Institut des Nanotechnologies de Lyon UMR 5270

In-Memory implementation of SBoxes using Ferroelectric transistors

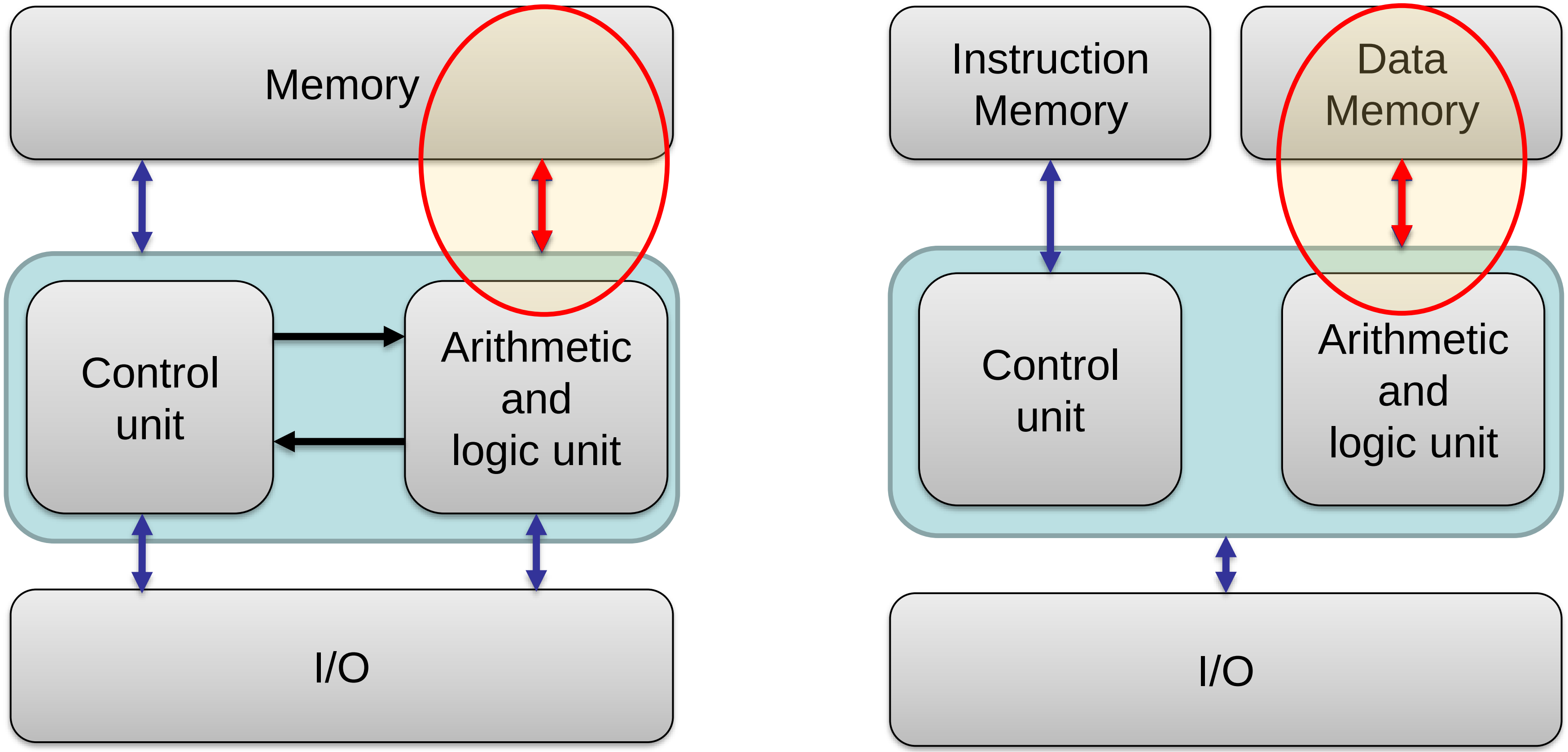
Cédric Marchand, Ian O'Connor, Stefan Slesazeck, Thomas Mikolajick

Cryptarchi 2022

Agenda

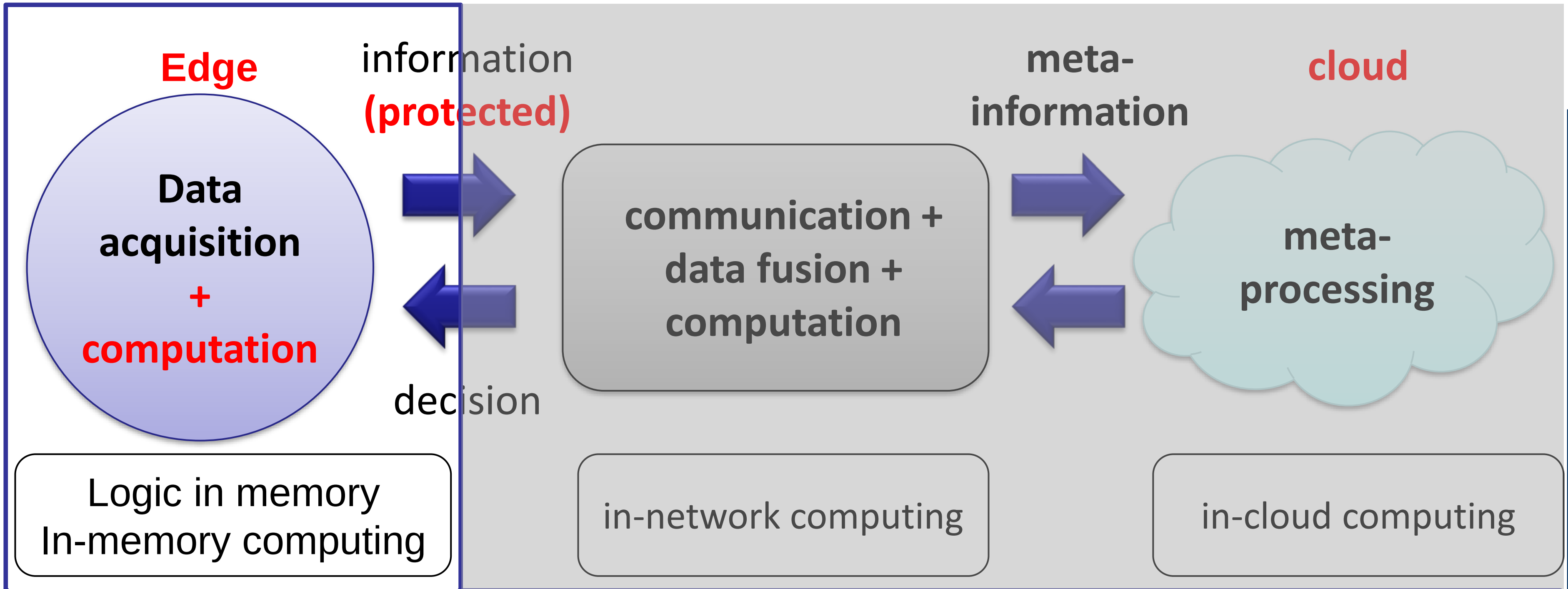
Context (Classical computing architectures)

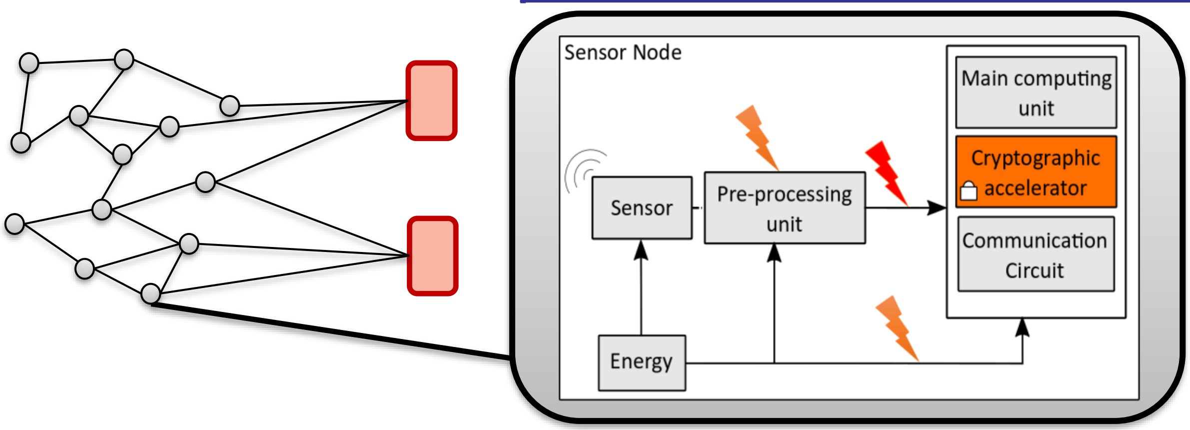
- Von Neumann Architecture/ Harvard Architecture
  - Data transfert congestion



Limit performances and energy efficiency

Sensor node security



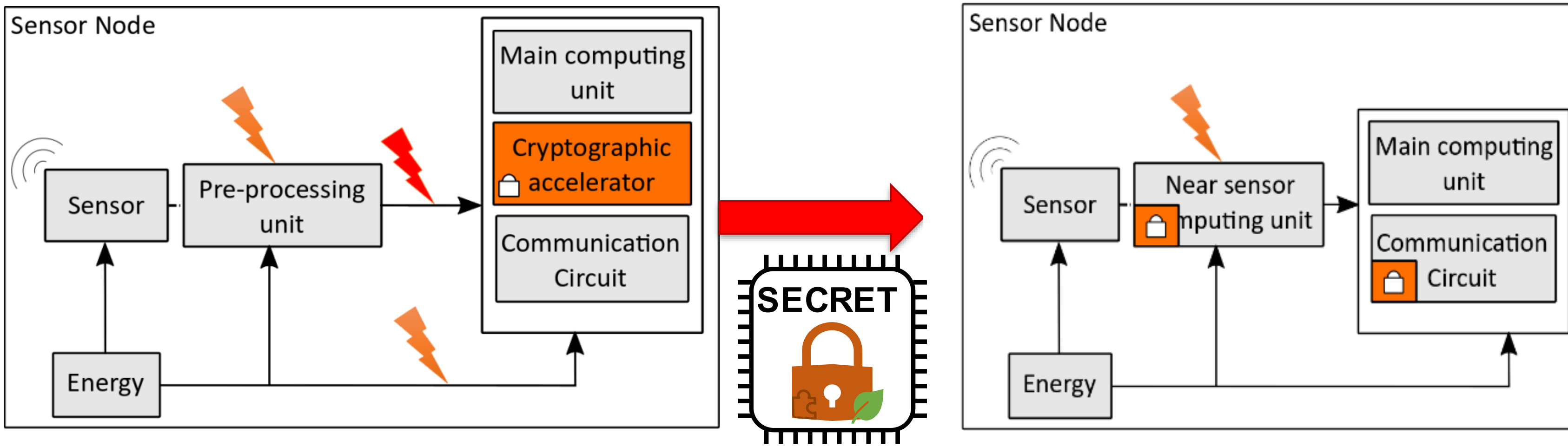


Need for a Secure and Highly energy efficient Computing platform

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

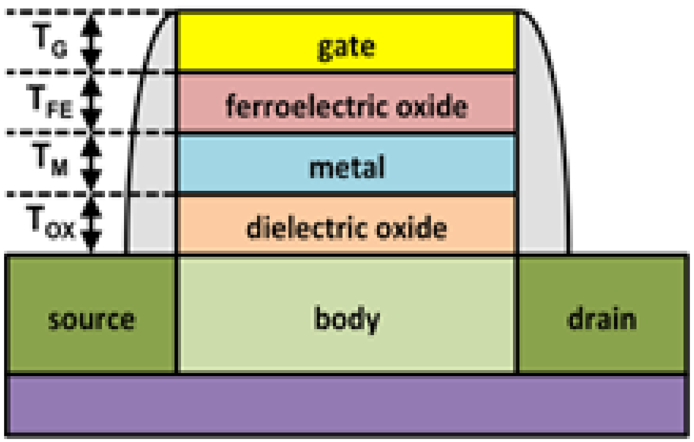


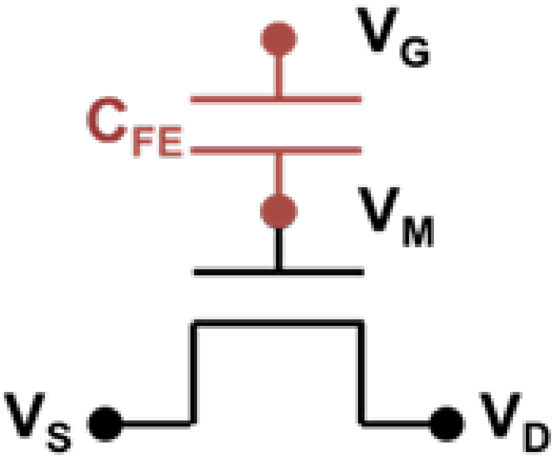
- Add a low-cost security layer in the preprocessing Unit :
  - Use emerging technologies (FeFet for example) to implement part of cryptographic operations inside the preprocessing Unit (Sbox, constant matrix multiplication, …)

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

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

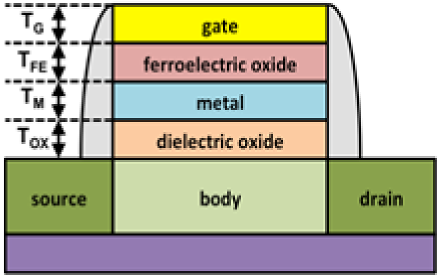
Ferroelectric Field Effect Transistor

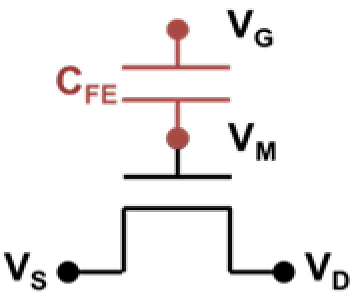


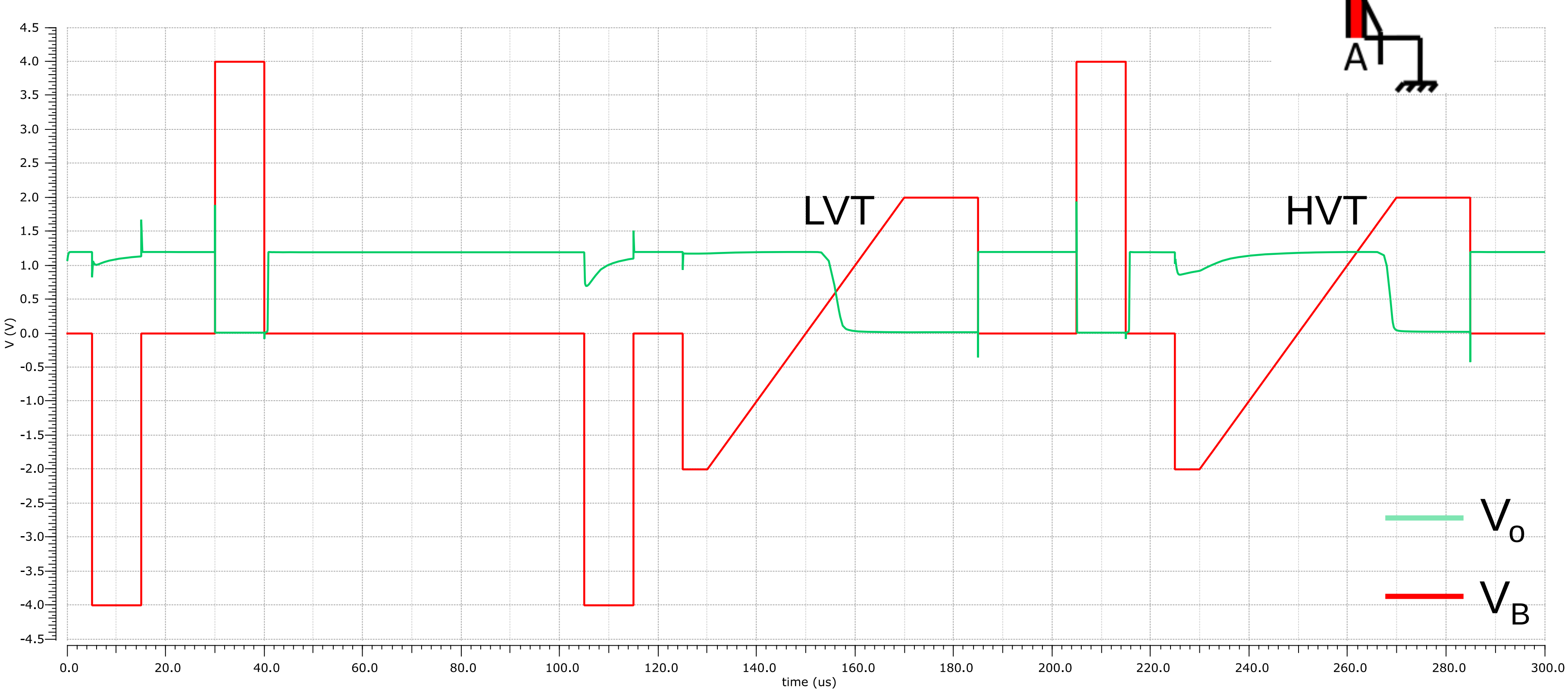


FeFET : single transistor characteristics

FeFET dimension:
W = 500 nm
L = 500 nm

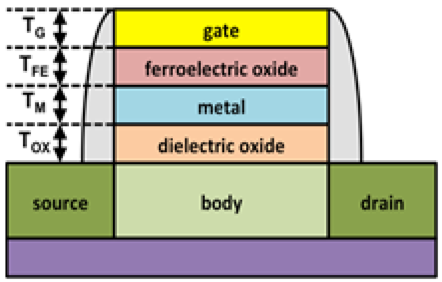


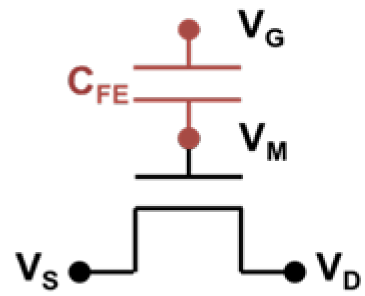


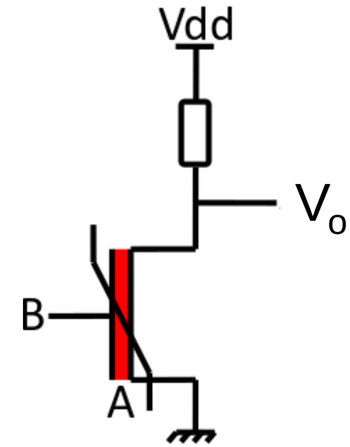


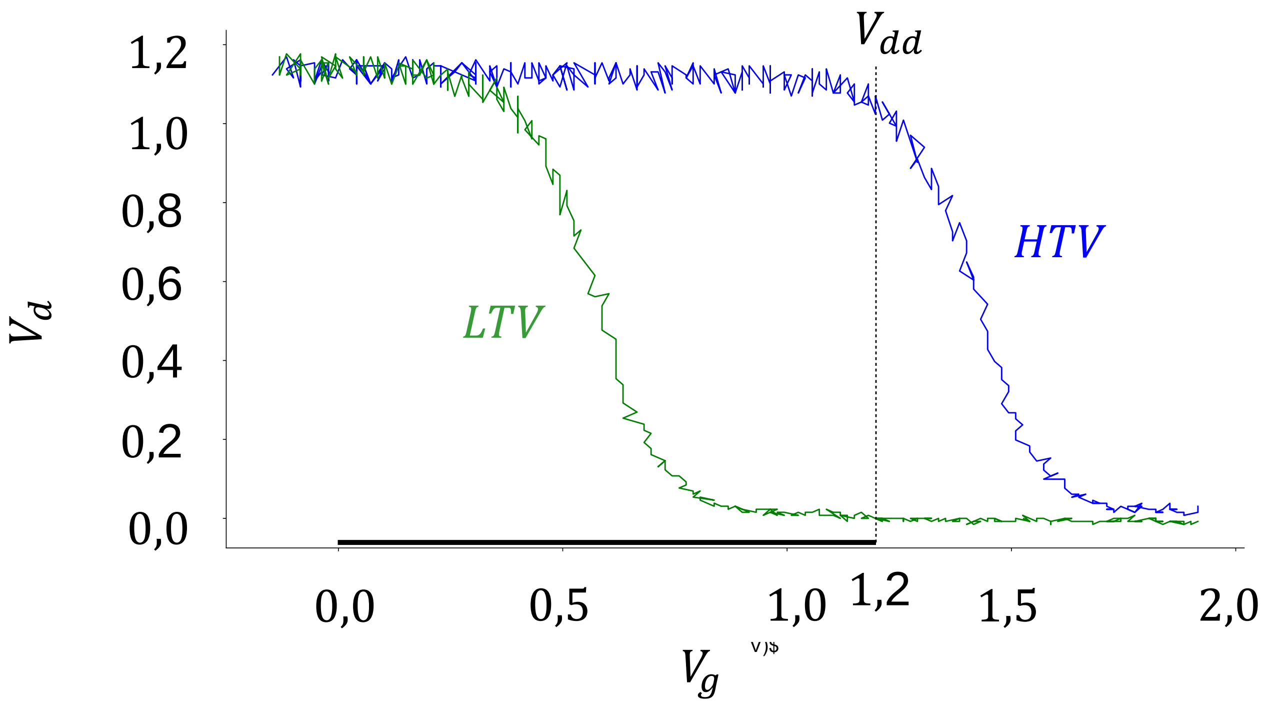
FeFET : single transistor characteristics

FeFET dimension:
W = 500 nm
L = 500 nm



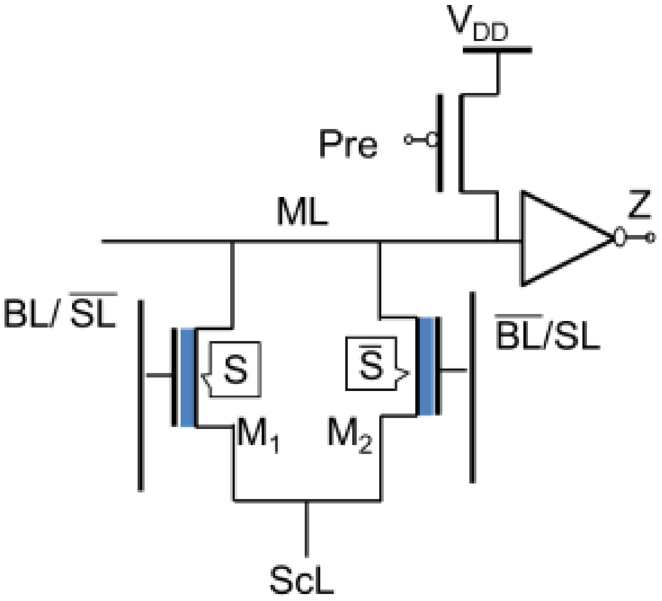




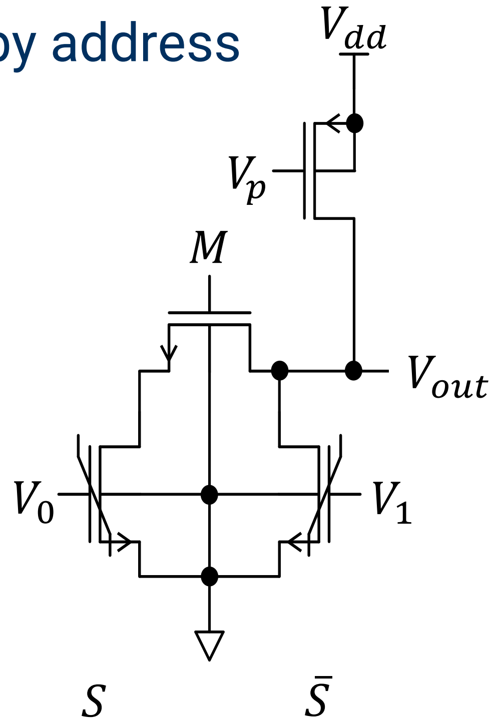


TC-MEM

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



TCAM[1]



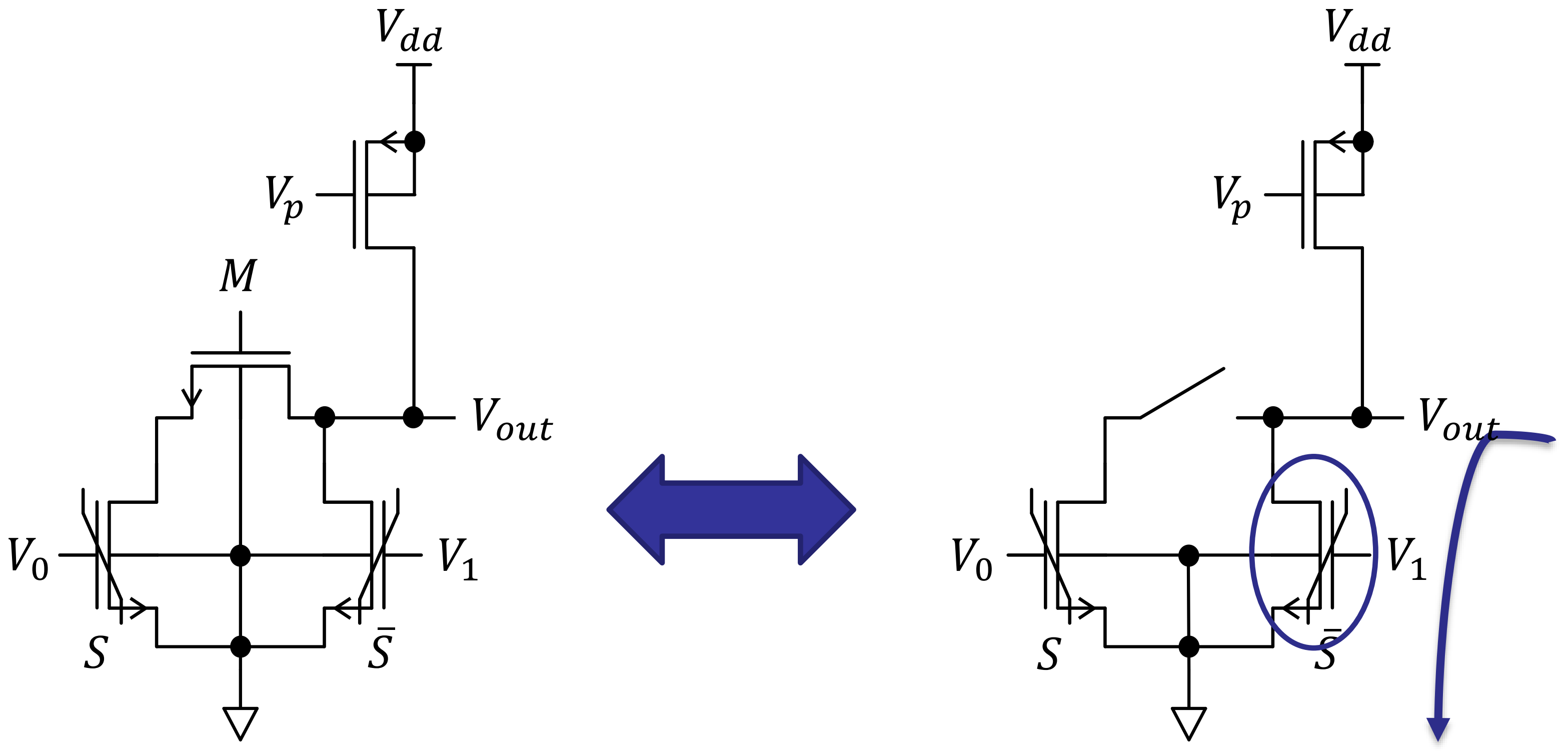
TC-MEM[2]

[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

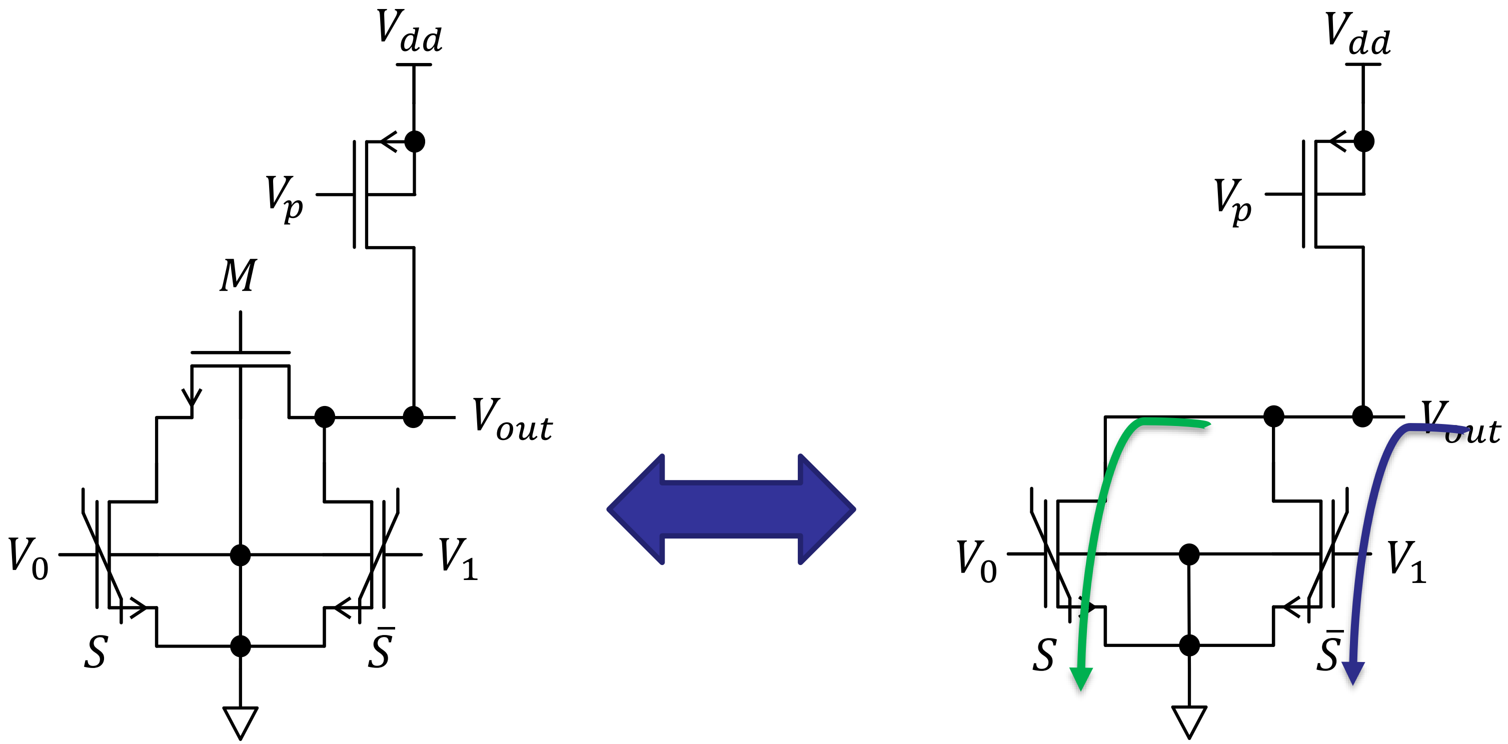


$$V_o = \overline{V_1 . \bar{S}}$$

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

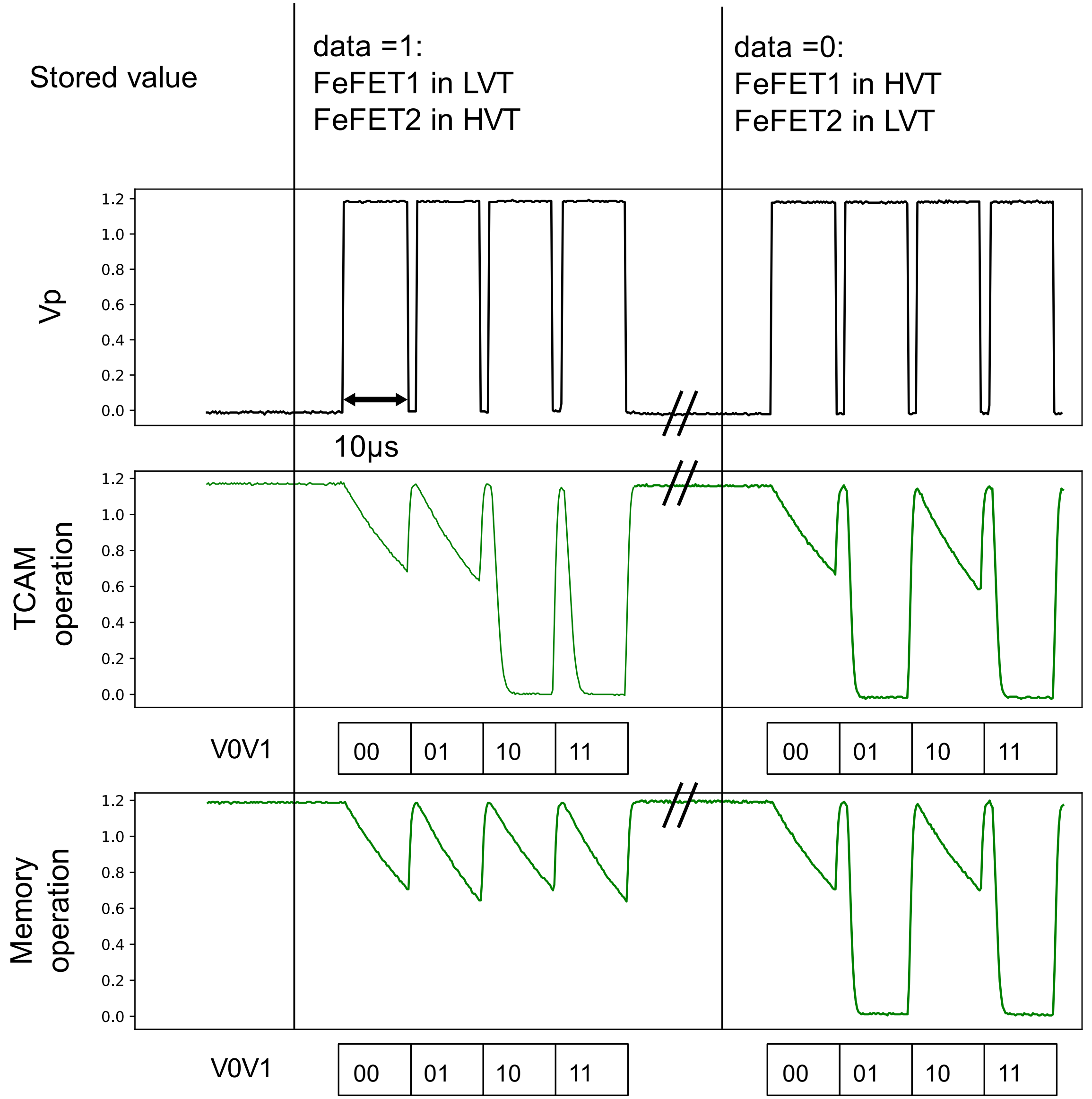
TC-MEM

- $M = 1$: TCAM mode

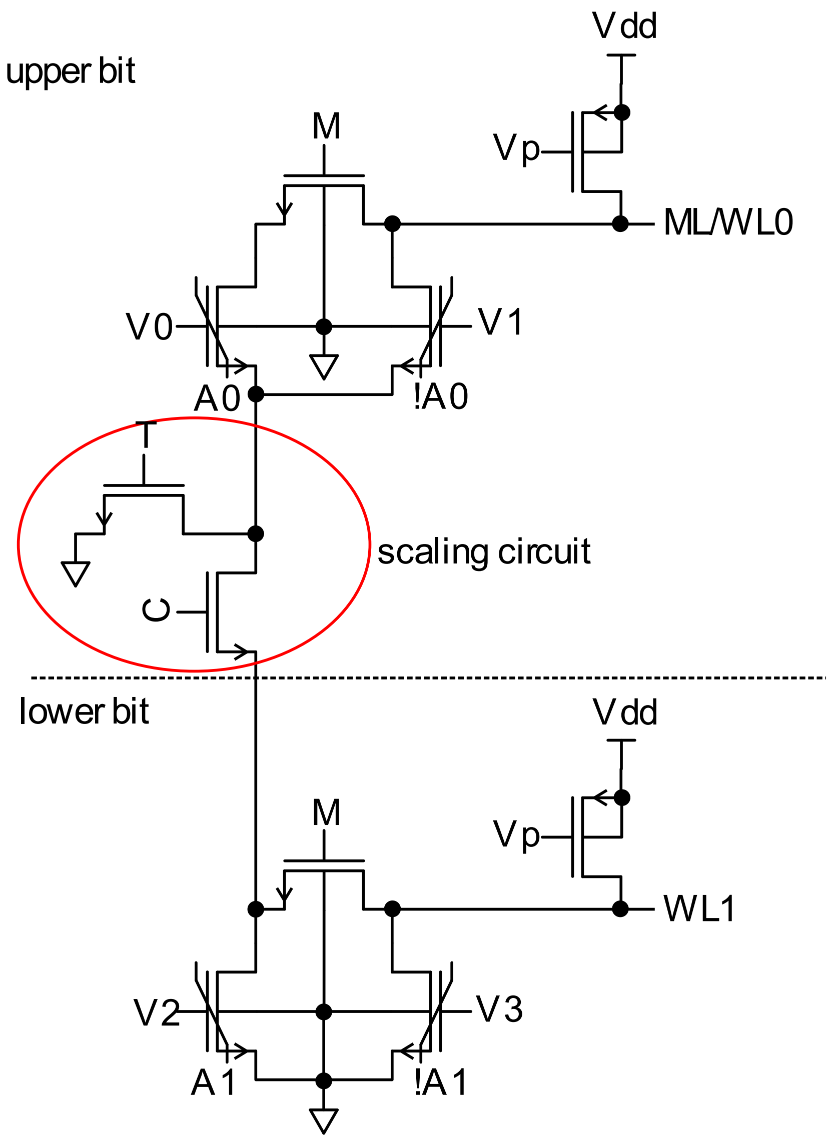


$$V_{out} = \overline{V_0 . S} . \overline{V_1 . \bar{S}}$$

TC-MEM (chip measurement)



TC-MEM 2-bit, 4-bit, …

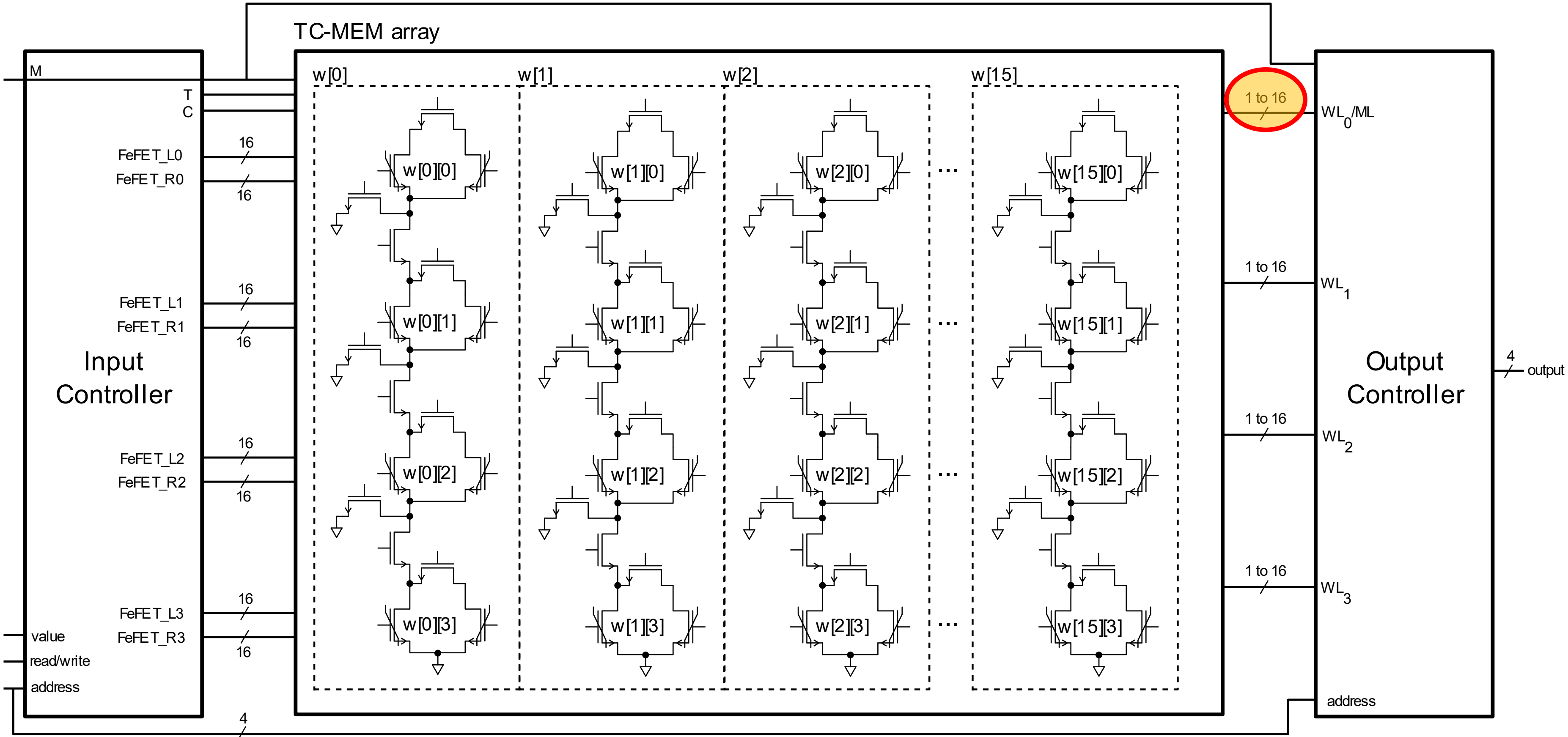


2-bit TC-MEM

PROs:
- Partial word search
- In-Memory-computing
- Easy to scale

CONs:
- Half memory is loosed in Memory mode
- Resistive path between match line and ground increase with the word size

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

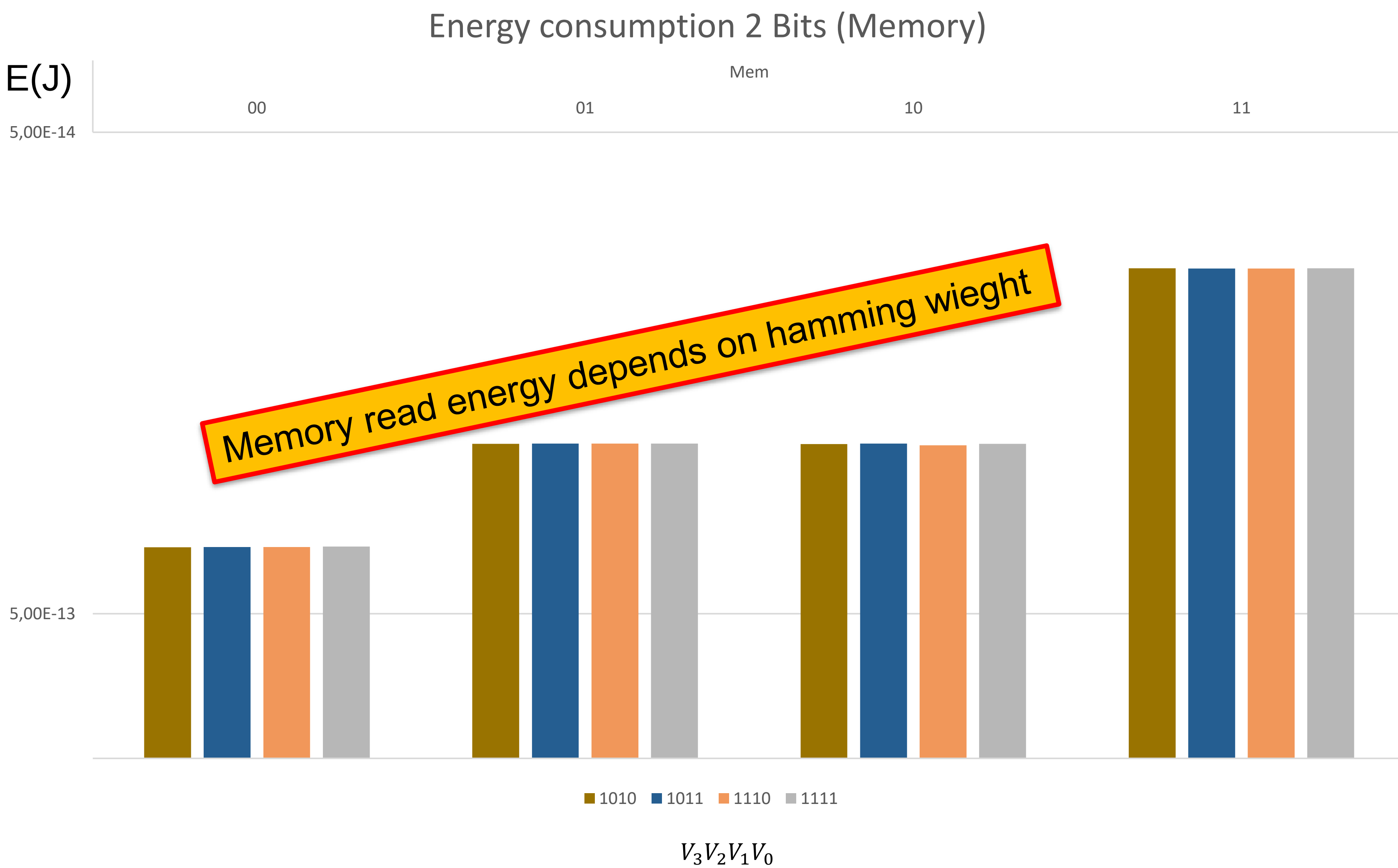
Sbox implementation 2:

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

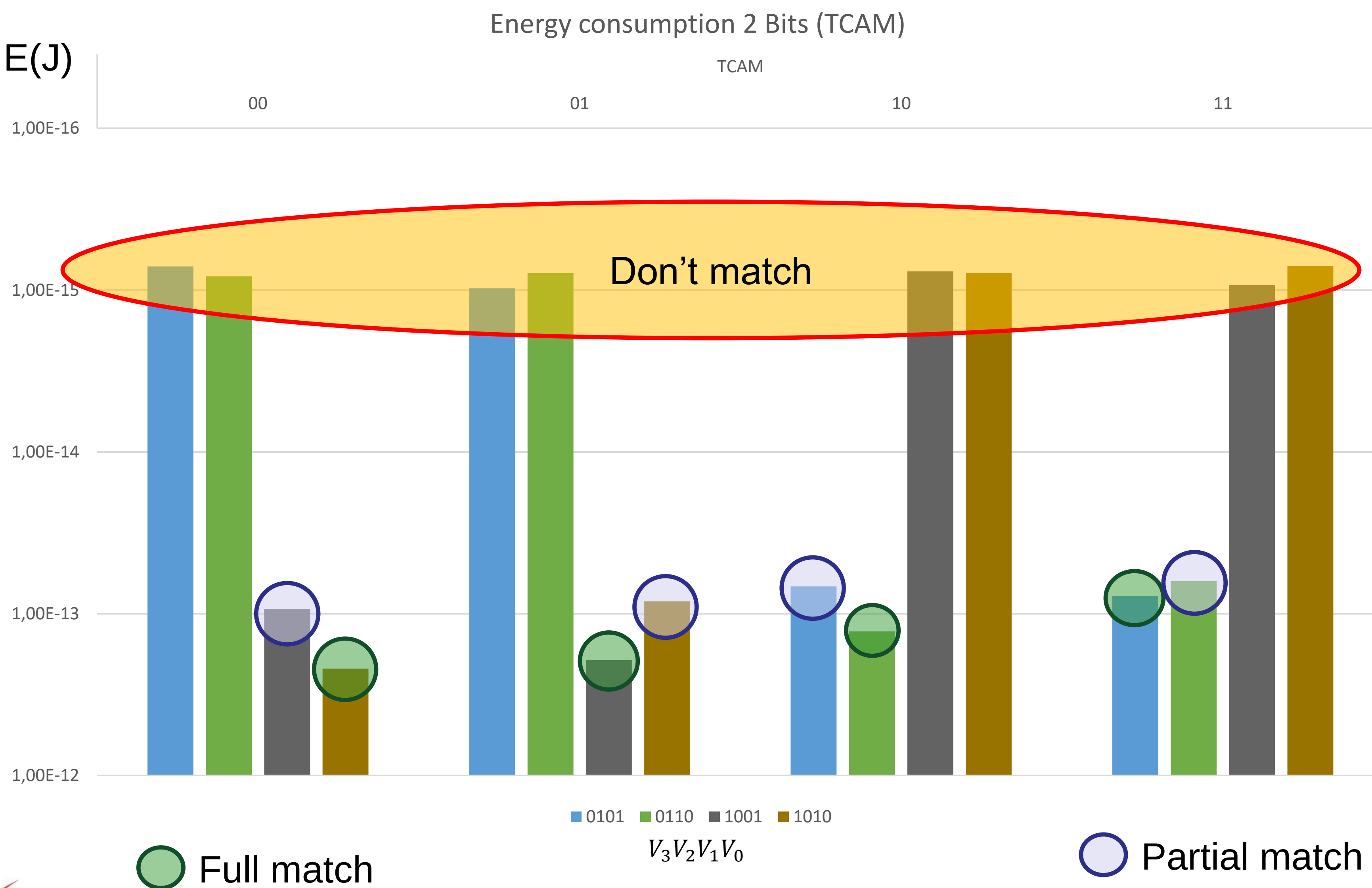
Shared vs separated match line

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 area Controller	Medium	small
Output area Controller	Small	high
Energy consumption	Variable to constant	High but constant

Energy consumption and side channel attacks

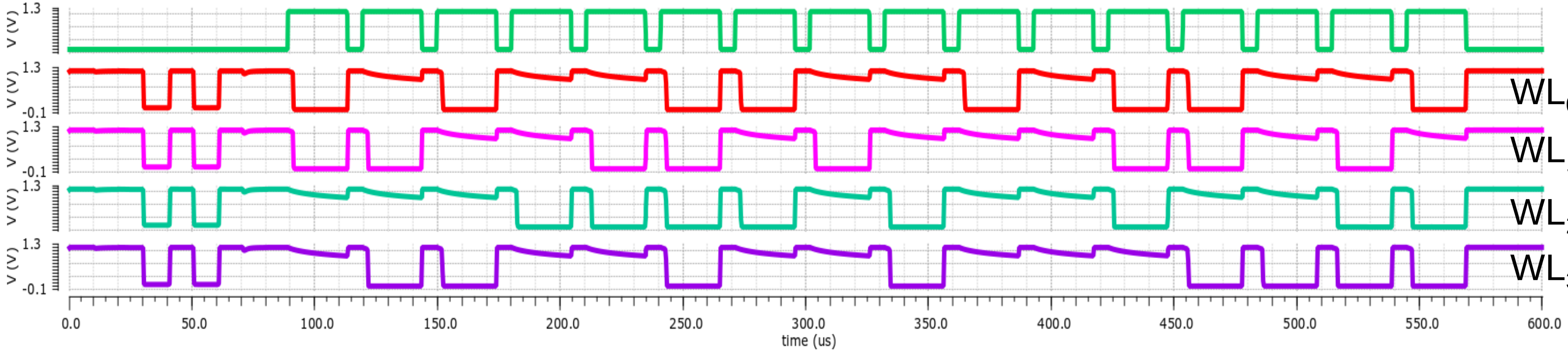


Energy consumption and side channel attacks



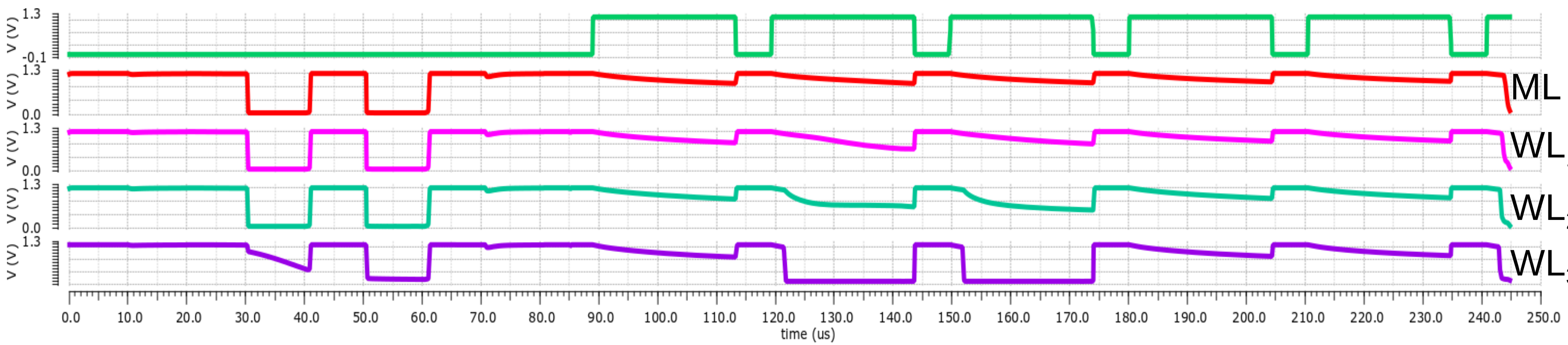
Photon-Beetle Sbox

Memory mode ($Sbox$)

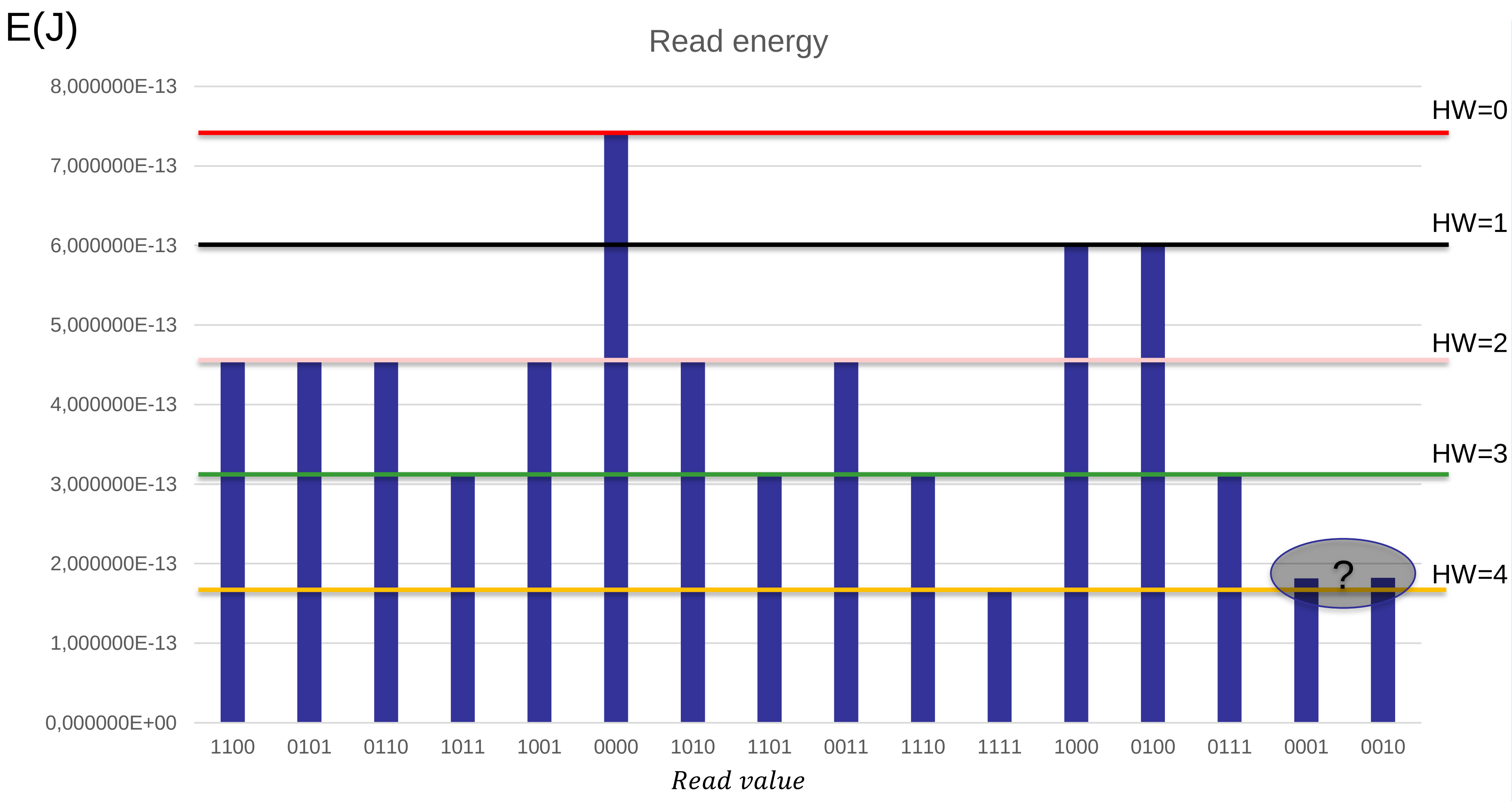


address	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Read value	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

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



Photon-Beetle Sbox - Memory mode



Conclusion

The TC-MEM:

1. New memory circuit accessible by address and by content
2. Easily scalable
3. Low transistor overhead compared to other TCAM memories

4. Can be used to implement cryptographic Sbox with high area and energy efficiency

However

- Half of the memory is lost in memory mode
- The read energy shows a dependency with the value which is read or searched → side channel attack may be possible

Future works

With TC-MEM:

- Complete Input and output controller implementation
- Manufacture a new test chip with TC-MEM array input/output controller if possible

With FeFET

- Implement gallois field operations with FeFET :
  - Scalar multiplication, Matrix Multiplication, addition, …
- codesign a full cryptographic algorithm implementation using FeFET (where constant can be found) and standard processing

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.