Institut des Nanotechnologies de Lyon UMR 5270

Cryptographic implementation using Ferroelectric transistor

Cédric Marchand, Ian O'Connor, Stefan Slesazeck, Thomas Mikolajick

SECRET

Journée thématique du GDR

Agenda

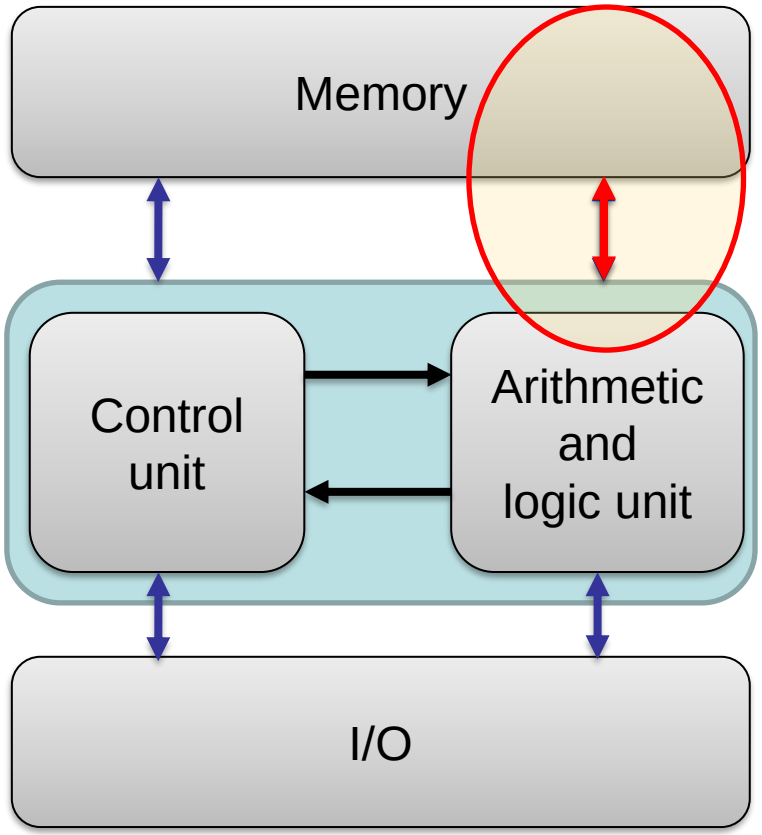
1. Introduction
2. Ferroelectric field effect transistor
3. TC-MEM memory and Sbox implementation
4. Non-volatile logic gates and operators for security
5. Conclusion

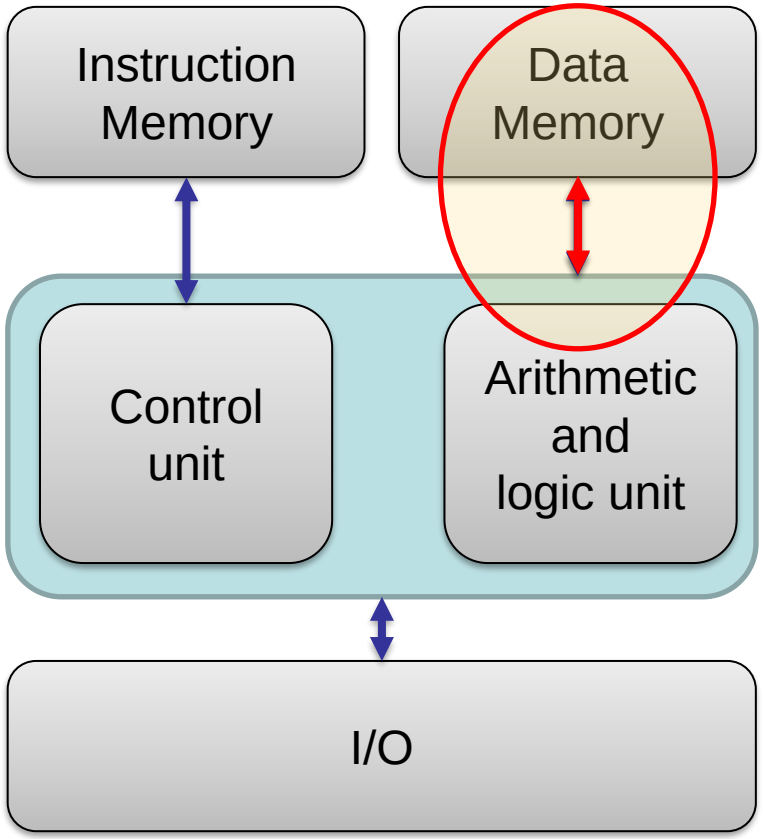
Agenda

1. Introduction
2. Ferroelectric field effect transistor
3. TC-MEM memory and Sbox implementation
4. Non-volatile logic gates and operators for security
5. Conclusion

Context (Classical computing architectures)

- Von Neumann Architecture/ Harvard Architecture
  - Data transfert congestion





Limit performances and energy efficiency

Sensor node security

Edge

Data acquisition + computation

information (protected)

decision

communication + data fusion + computation

meta-information

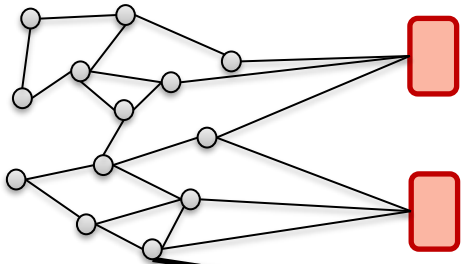
cloud

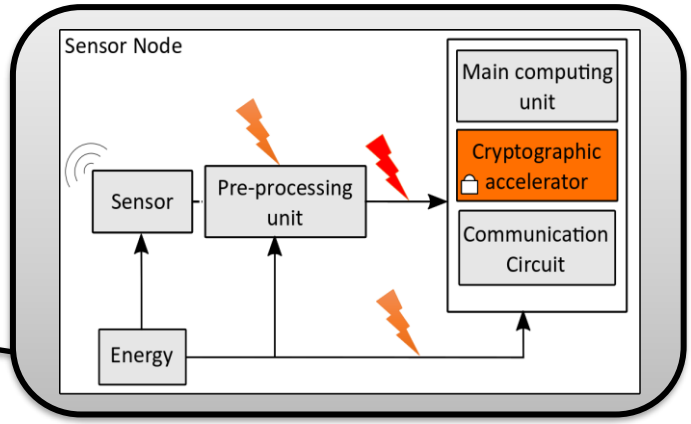
meta-processing

Logic in memory
In-memory computing

in-network computing

in-cloud computing





Need for a Secure and Highly energy efficient Computing platform

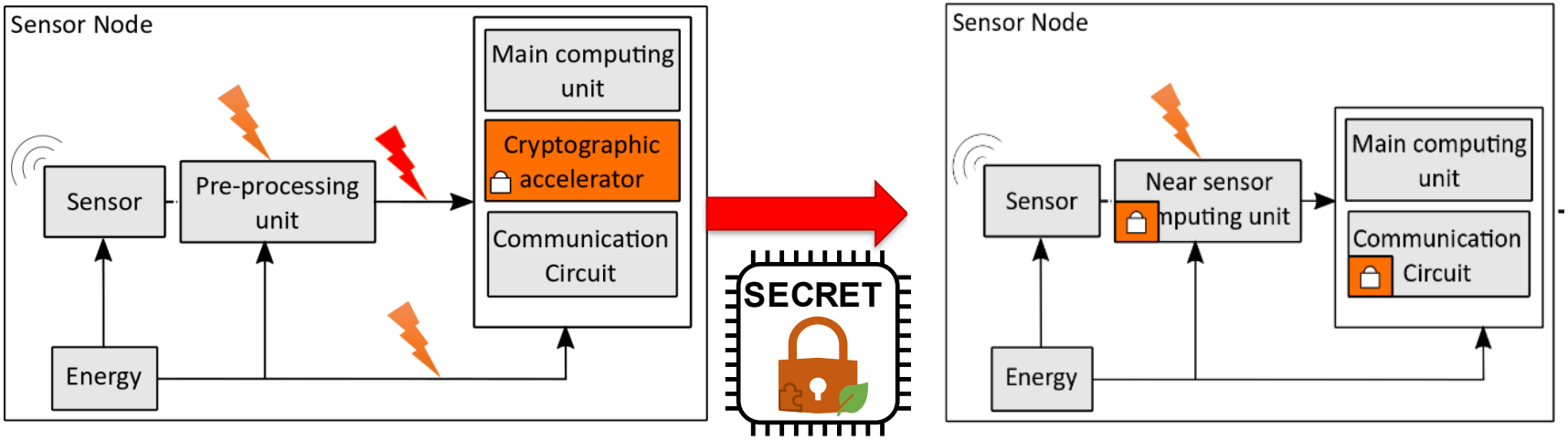
Non-volatile Opportunities

- Emerging and CMOS compatible Non-Volatile memory technologies:
  - New non-volatile logic capabilities
  - Logic in memory

- Opportunity to change the Hardware architectures of computing unit to include Non-Volatile structures:
  - Memory array with computing capabilities
  - Programmable logic gate
  - Custom logic operation with non-volatile operand(s)

- Concept of near-sensor cryptography using non-volatile operations in the pre-processing unit

Non-volatile emerging technologies opportunities



- Add a low-cost security layer in the preprocessing Unit :
  - Use emerging technologies (FeFet for example) to implement part of cryptographic operations inside the preprocessing Unit (Sbox, constant matrix multiplication, …)

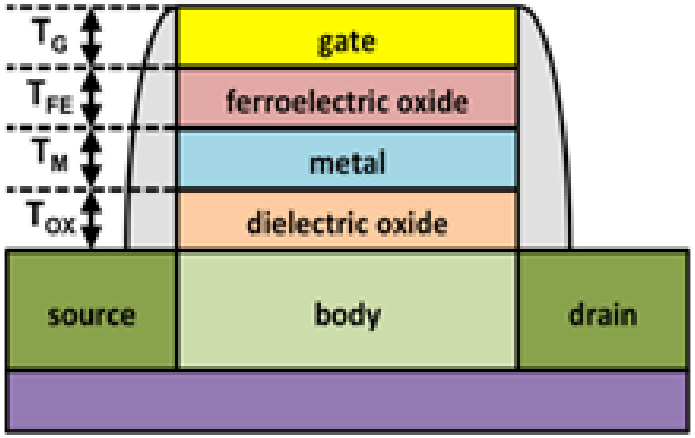
  → **In-Memory-Computing** can play a role

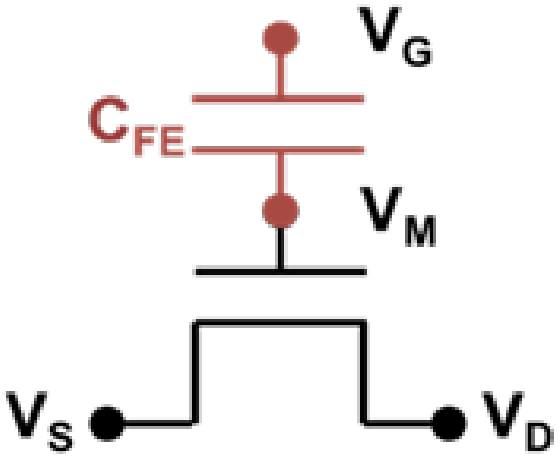
  → Emerging **TCAM** design → possibility to create a hybrid memory (TCAM and MEM) : the TC-MEM

Agenda

1. Introduction
2. Ferroelectric field effect transistor
3. TC-MEM memory and Sbox implementation
4. Non-volatile logic gates and operators for security
5. Conclusion

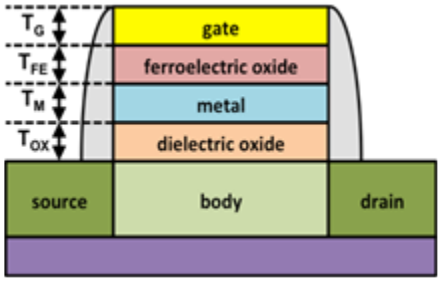
Ferroelectric Field Effect Transistor

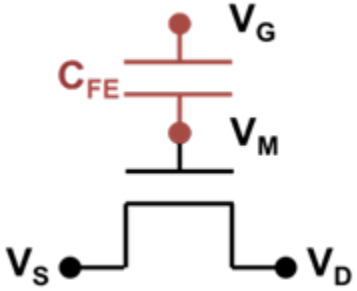


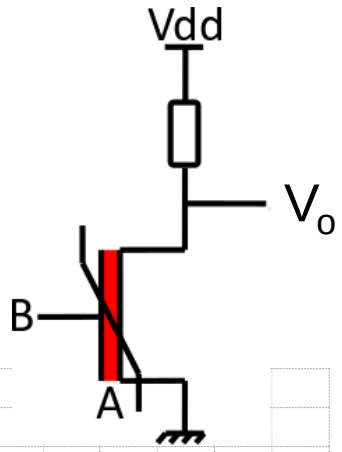


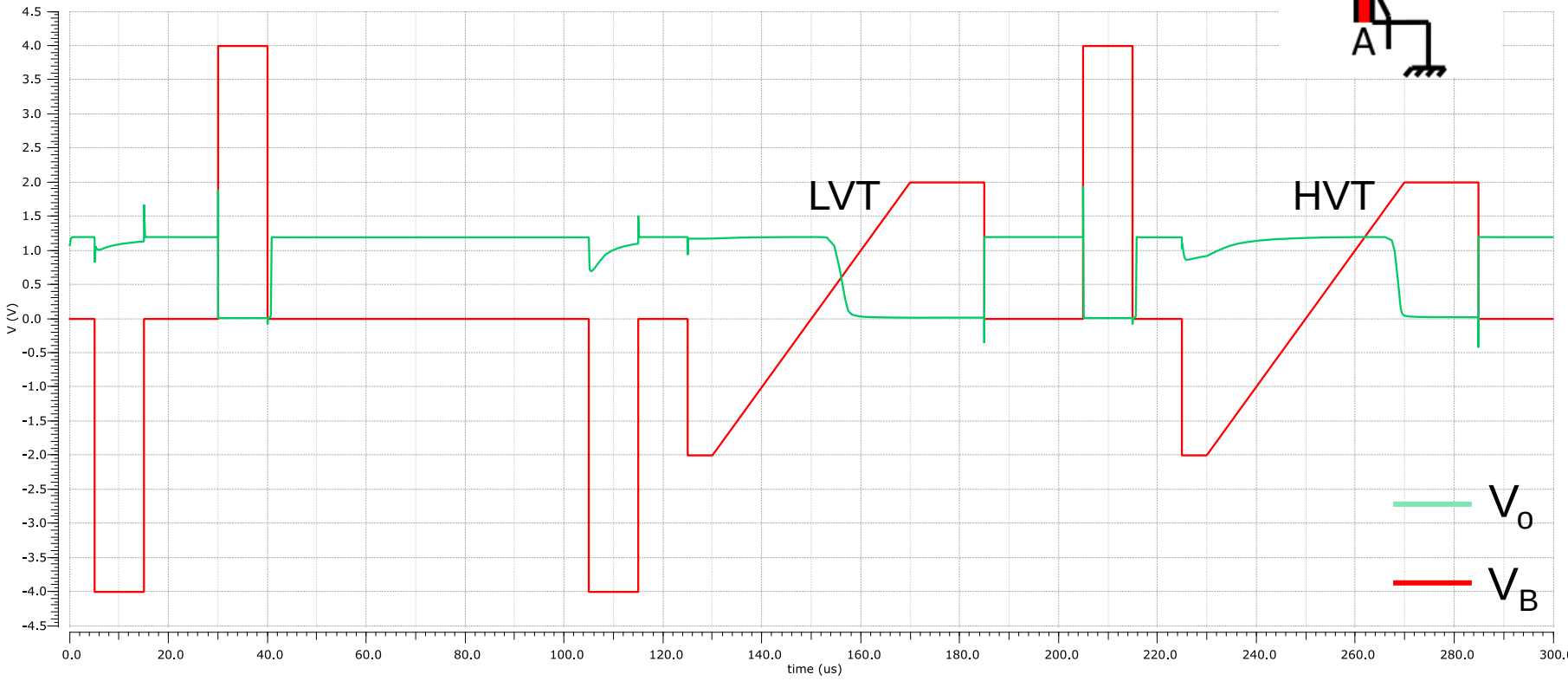
FeFET : single transistor characteristics

FeFET dimension:
W = 500 nm
L = 500 nm



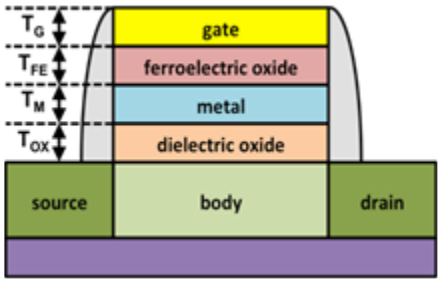


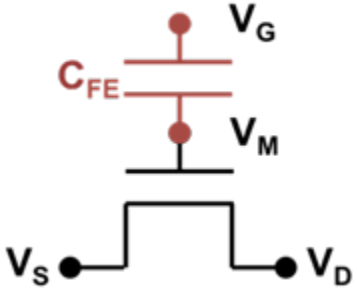


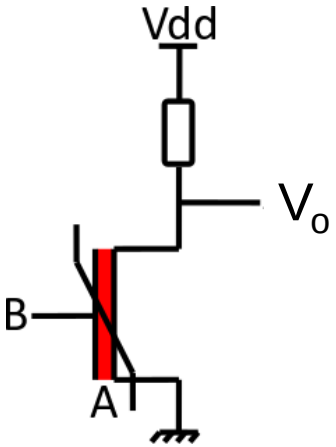


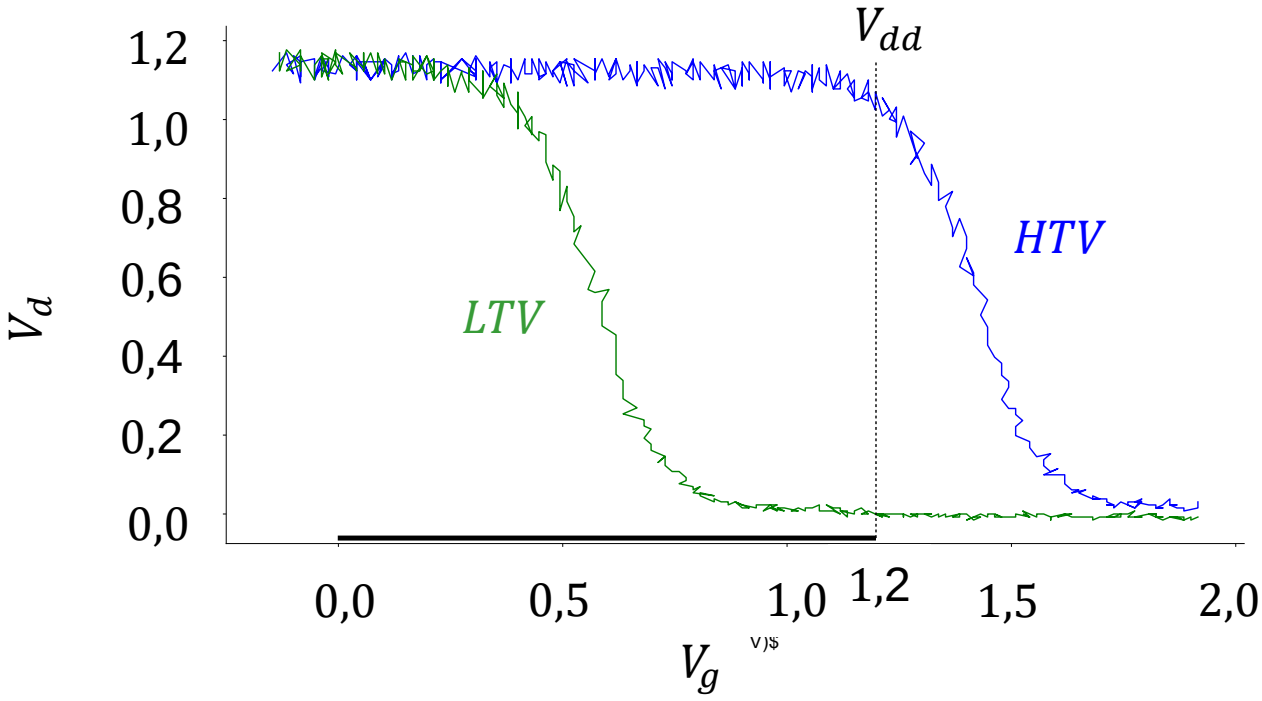
FeFET : single transistor characteristics

FeFET dimension:
W = 500 nm
L = 500 nm







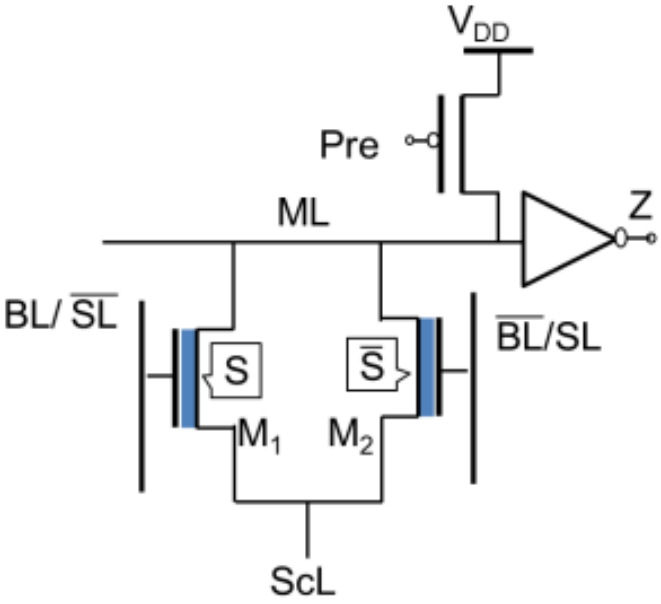


Agenda

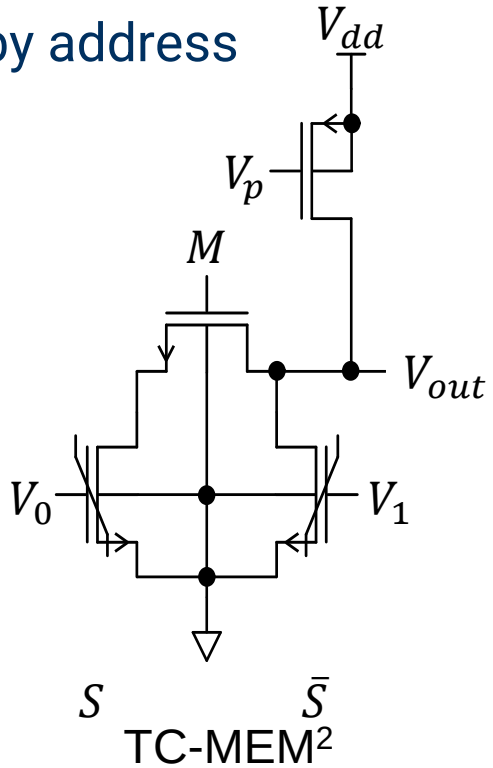
1. Introduction
2. Ferroelectric field effect transistor
3. TC-MEM memory and Sbox implementation
4. Non-volatile logic gates and operators for security
5. Conclusion

TC-MEM

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



TCAM[1]



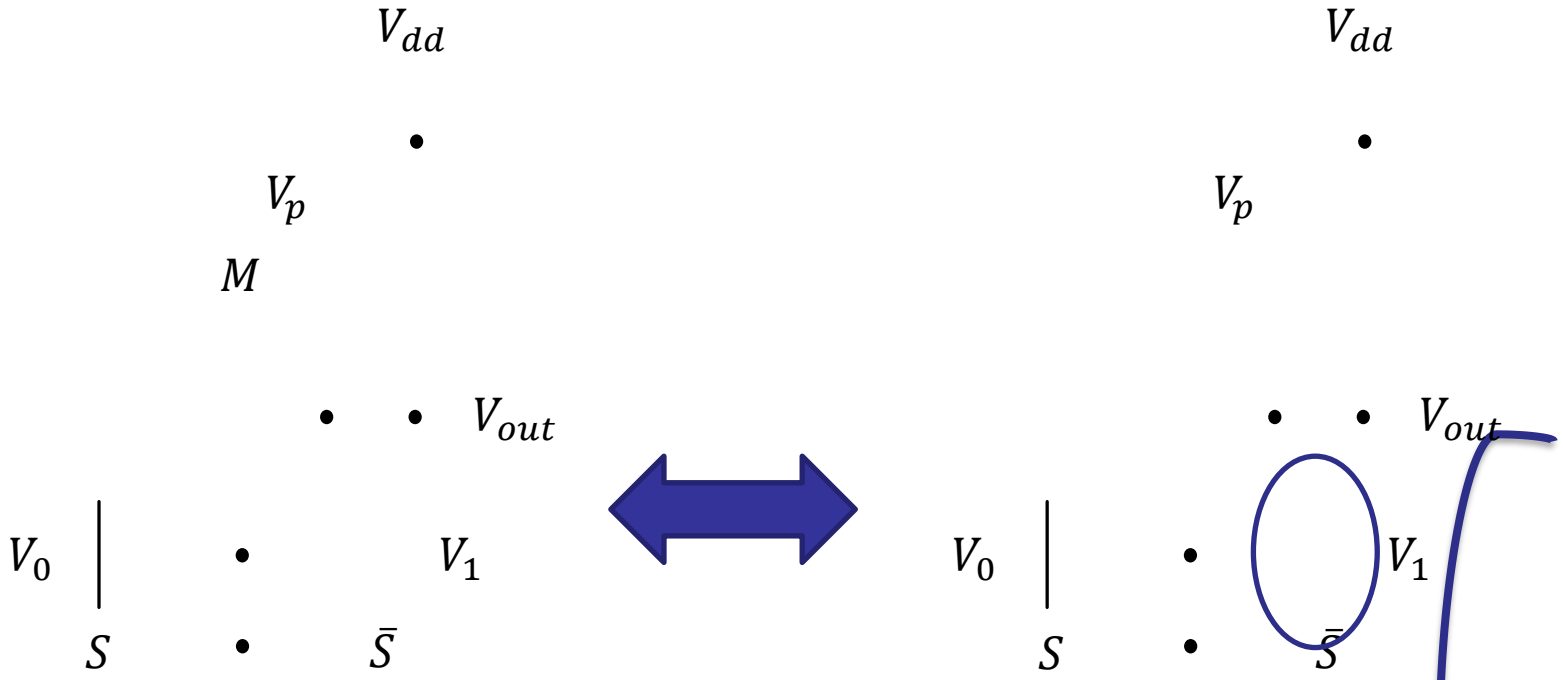
TC-MEM[2]

[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.

[2] C. Marchand, I. O'Connor, M. Cantan, E. T. Breyer, S. Slesazeck and T. Mikolajick, "**A FeFET-Based Hybrid Memory Accessible by Content and by Address**," in IEEE Journal on Exploratory Solid-State Computational Devices and Circuits, vol. 8, no. 1, pp. 19-26, June 2022, doi: 10.1109/JXCDC.2022.3168057.

TC-MEM

- $M = 0$: Memory mode

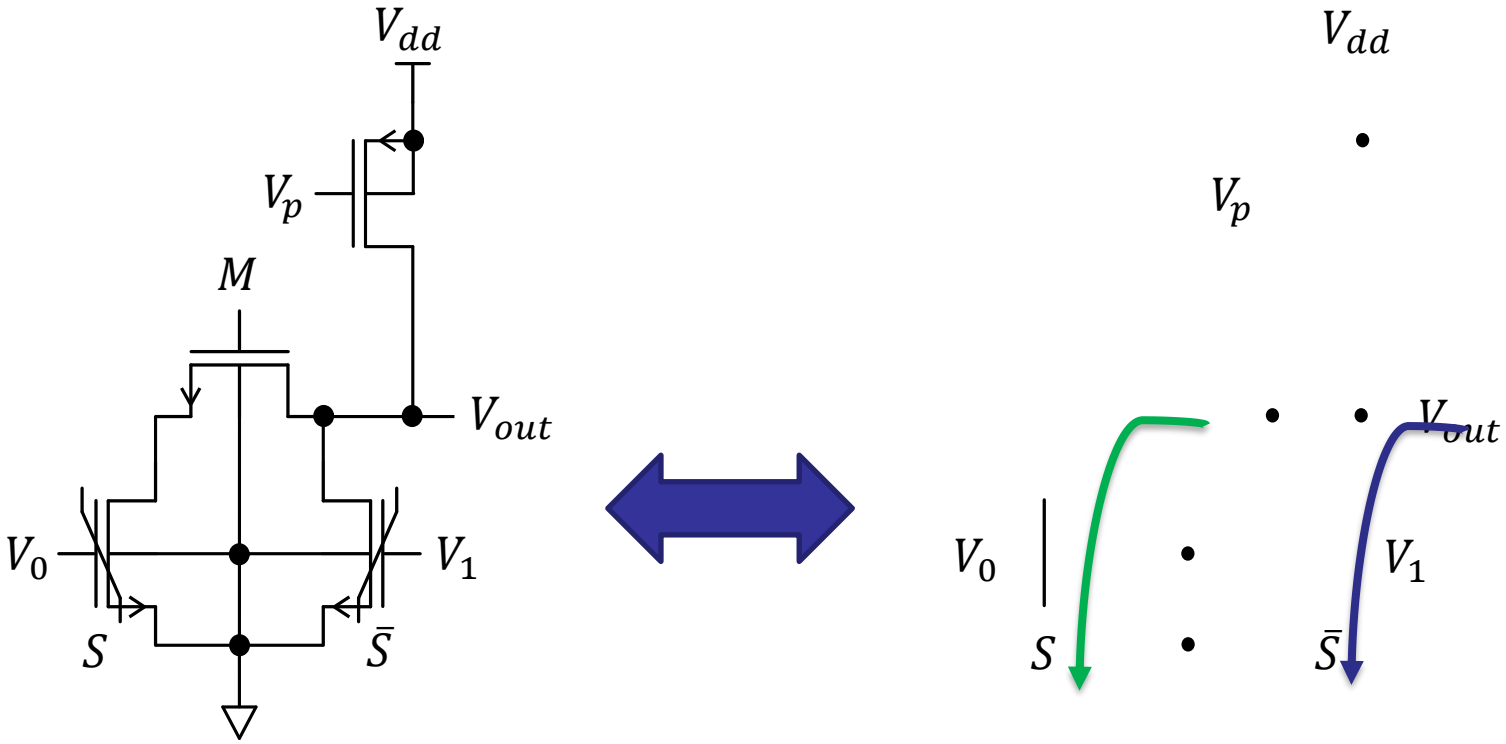


$$V_o = \overline{V_1 . \bar{S}}$$

- When the bit is read, $V_1 = 1 \Rightarrow V_o = \overline{1 . \bar{S}} = S$

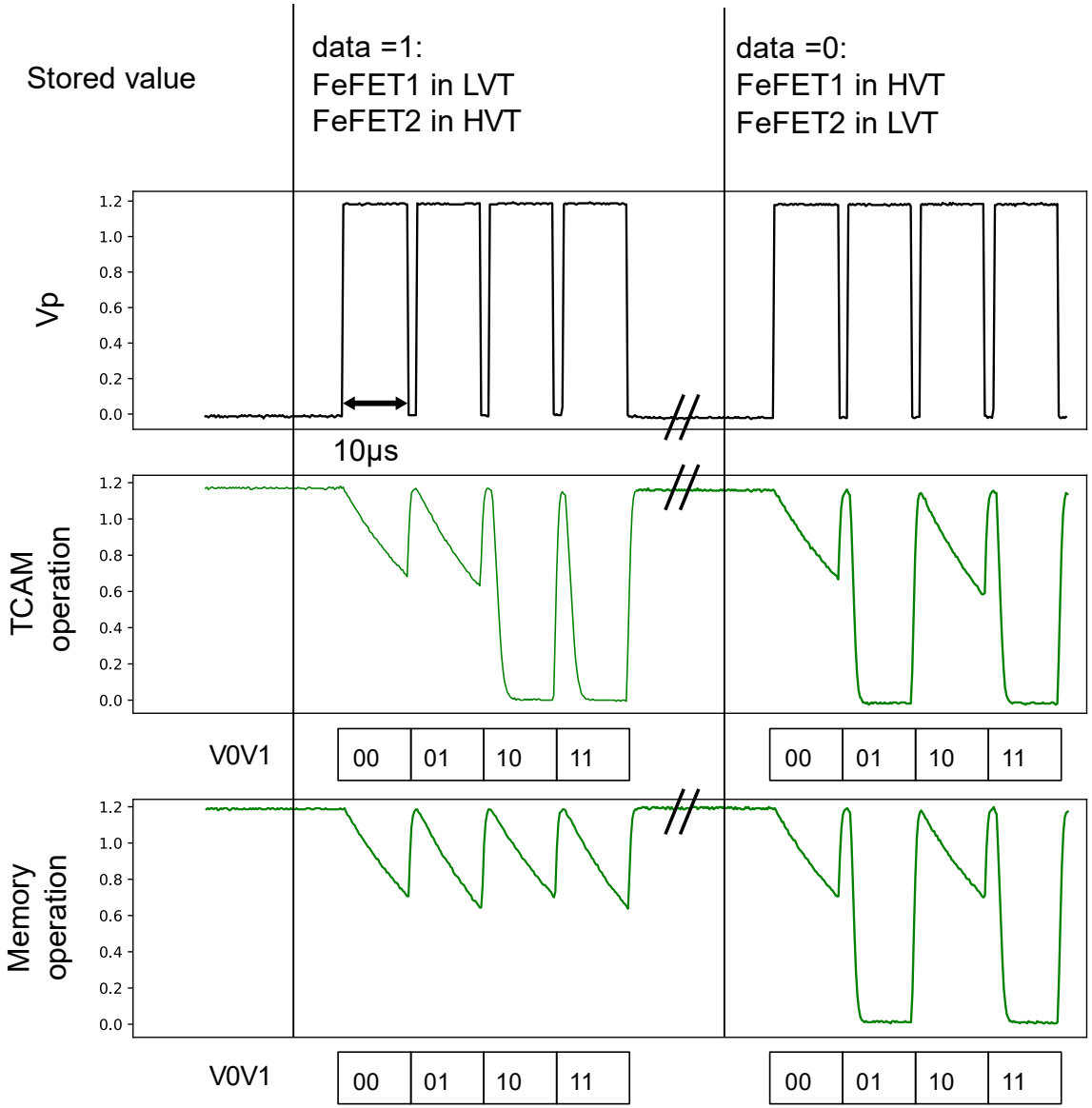
TC-MEM

- $M = 1$: TCAM mode



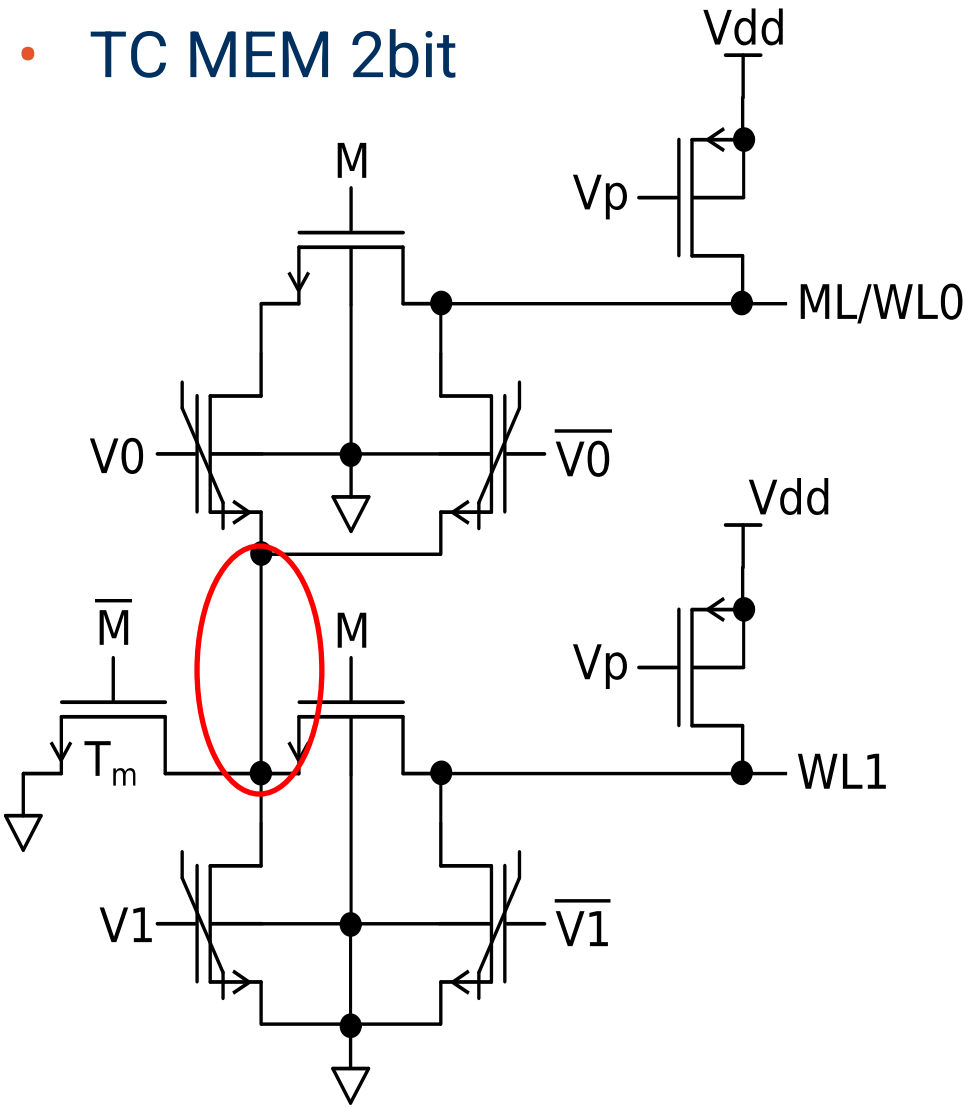
$$V_{out} = \overline{V_0.S}.\overline{V_1.\bar{S}}$$

TC-MEM (chip measurement)



TC MEM 1st generation

- TC MEM 2bit

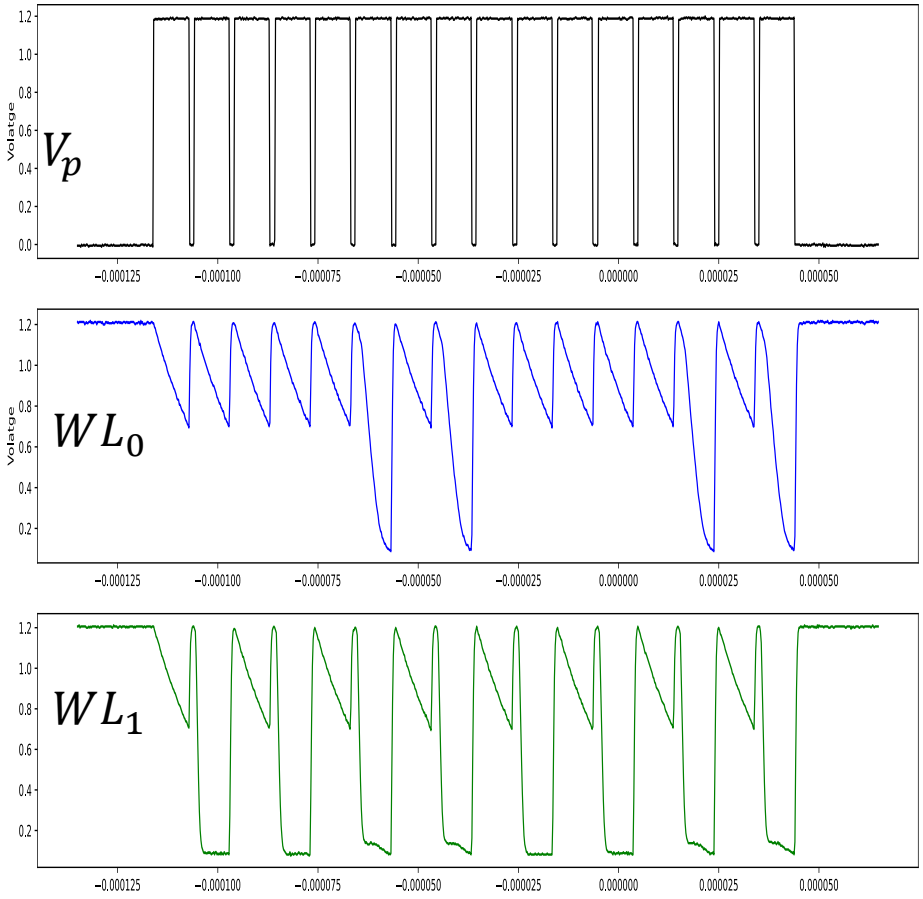


Serial connection problem :

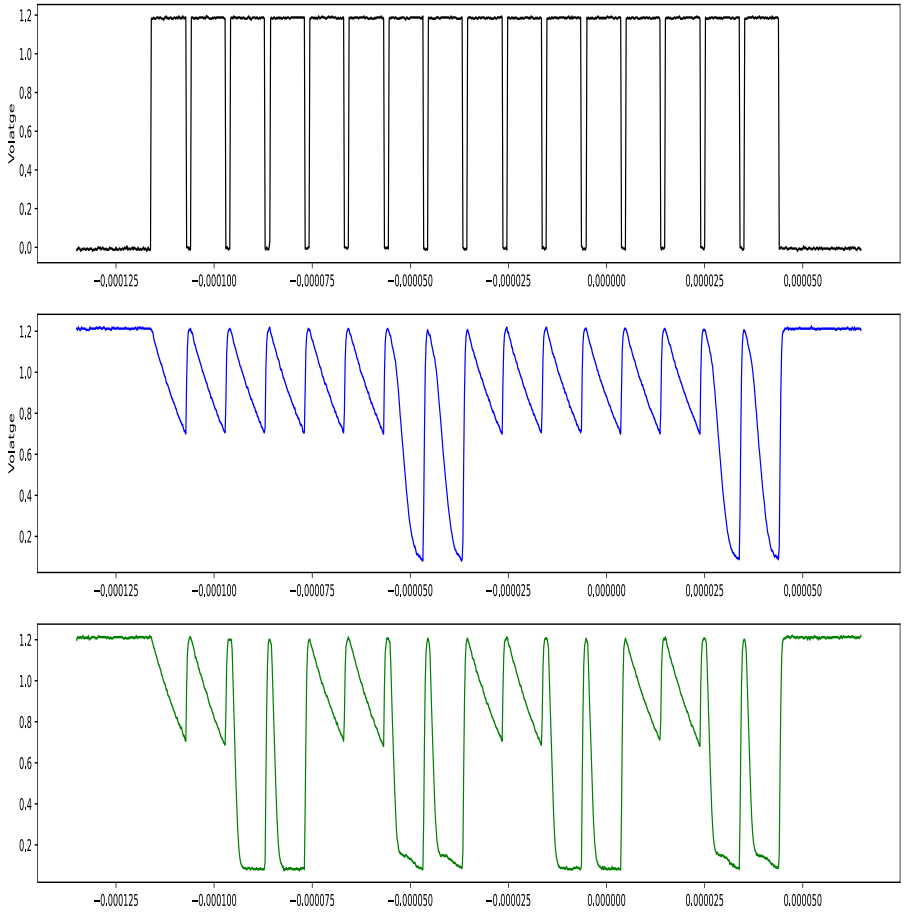
- Programming in TCAM mode:
  - Left FeFET powered
  - Upper FeFET connected to V_{dd} from drain and source
- Consequence :
  - The upper left FeFET remains un-program in some cases.
- Possible solution :
  - Bring a possible separation between the bitcell.

TC MEM 1st generation

- Cannot program $FeFET_0$ (connected to V_0)



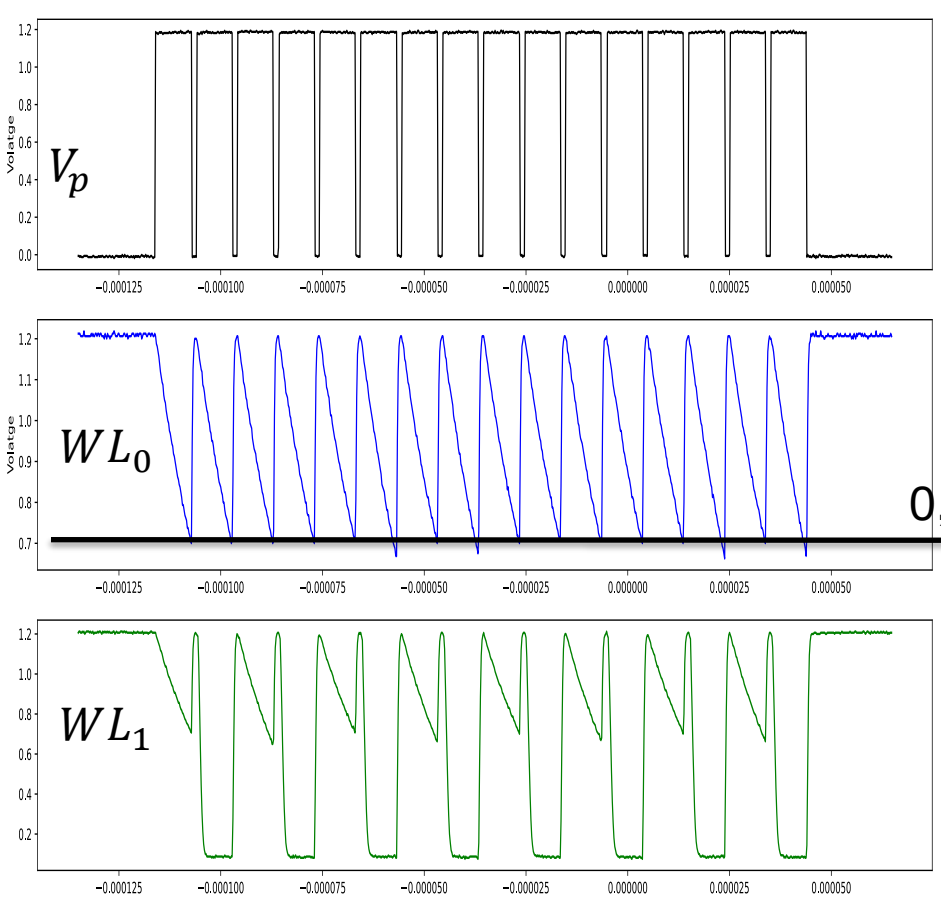
$A_0A_1 = 00$



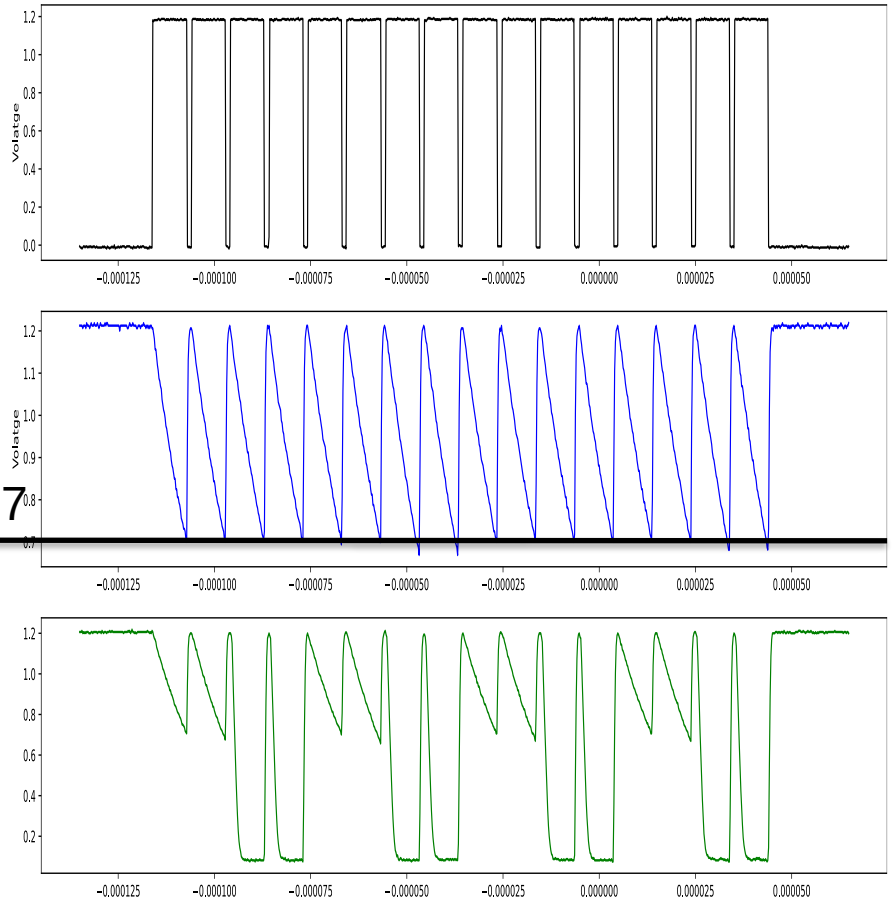
$A_0A_1 = 01$

TC MEM 1st generation

- Cannot program $FeFET_0$ (connected to V_0)

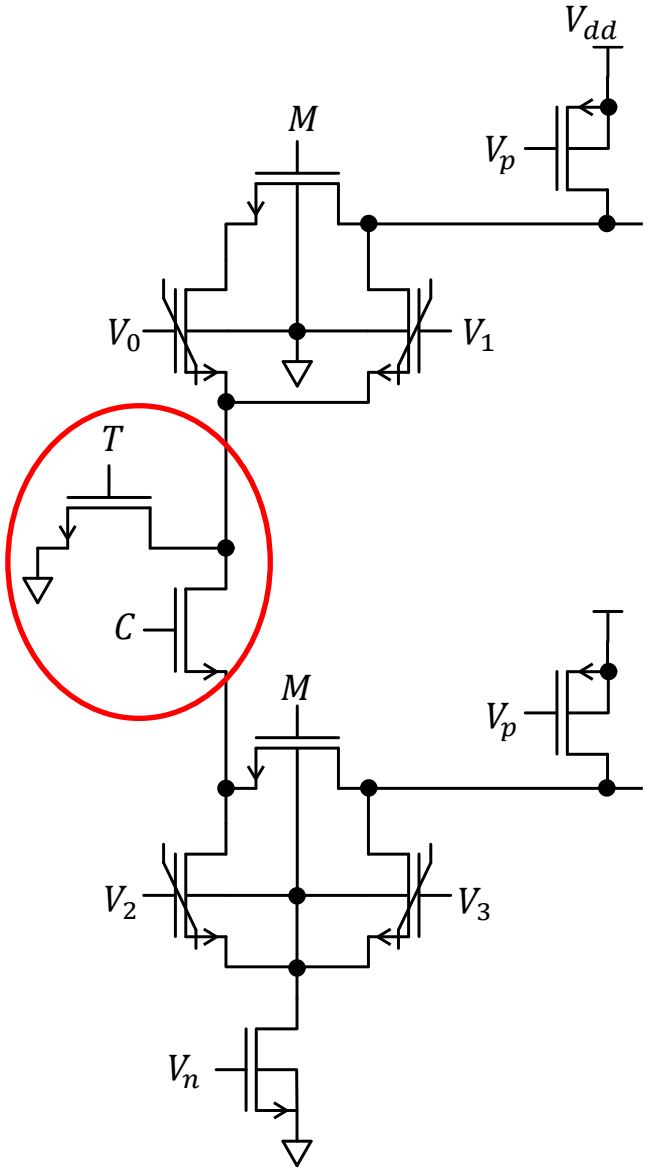


$A_0A_1 = 10$



$A_0A_1 = 11$

TC MEM 2nd generation



New scaling circuit :

- Programming the bitcells:
  - TCAM Mode
  - T=1 and C=0

→ Ensure disconnected bitcells and proper programming

- Existence of forbidden state:
  - $M = T = C = 0$
  - $M = 1, T = C = 0$

  } Floating node

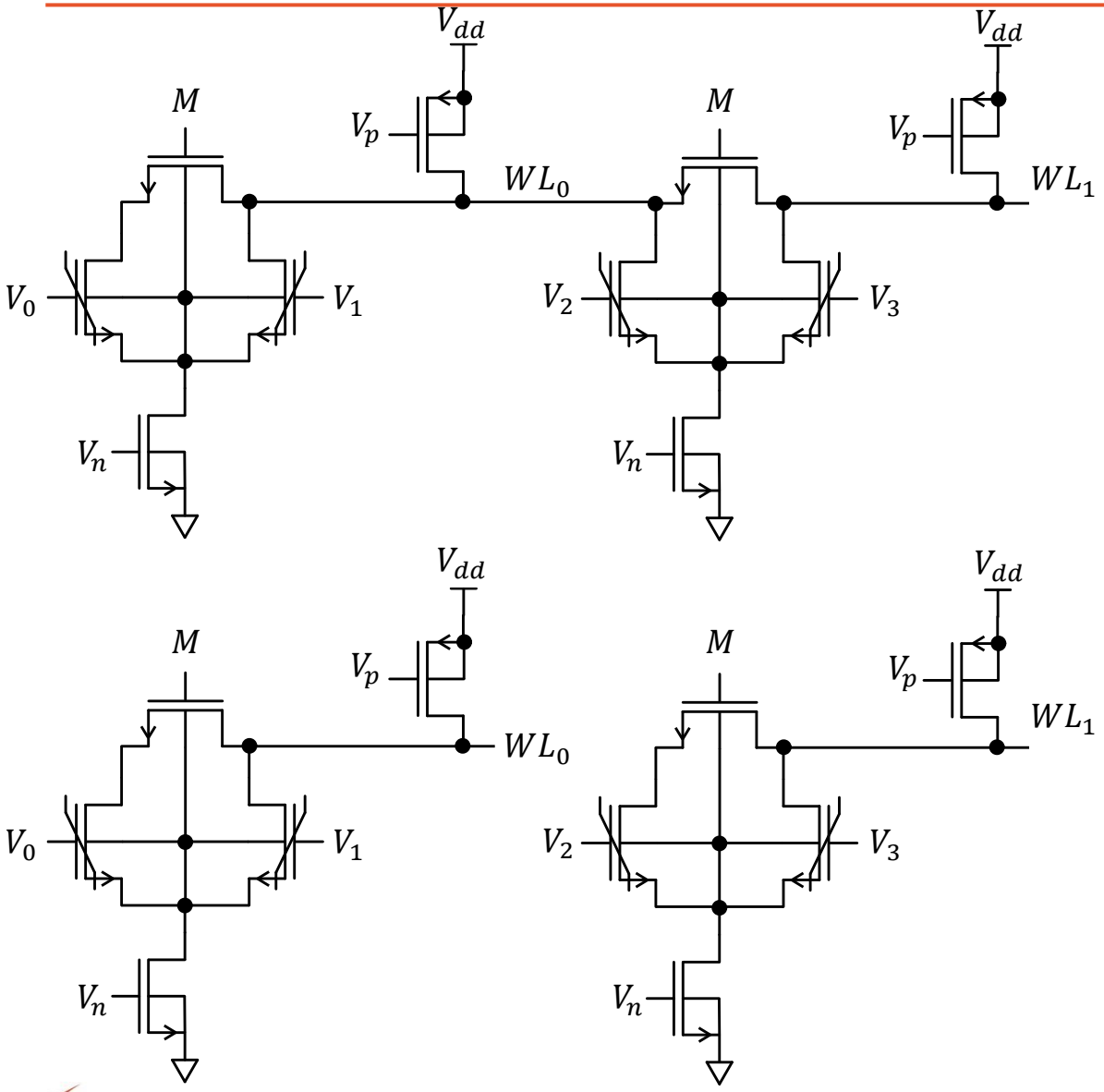
  - $M = 0, T = C = 1$
  - $M = T = C = 1$

  } Possible but useless

  → $\boldsymbol{T = \overline{C}}$

  → 4 remaining utilizations :
    - → Memory
    - → TCAM
    - → Bitwise Xor
    - → Memory with connected bits ?

TC MEM other solutions



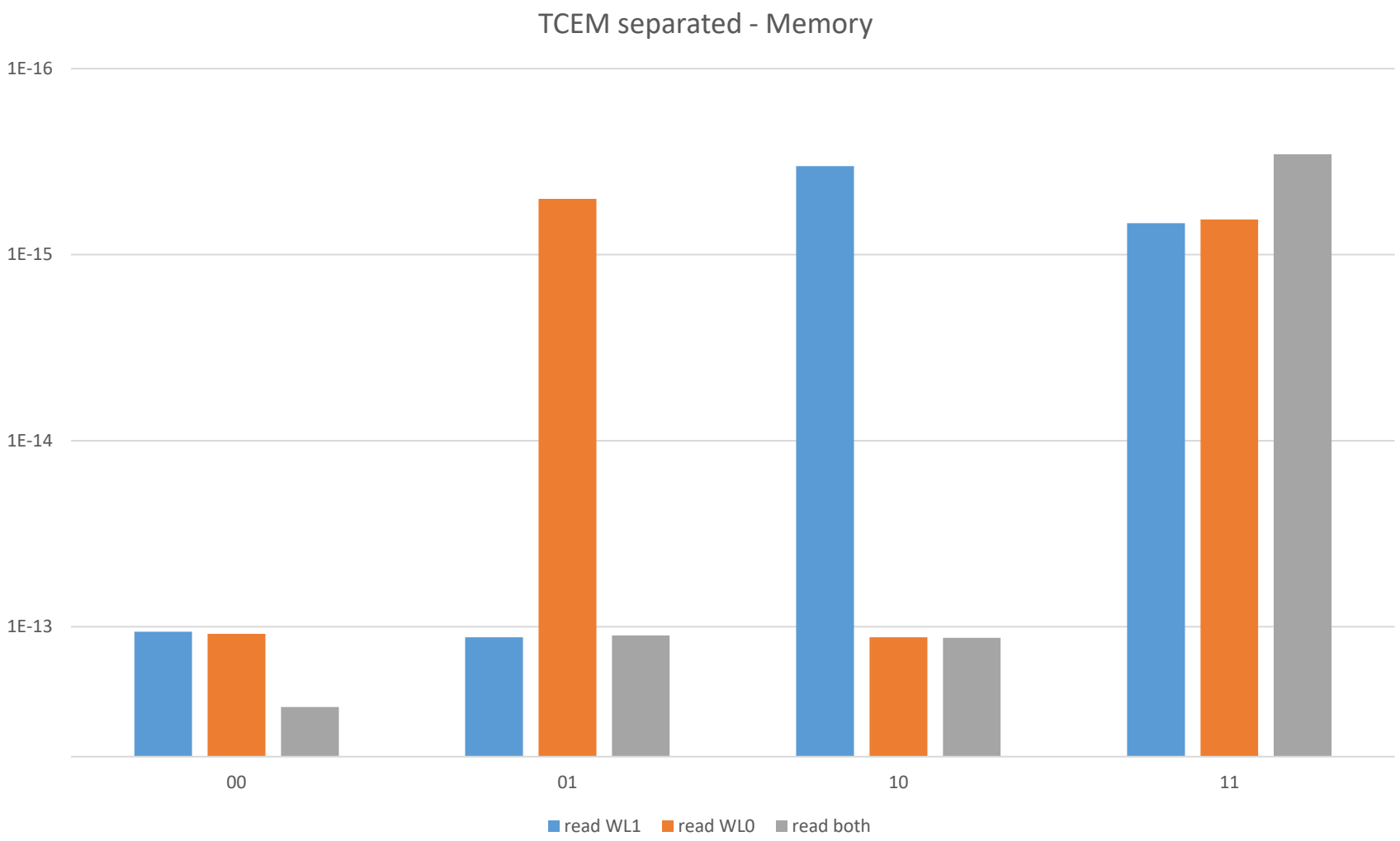
Parallelly connected:

- Global match
- No limit in size ?
- More difficult to read in memory
- fewer functionality

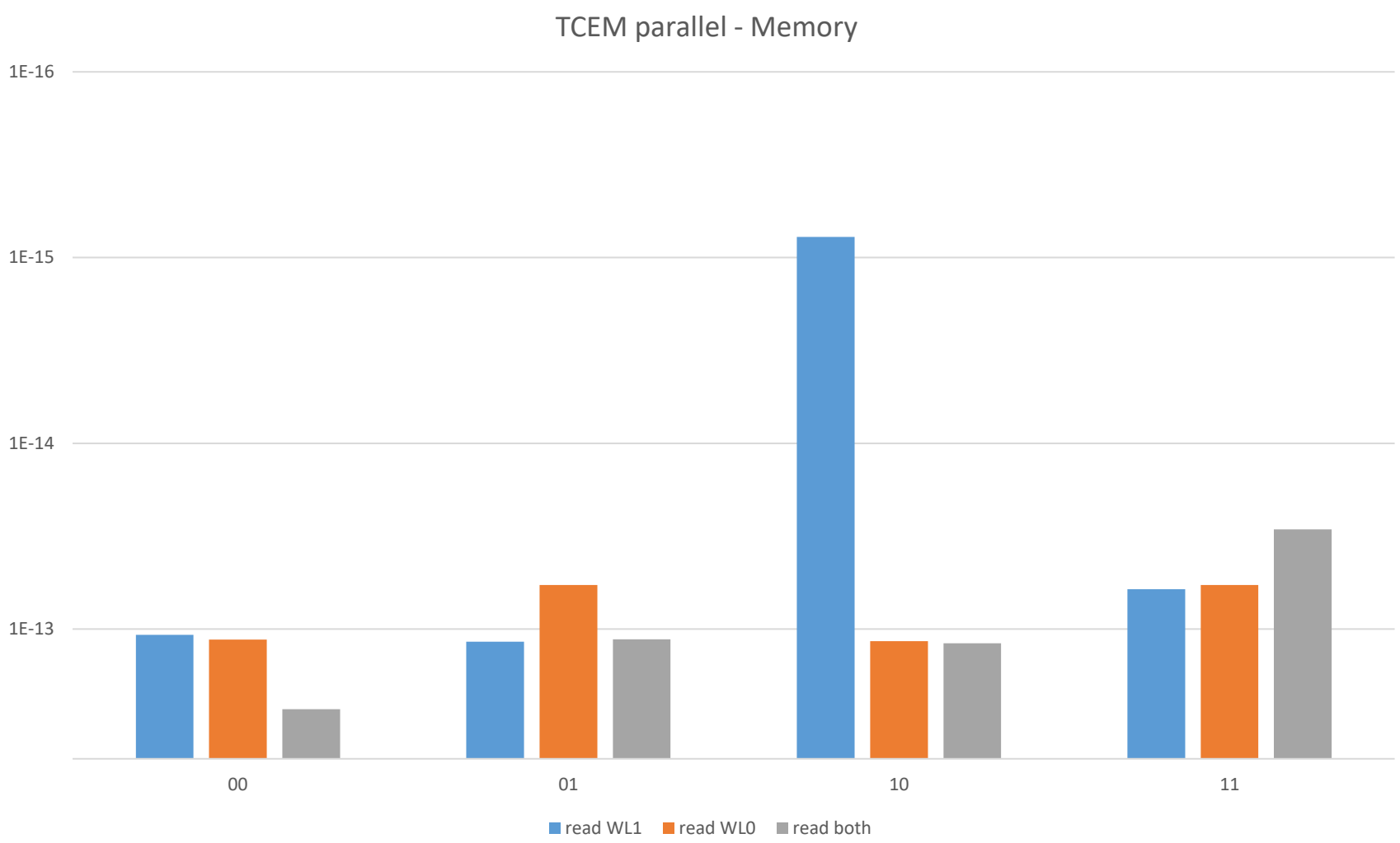
Fully separated:

- No global match
  - Bigger output circuit
- No limit in size ?
- All functionality are possible

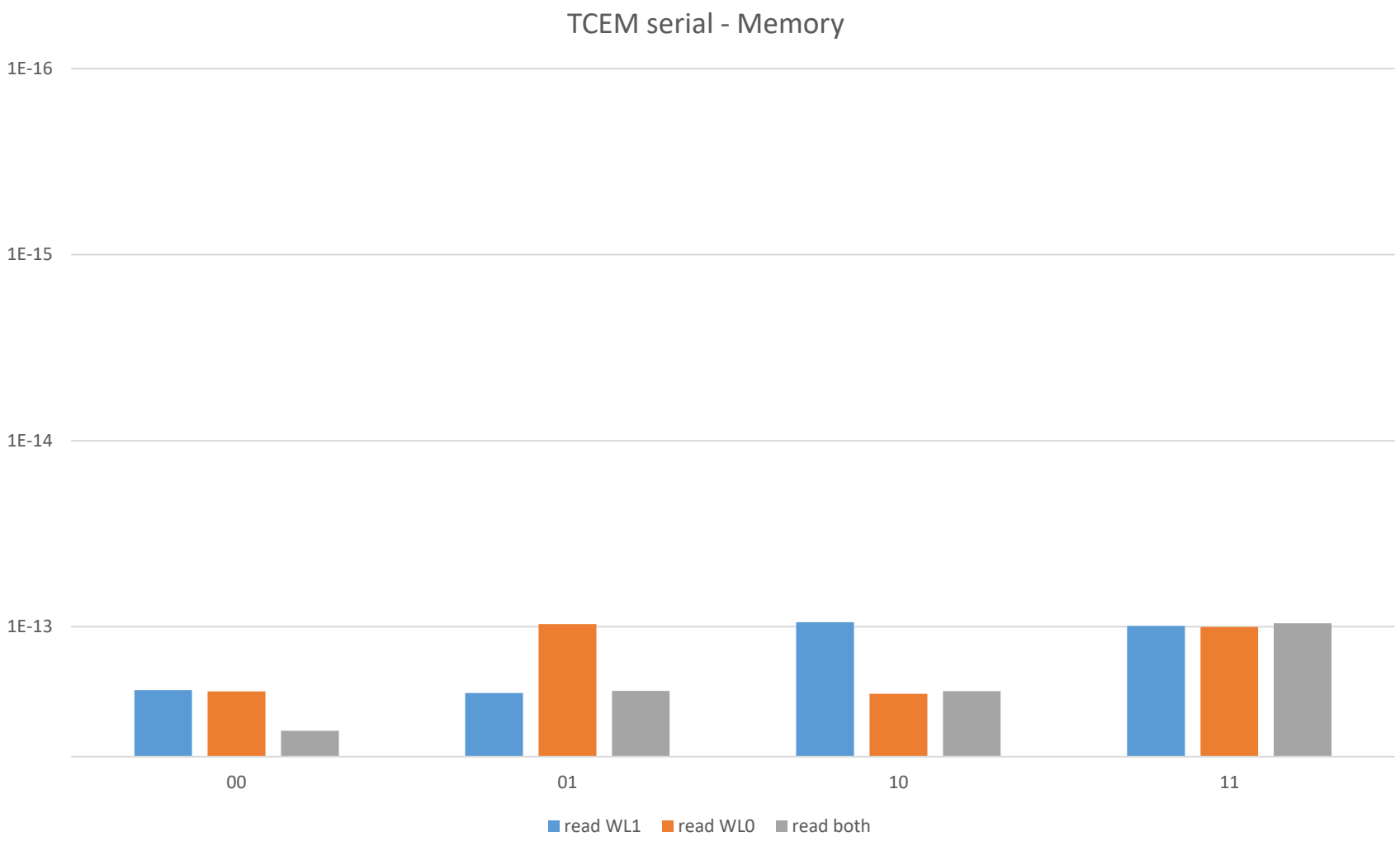
Memory mode : 2-bit fully separated



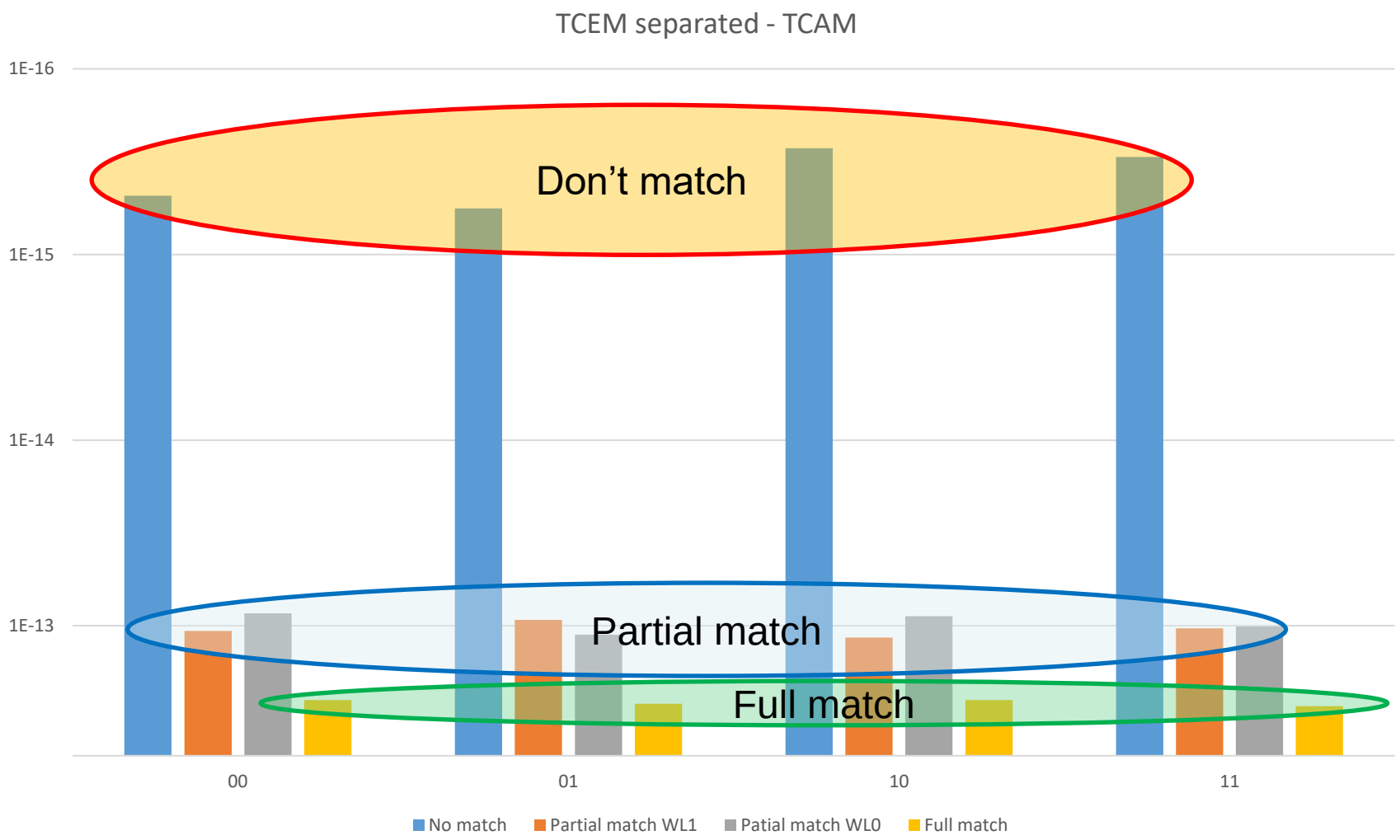
Memory mode : 2-bit parallelly connected



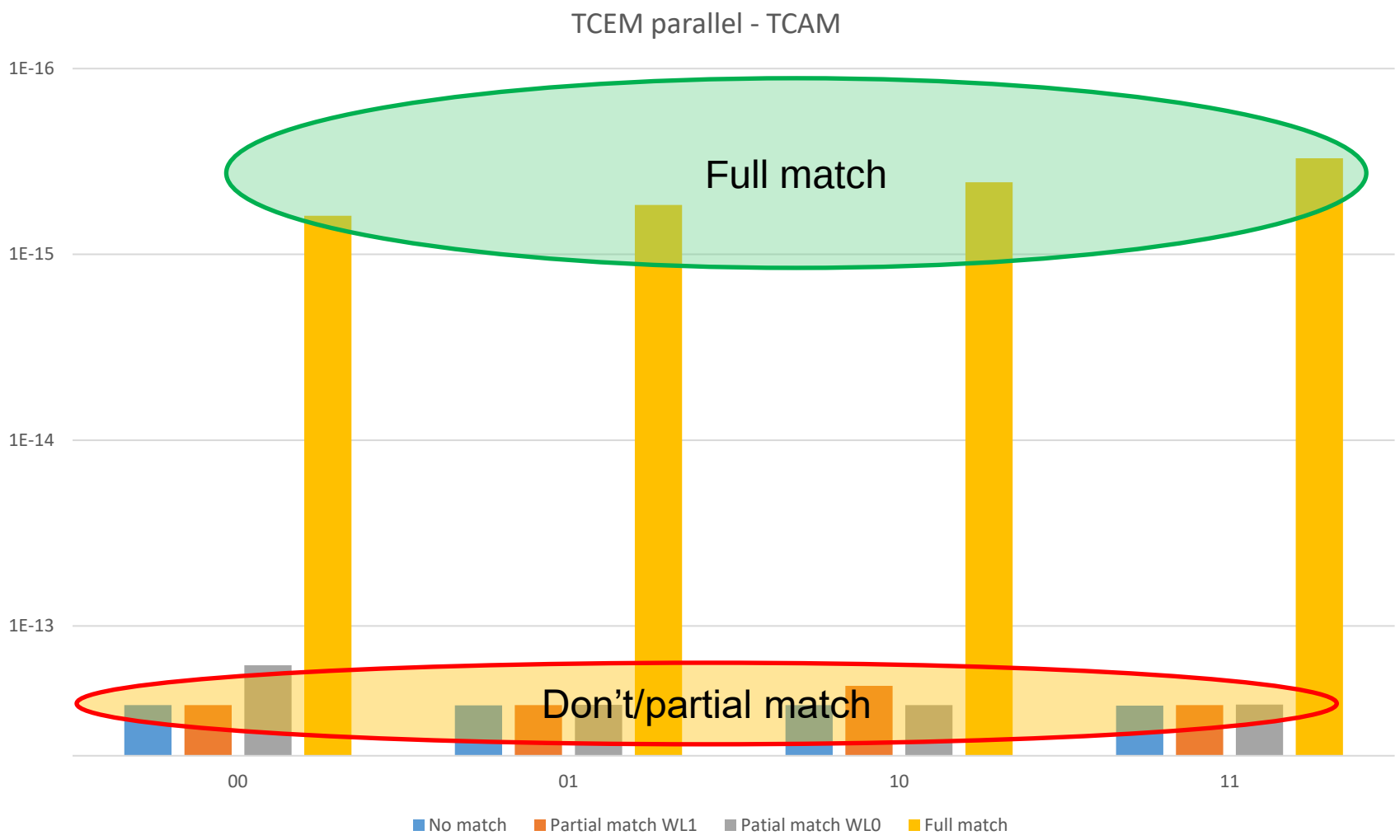
Memory mode : 2-bit serially connected



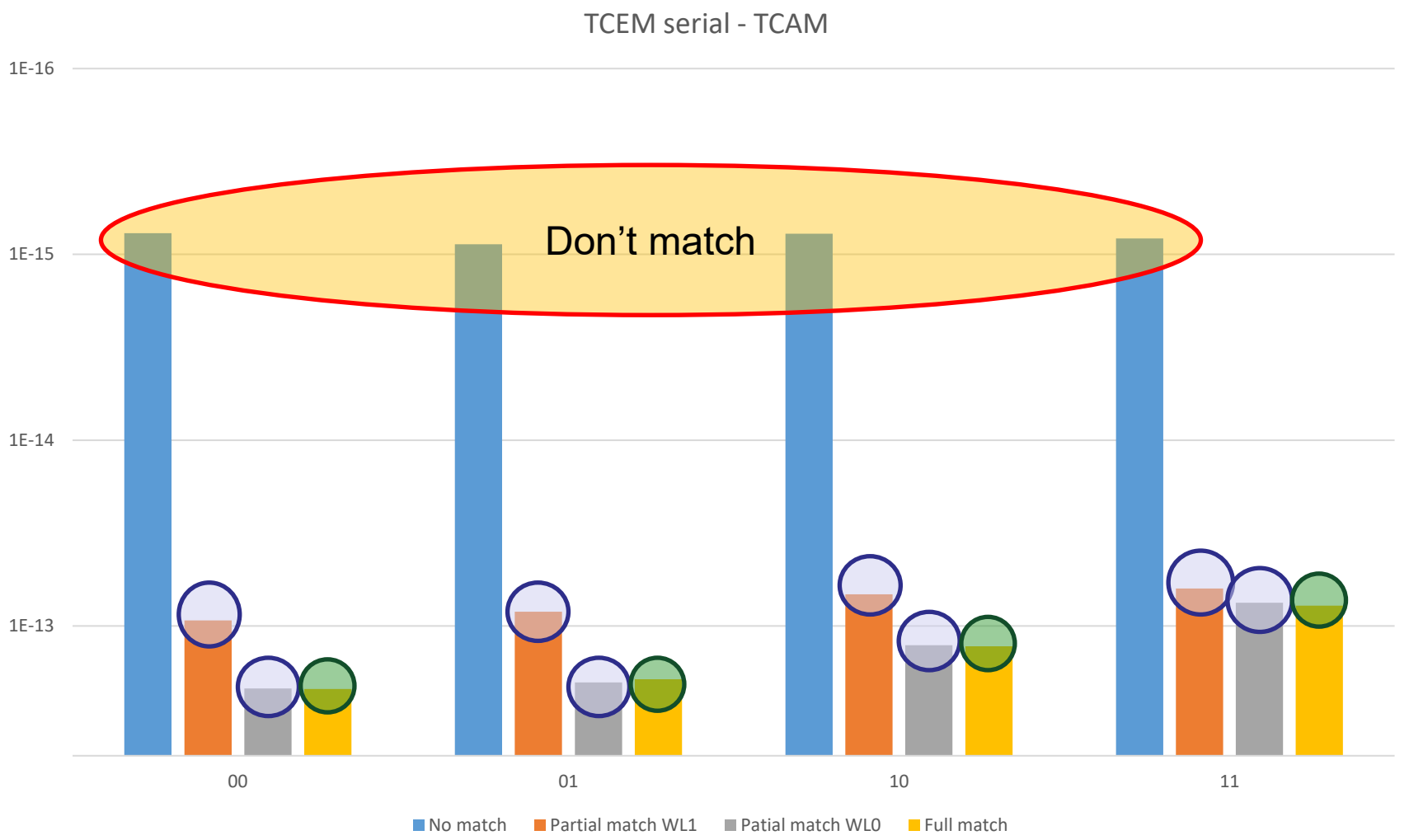
TCAM mode : 2-bit fully separated



TCAM mode : 2-bit parallelly connected



TCAM mode : 2-bit serially connected



Comparison and discussion

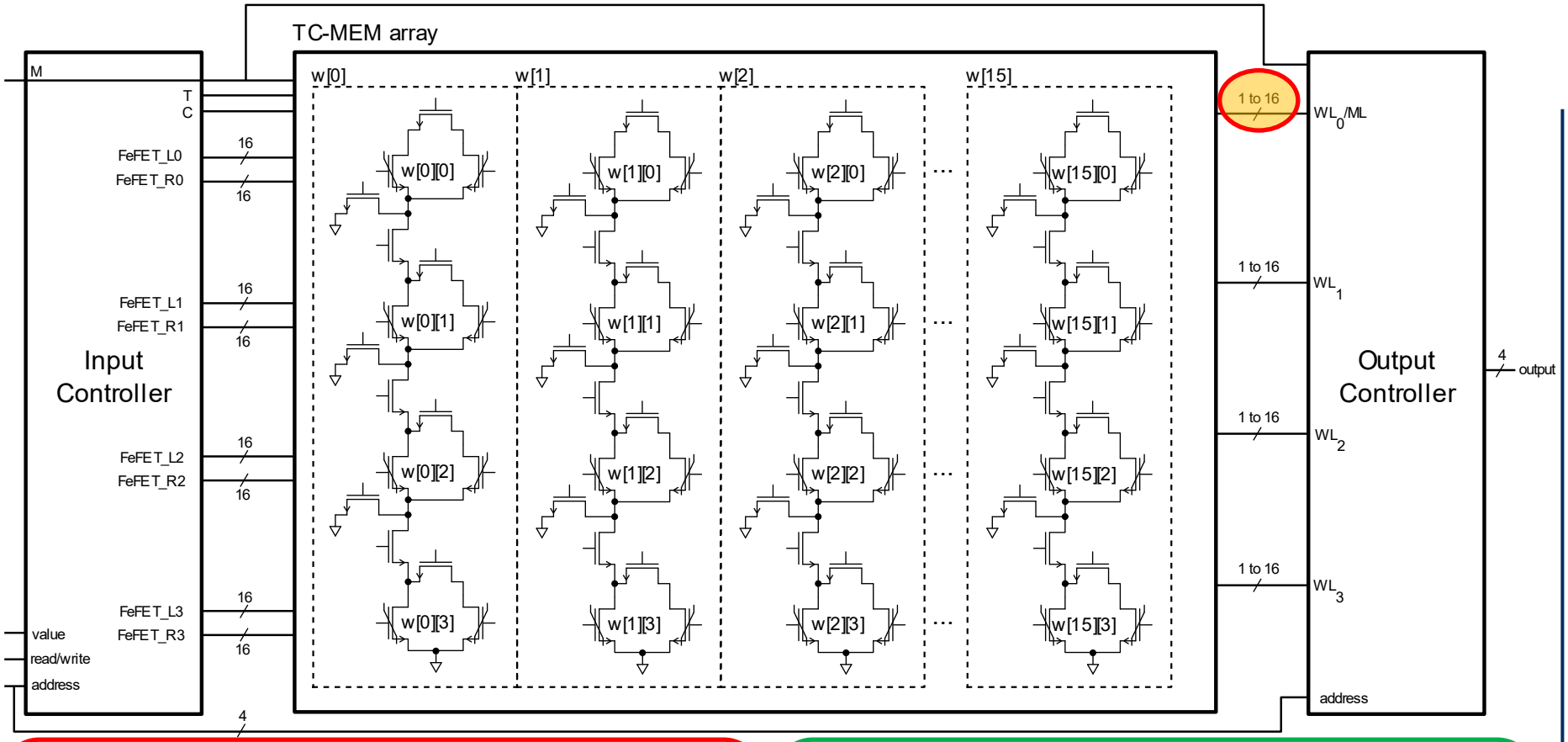
Memory Mode

Circuit	HW 0	HW 1	HW 2	HW dependency	Order
2-bit separated	$2{,}70e^{-13}$	$1{,}13e^{-13}$	$2{,}89e^{-16}$	Yes	3
2-bit parallel	$2{,}71e^{-13}$	$1{,}17e^{-13}$	$2{,}91e^{-14}$	Yes	1
2-bit serial	$3{,}63e^{-13}$	$2{,}22e^{-13}$	$9{,}59e^{-14}$	Yes	<1

TCAM Mode

Circuit	No match	Partial Match WL1	Partial Match WL0	Full Match	Dependency
2-bit separated	$4{,}04e^{-16}$	$1{,}05e^{-13}$	$9{,}67e^{-14}$	$2{,}59e^{-13}$	+ (<1)
2-bit parallel	$2{,}68e^{-13}$	$2{,}53e^{-13}$	$2{,}40e^{-13}$	$4{,}69e^{-16}$	++ (3)
2-bit serial	$8{,}11e^{-16}$	$7{,}69e^{-14}$	$1{,}55e^{-13}$	$1{,}55e^{-13}$	-

TC-MEM array (4-bit Sbox implementation)



Sbox implementation 1:

- Store $sbox(x)$ in $w[x]$ for $x \in \{0;15\}$
  - Encryption → Memory
  - Decryption → TCAM

Sbox implementation 2:

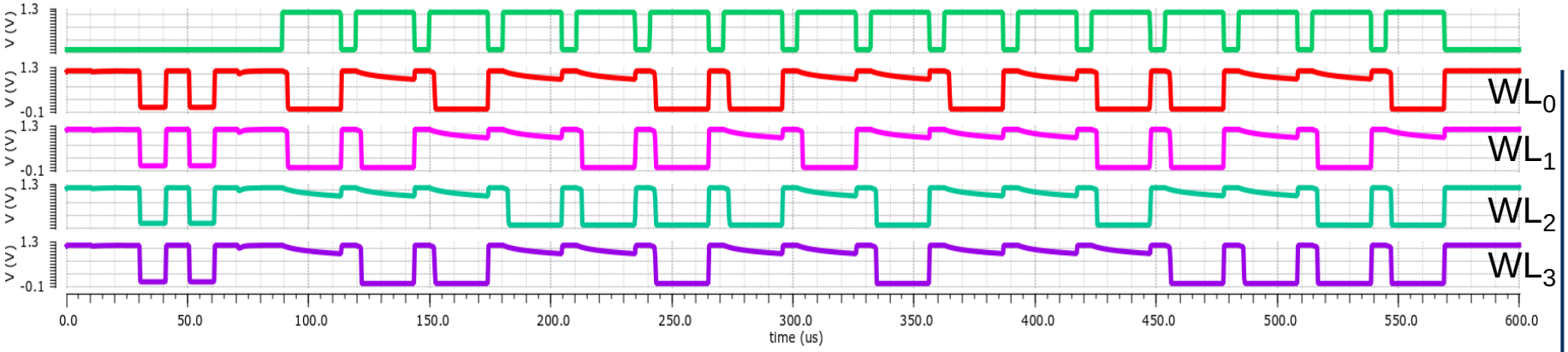
- Store x in $w[sbox(x)]$ for $x \in \{0;15\}$
  - Encryption → TCAM
  - Decryption → Memory

Shared vs separated match line

Match line	Shared (1)	Separated (n)
Search time	1 address per clock cycle	1 clock cycle
Implementation constraint	RNG (security purpose) + counter, time constant ?	-
Input Controller area	Medium	small
Output Controller area	Small	high
Energy consumption	Variable to constant	High but constant

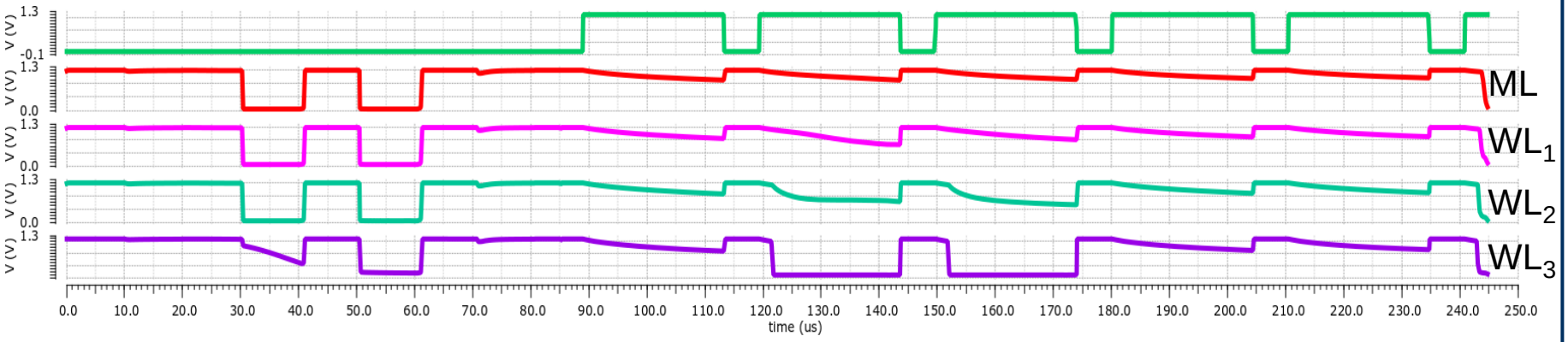
Photon-Beetle Sbox

Memory mode ($Sbox$)



address	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Read value	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

TCAM mode ($Sbox^{-1}$) : Shared ML, search value = 0



Agenda

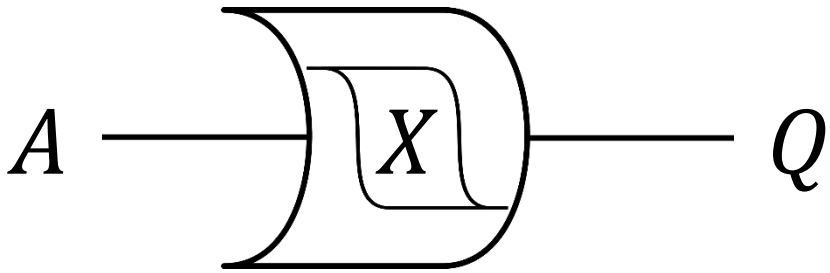
1. Introduction
2. Ferroelectric field effect transistor
3. TC-MEM memory and Sbox implementation
4. Non-volatile logic gates and operators for security
5. Conclusion

Hardware desing

- We define a non-volatile logic gate with one input A and one output Y;
- This gate perform a logical function symbolised with the operator $\circ\ (\cdot, +, \oplus)$;
- It contains a preprogrammed value X include in $GF(2) = \{0,1\}$ and perform the following operation :

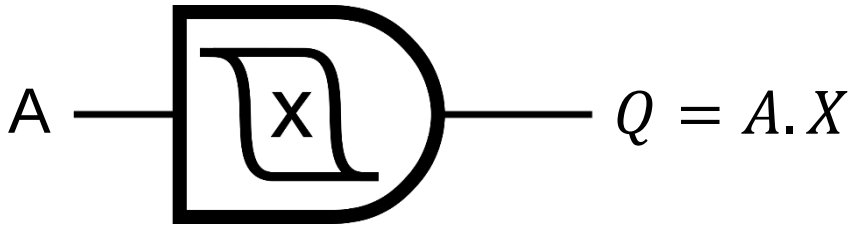
$$Q = A \circ X\ ;$$

- Its symbol is :

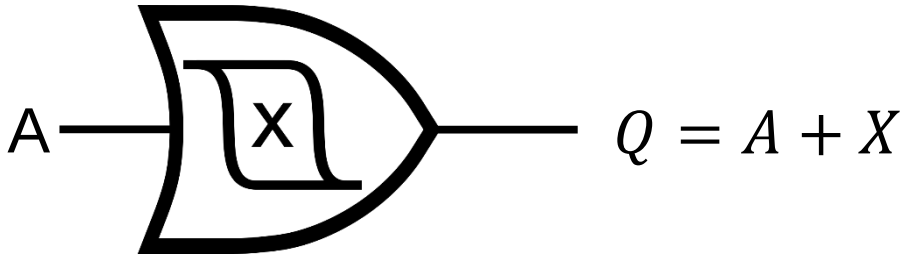


Hardware desing

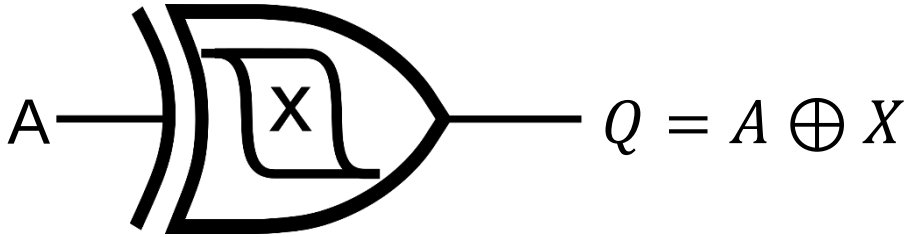
- AND gate :



- OR gate :



- XOR gate :



Non-volatile GF(2^4) adder

- Adding in GF(2^m) corresponds to a bit XORing

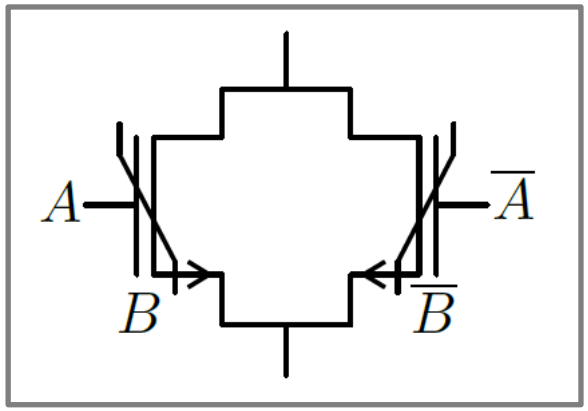


Fig. 2 : Porte XOR en FeFET[1]

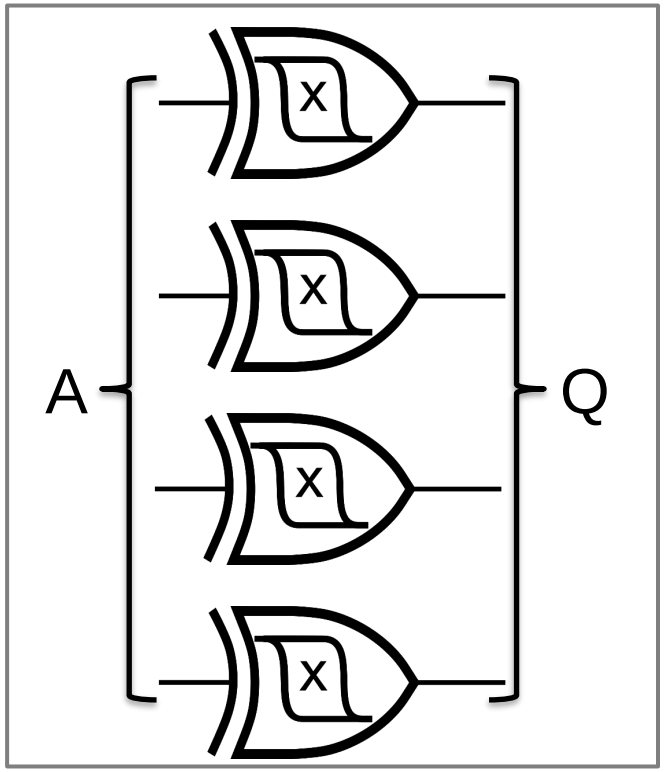


Fig. 3 : Non-volatile adder.

[1]C. Marchand, I. O'Connor, M. Cantan, E. T. Breyery, S. Slesazecky and T. Mikolajick, "FeFET based Logic-in-Memory: an overview", DTIS 2021.

GF(2^4) multiplier

- Two architectures possible:
  - Combinatory (need more component)
  - Sequencial (with a complexity depending of the size-bit; O(n)

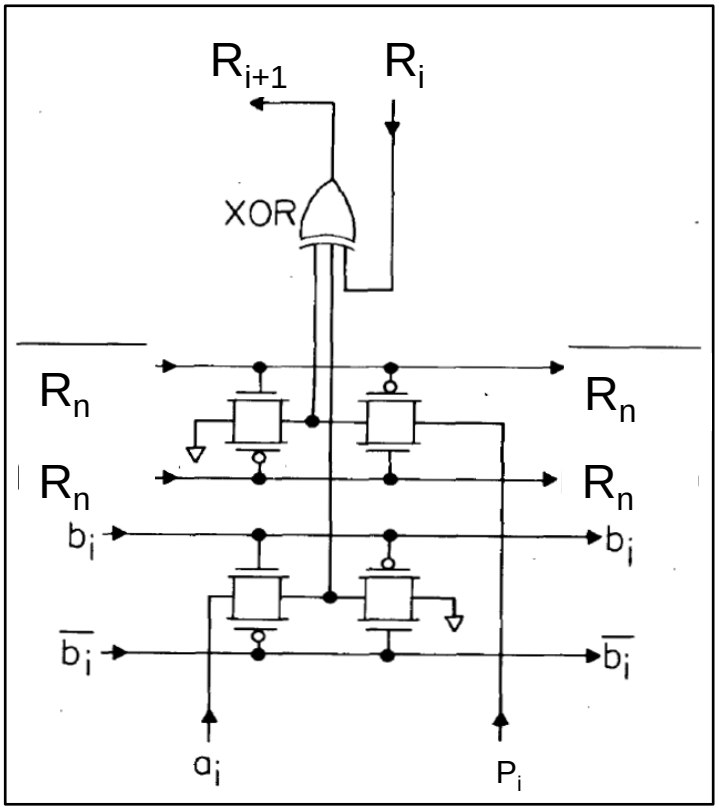


Fig. 4 : 1-bit Galois field multiplier[1].

[1]P. A. Scott, S. E. Tavares, L. E. Peppard, “A Fast VLSI Multiplier for GF(2^m)”, *IEEE Journal on Selected Areas in Communications*, Vol. 4, Issue 1, January 1986.

Non-Volatile GF(2^4) multiplier

- Store irreductible polynomial
- Store one constante ?

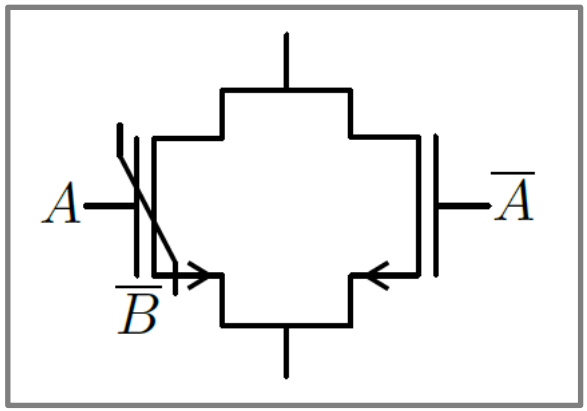


Fig. 5 : Porte AND en FeFET

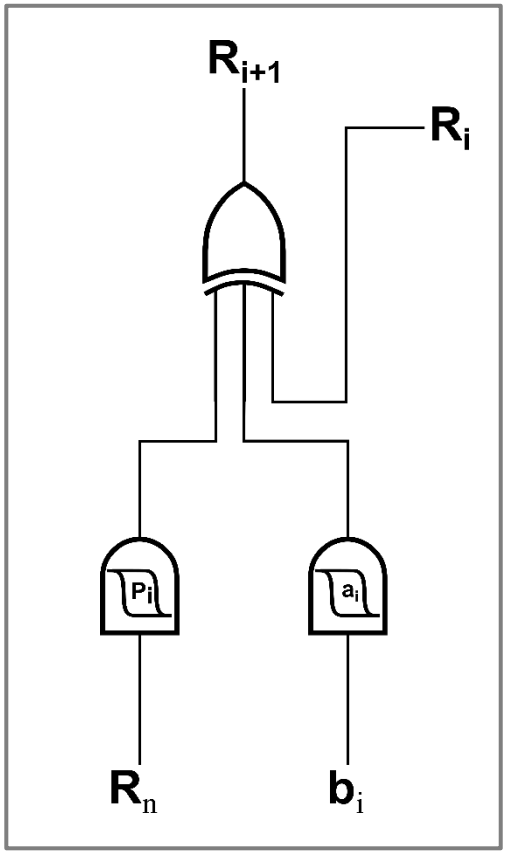


Fig. 6 : 1-bit Galois field multiplier

Non-Volatile GF(2^4) multiplier

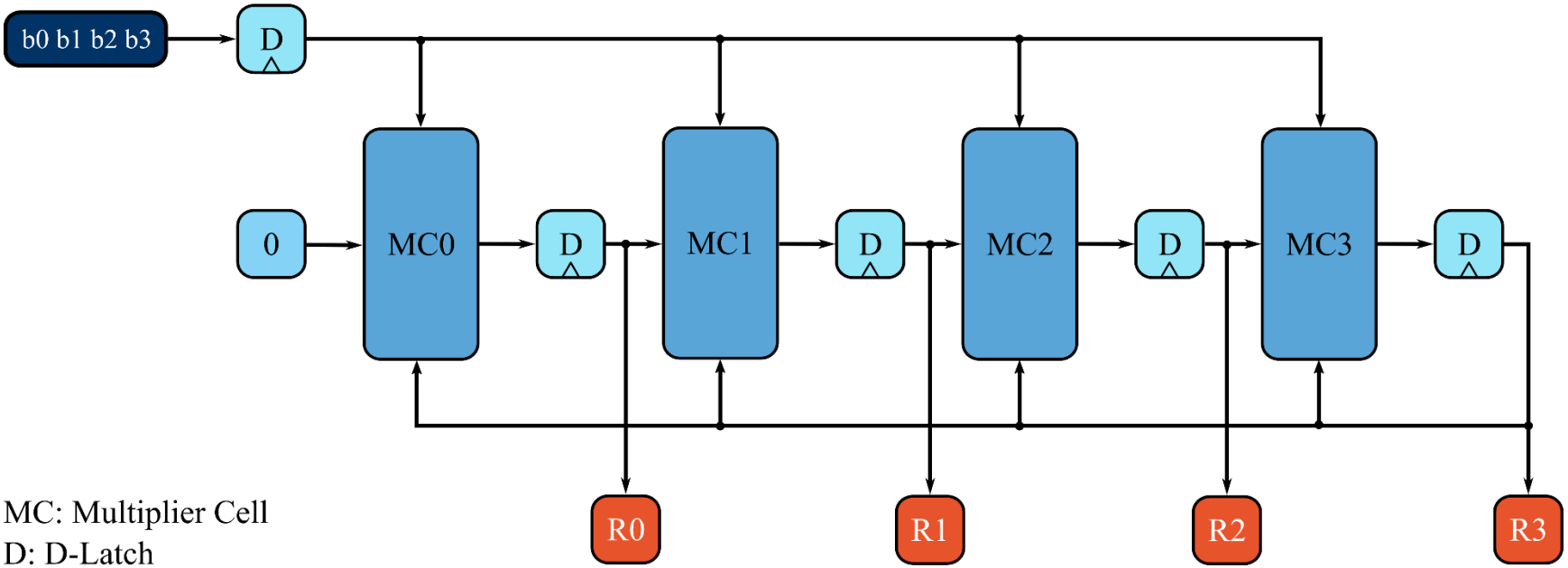


Fig. 7 : Non-volatile 4-bits Multiplier architecture.

Conclusion

The TC-MEM:

1. New memory circuit accessible by address and by content
2. Can be used to implement cryptographic Sbox with high area and energy efficiency

3. Serial implementation seems to be more interesting for security

Non-volatile logic gates :

1. Can be used to implement specific operation storing constants :
    1. Adder
    2. Multiplier, …

Future works :

1. Implement all these operations in a RISC-V environment
2. Design an ASIC to validate and evaluate the operators
3. …

Thank you for your attention

This work has been carried out using the framework of the SECRET project supported by the French “Agence Nationale de la Recherche” under project number ANR-20-CE39-0006.