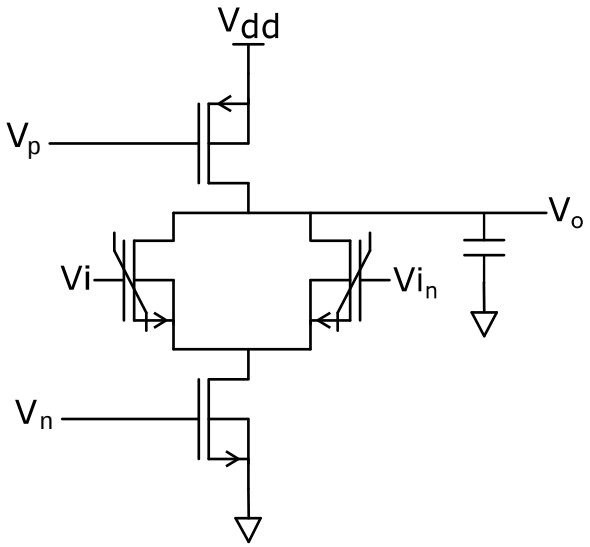
Custom Logic Gate (Dynamic design)





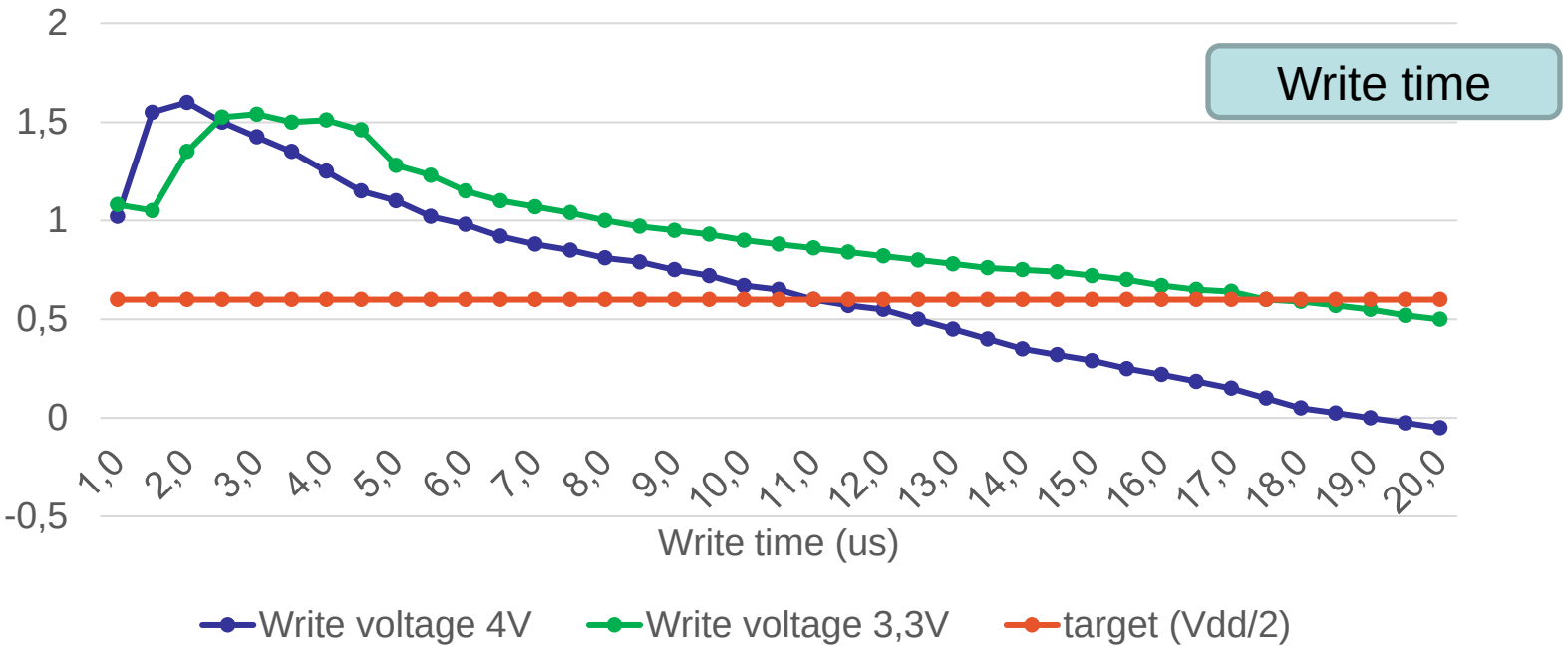
Custom Logic Gate (Dynamic design)



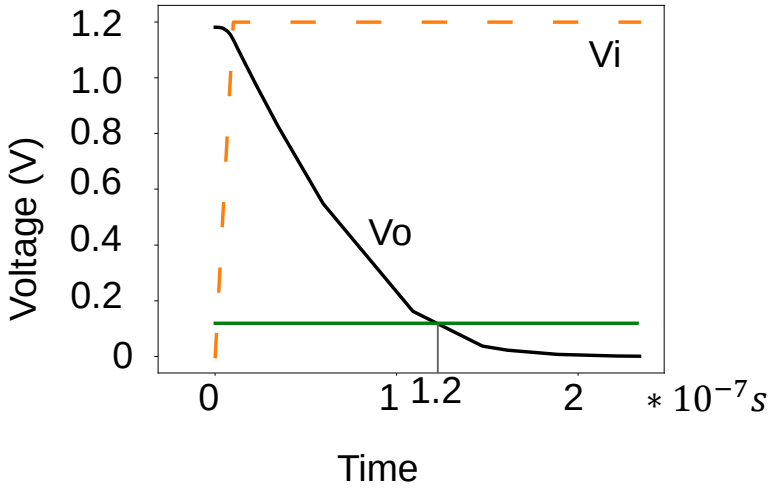


Custom Logic Gate (Characterization)

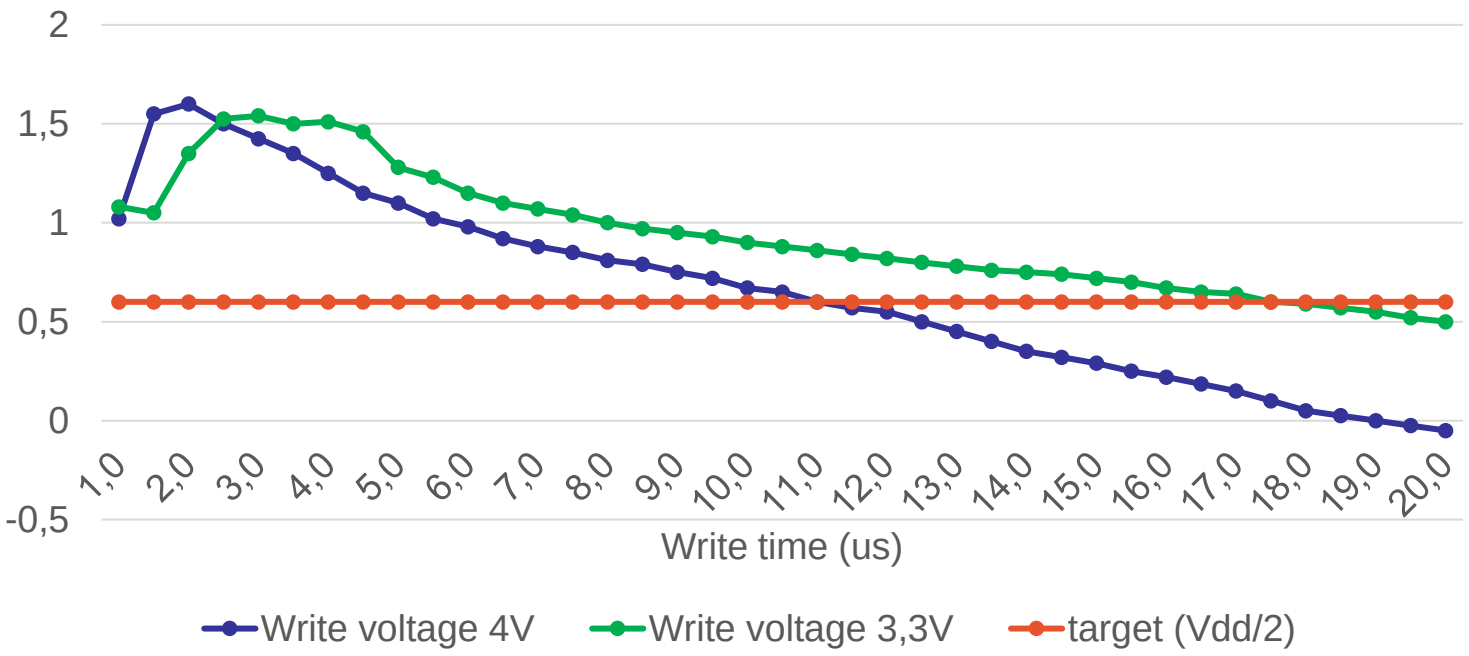
Write time



Read time



Custom Logic Gate (Characterization)



	Read time (s)		Max Frequency (MHz)	
Write pulses	3,3V	4V	3,3V	4V
Nand	$1{,}07e^{-7}$	$1{,}21e^{-7}$	9,35	8,26
And	$1{,}19e^{-7}$	$1{,}38e^{-7}$	8,40	7,24
Xor	$1{,}26e^{-7}$	$1{,}35e^{-7}$	7,94	7,41

Custom Logic Gate (Characterization)

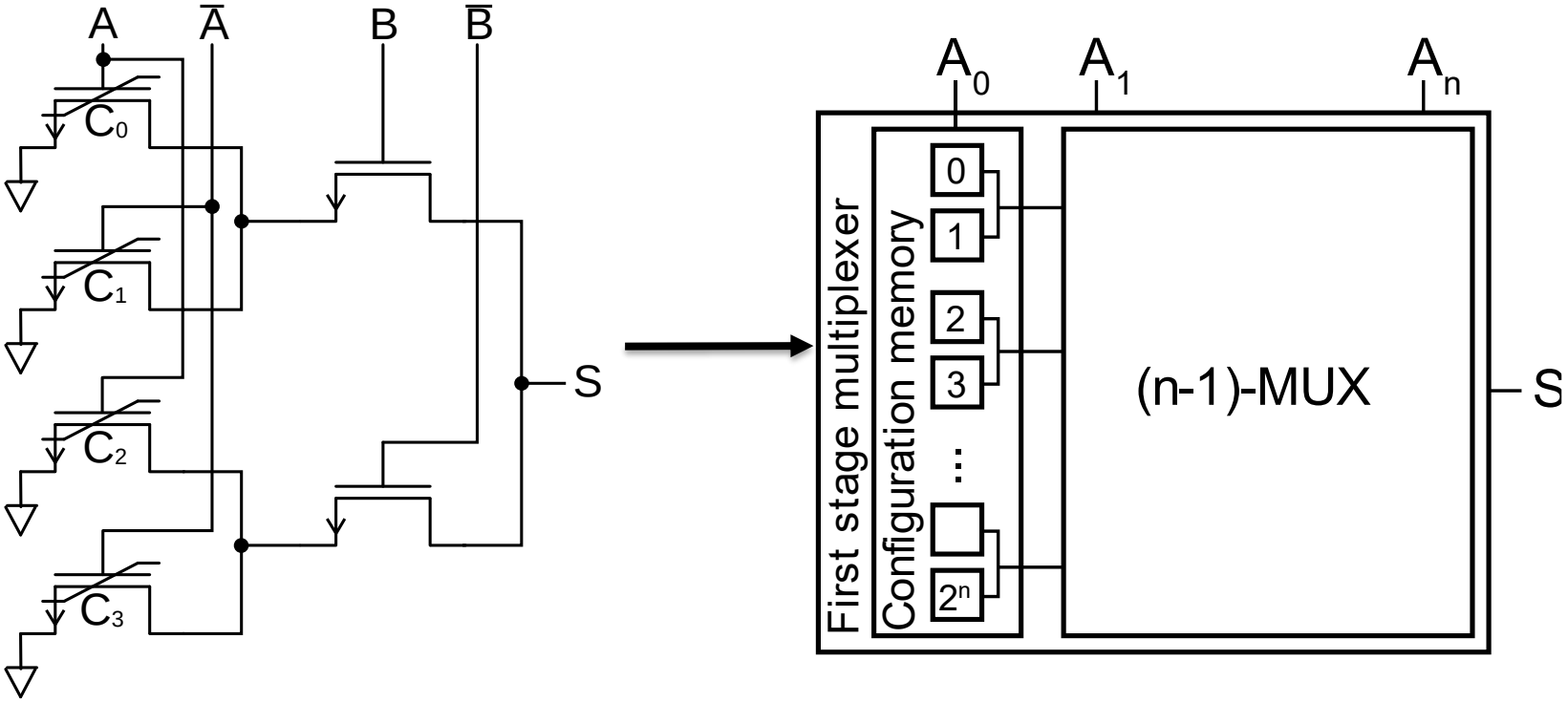
	Static (nJ)		Write (pJ)		Read (fJ/bit)			
Value	0	1	0	1	**0**0	**0**1	**1**0	**1**1
Nand	19,2	0,24	599	5,7	X	0,34	X	3,8
And	9,2	0,02	605	6,1	0,29	0,36	0,42	3,0
Xor	10,7	10,7	574	576	3,3	0,34	0,31	3,2

4V write pulses

	Static (nJ)		Write (pJ)		Read (fJ/bit)			
Value	0	1	0	1	**0**0	**0**1	**1**0	**1**1
Nand	11,3	0,08	973	4,4	X	0,37	X	3,3
And	6,5	0,03	985	4,7	0,25	0,32	0,25	4,0
Xor	8,4	10,3	928	933	2,5	0,58	0,78	3,3

3,3V write pulses

Generic Logic Gate (FeLUT)

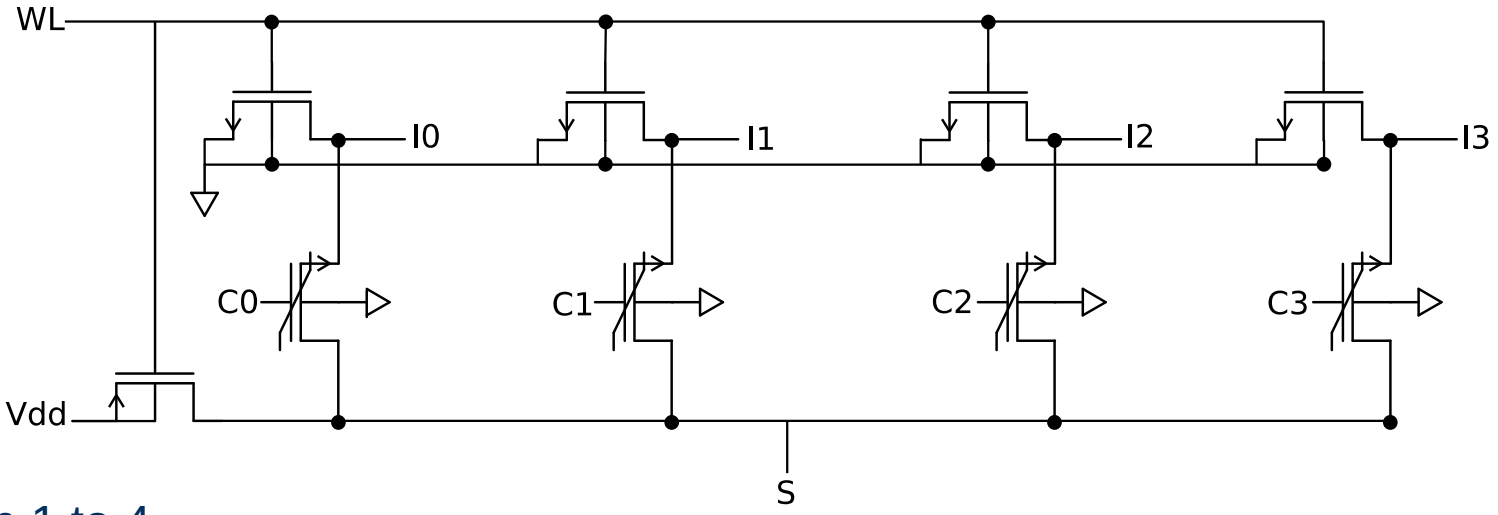


$2 - bit$ $\qquad$ $n - bit$

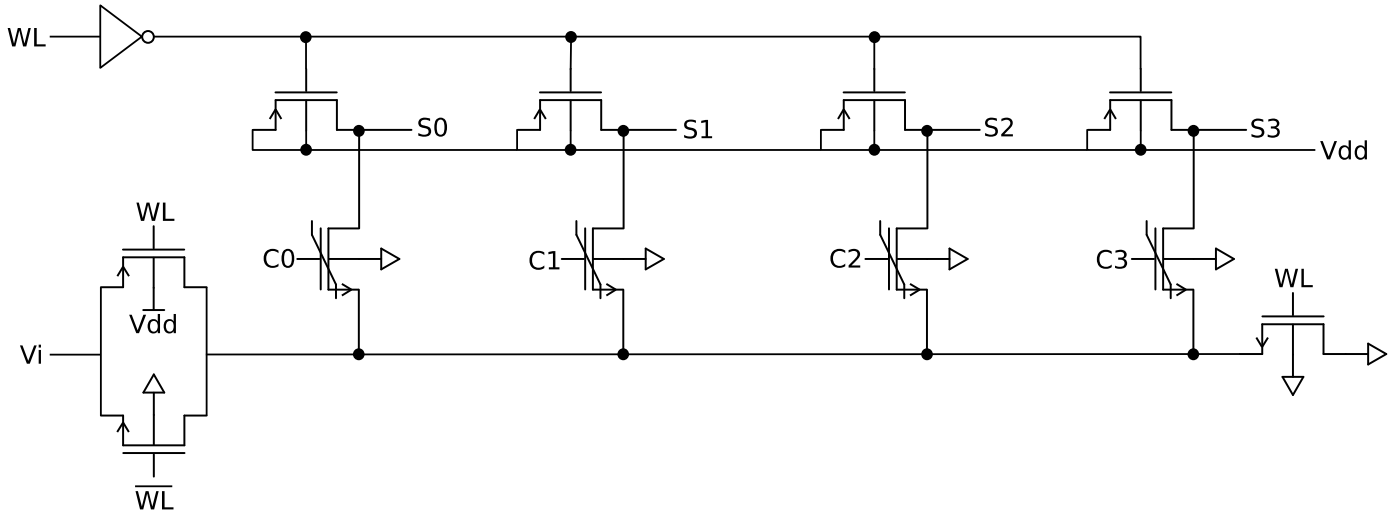
$$\bar{S} = B.(C_0.A + C_1.\bar{A}) + \bar{B}.(C_2.A + C_3.\bar{A})$$

Generic Logic Gate (Routing structures)

Mux 4 to 1

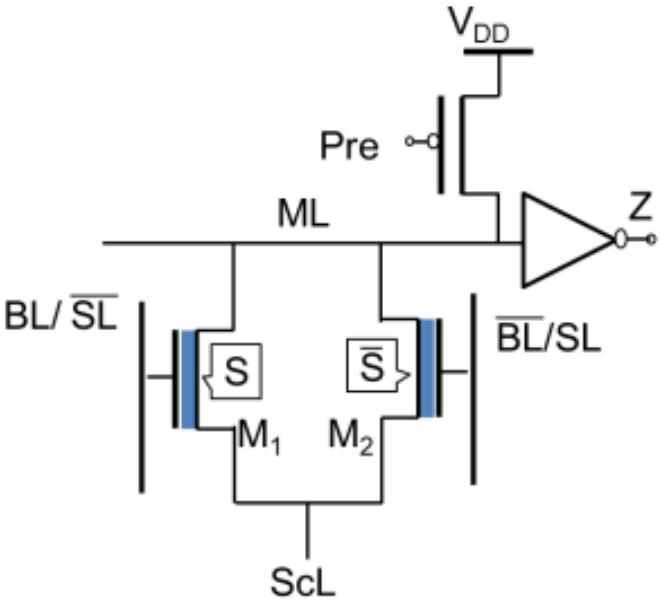


Switch 1 to 4

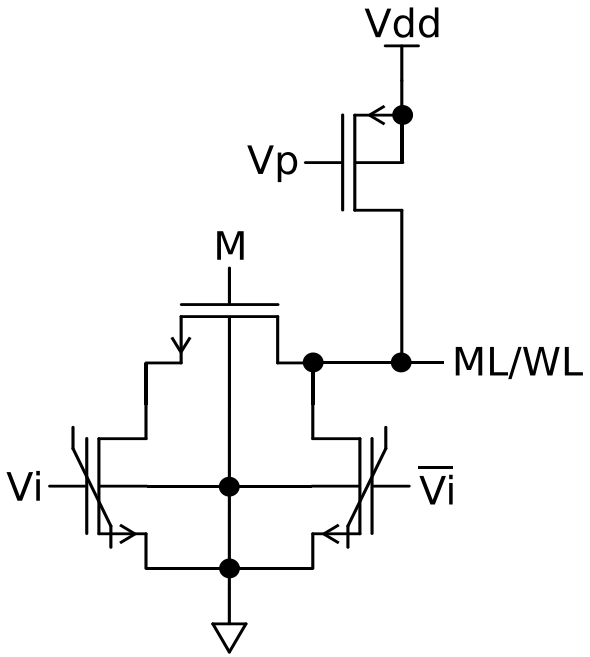


TCAM/RAM

- New design bloc:
  - TCAM : Ternary content addressable memory
  - RAM: classical memory addressable by address



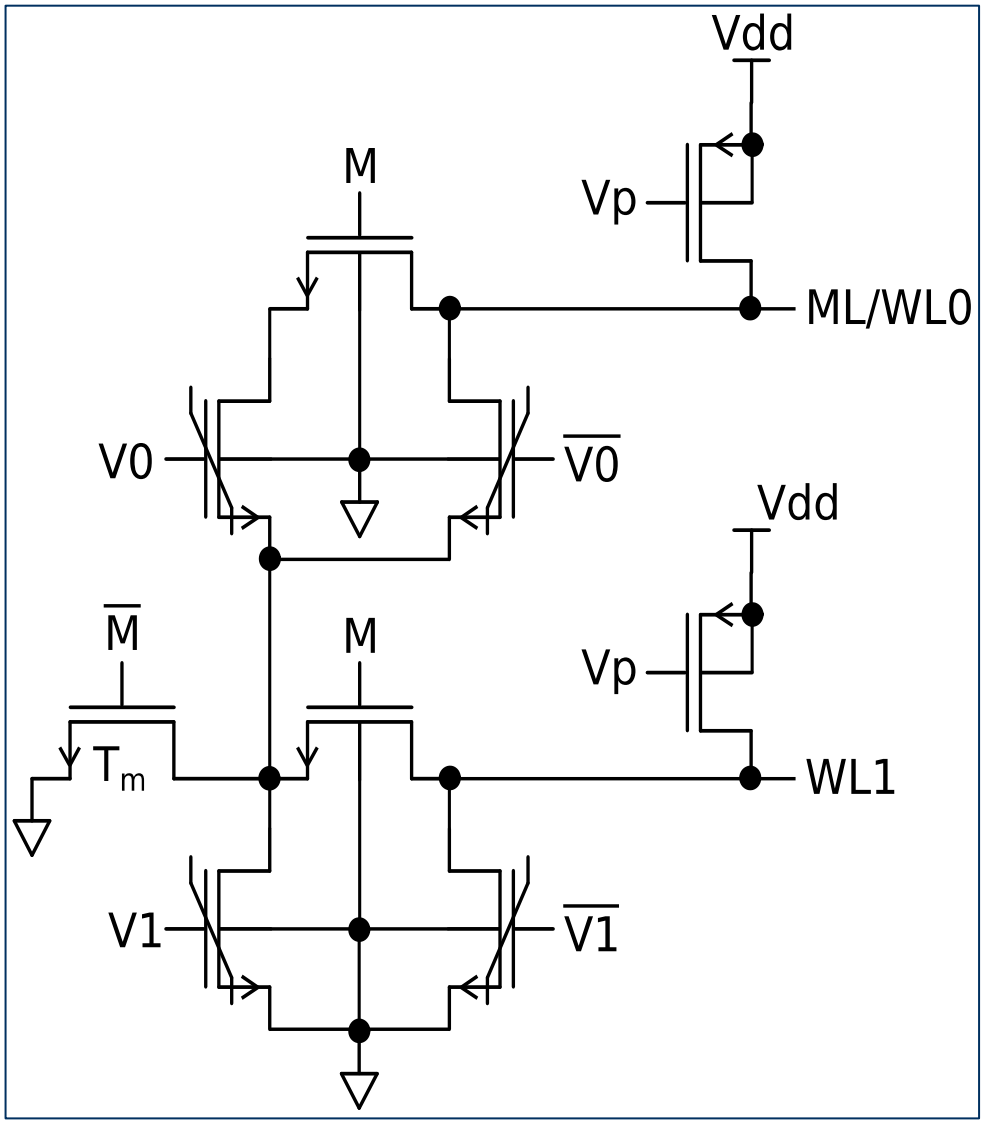
TCAM [1]



TCAM/RAM

[1] X. Yin, K. Ni, D. Reis, S. Datta, M. Niemier and X. S. Hu, "An Ultra-Dense 2FeFET TCAM Design Based on a Multi-Domain FeFET Model," in *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 66, no. 9, pp. 1577-1581, Sept. 2019, doi: 10.1109/TCSII.2018.2889225.

TCAM/RAM 2-bit, 4-bit, …



Multi-bit TCAM/RAM

PROs:
- Serially connected
- Partial word search
- Easy to scale

CONs:
- Half memory is loosed in RAM mode

TCAM/RAM (Sbox opportunities ?)

- Substitution operation is one of the most problematic in cryptographic implementations
  - Non-linear operation
  - Bijective operation

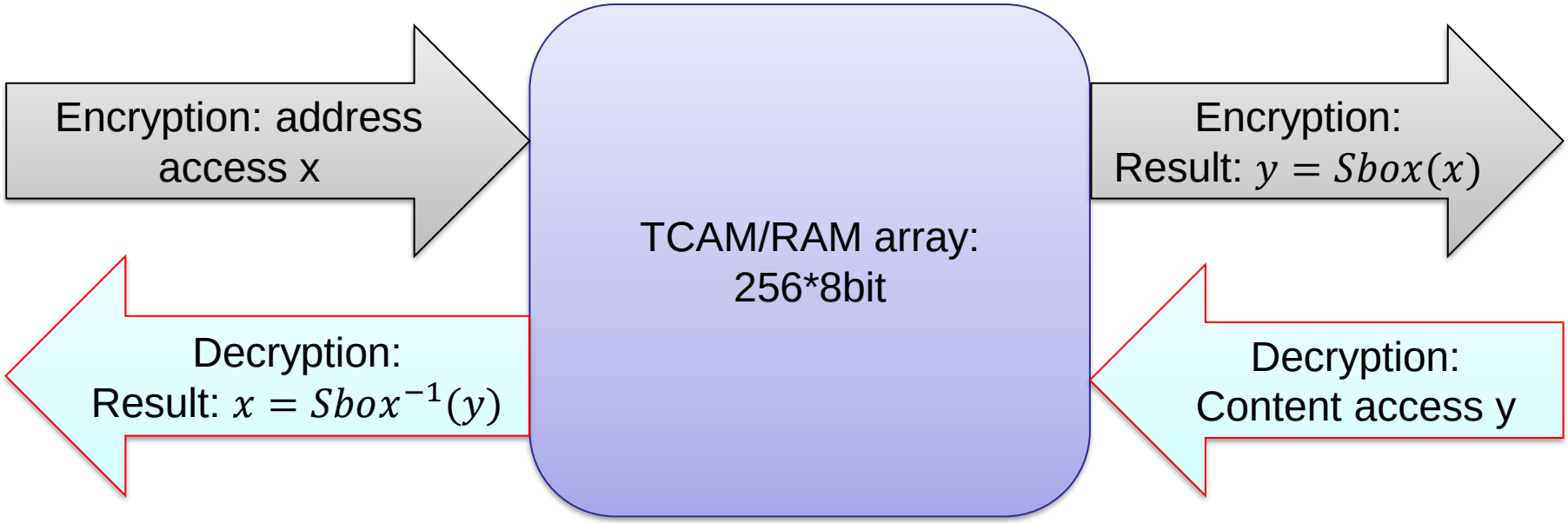
  →Lead to most side channel attacks

- In Von Neuman computing:
  - 1 memory table for encryption
  - 1 memory table for decryption

- Using TCAM/RAM:
  - 1 memory table only → inside the processor ?

TCAM/RAM (Sbox opportunities ?)

AES Exemple



Questions:

- Access pattern to avoid timing side channel attacks ?
- Does symmetric structures lead to power attacks resilience ?

Conclusion

- Ferroelectric CMOS compatibility:
  - Design non-volatile custom logic gates
  - Design non-volatile generic logic gates and routing structures
  - Explore new memory element

- Investigate security primitives' implementations:
  - Inside/aside processors ? Cryptographic operation ?
  - Specific primitives (PUF/TRNG)
    - Already exist with Magnetic and resistive technologies
    - To explore with ferroelectric technology

Thank you for your attention