Institut des Nanotechnologies de Lyon UMR 5270

FeFET based Logic-in-Memory design methodologies, tools and open challenges

Cédric Marchand, Alban Nicolas, Paul-Antoine Matrangolo, David Navarro, Alberto Bosio, Ian O'Connor

Agenda

1. Introduction
   a) The INL and our team
   b) Context

2. Exploring Logic-in-Memory based on FeFET
   a) FeFET technology and elementary logic gates
   b) Galois field operations
   c) TC-MEM and Sbox implementation

3. Platform and evaluation tool

4. Open challenge and future direction

Agenda

1. Introduction
   a) The INL and our team
   b) Context
2. Exploring Logic-in-Memory based on FeFET
   a) FeFET technology and elementary logic gates
   b) Galois field operations
   c) TC-MEM and Sbox implementation
3. Platform and evaluation tool
4. Open challenge and future direction

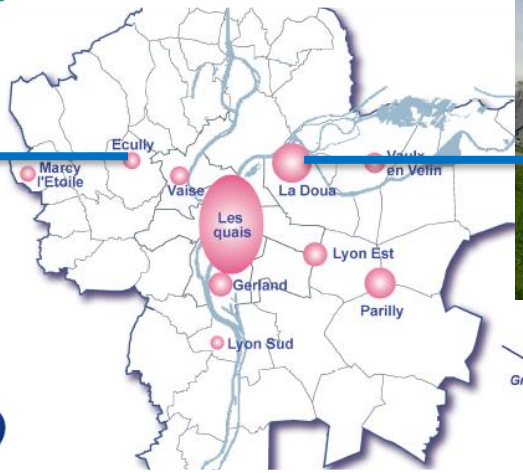
Lyon Institute of Nanotechnology

Joint Research Unit (CNRS, ECL, INSA Lyon, U. Lyon 1, CPE)
Materials – Photonics – Electronics – Biotechnologies
Applications in ICT, Energy, Health & Environment
250 people

Lyon West Campus

ÉCOLE CENTRALE LYON

cnrs



La Doua Campus

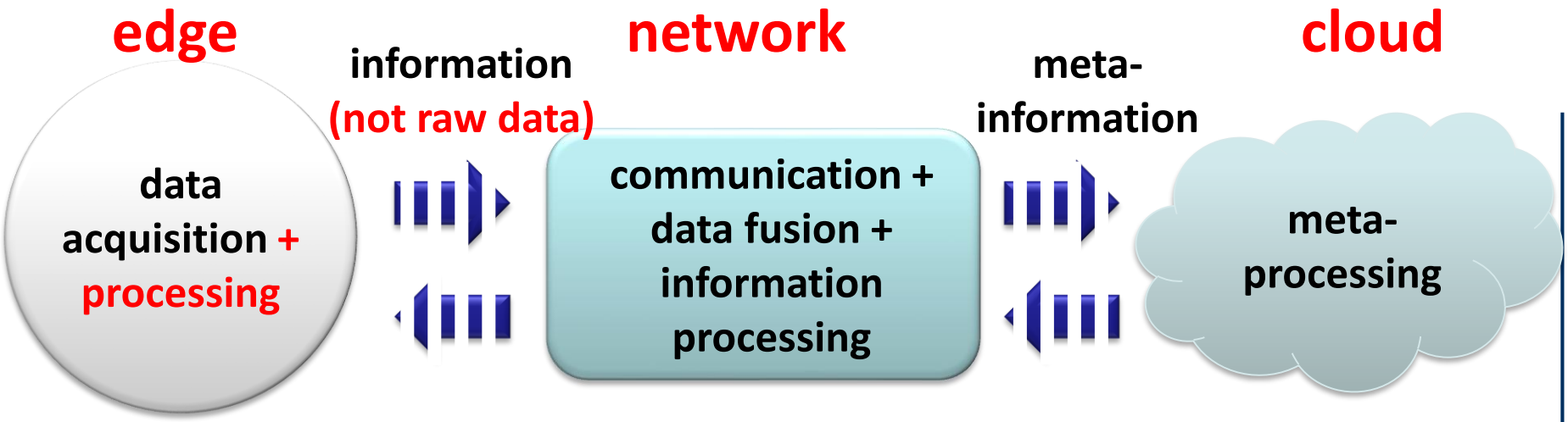
INSA

Lyon 1

CPE LYON

cnrs

Our aims



Application challenges

- Edge **sensing**: sensitivity, bandwidth
- **Computing** energy efficiency

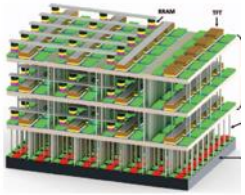
Cross-cutting challenges

- Security
- Hardware reliability

Approaches

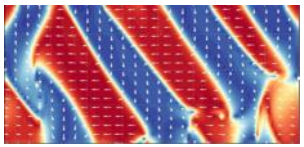
CMOS diversification	Emerging technologies	Emerging paradigms
SPAD, photodetectors, MEMS/NEMS	Transistors and memory, silicon photonics, ...	Embedded AI, stochastic / approximate computing, …

Our knowhow



System and circuit design

- Heterogeneous systems
- Design methodologies
- Analog/digital design



Simulation & Modeling

- Compact modeling
- Simulation (TCAD, FEM…)
- Numerical modeling

Multiphysics multi-scale modeling

- Interface analysis (RX)
- AFM measurements
- Constrained electrical characterization

Micro/Nanofabrication

- Devices
- Test structures
- Thin films

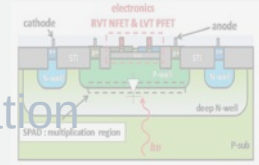
Research tracks

Electronics Team

SENSORS

Sensors & Instrumentation

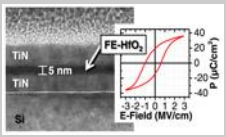
- SPAD, Image sensors
- Detectors & instrumentation
- MEMS / NEMS



EMERGING RESEARCH DEVICES

Ferro. devices (FerroTeam)

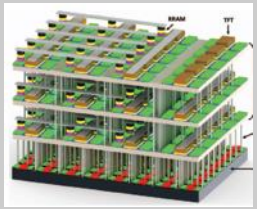
- Thin film analysis
- Device integration
- Emerging Memory devices



DESIGN: EMERGING TECHNOLOGIES, EMERGING PARADIGMS

Reliable Ultra energy-efficient Secure compuTing (RUST)

- New computing paradigms
- Hardware security, reliability
- Design methodologies



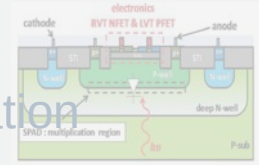
Research tracks

Electronics Team

SENSORS

Sensors & Instrumentation

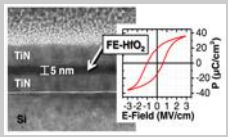
- SPAD, Image sensors
- Detectors & instrumentation
- MEMS / NEMS



EMERGING RESEARCH DEVICES

Ferro. devices (FerroTeam)

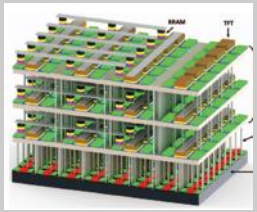
- Thin film analysis
- Device integration
- Emerging Memory devices



DESIGN: EMERGING TECHNOLOGIES, EMERGING PARADIGMS

Reliable Ultra energy-efficient Secure compuTing (RUST)

- New computing paradigms
- Hardware security, reliability
- Design methodologies



Agenda

1. Introduction
   a) The INL and our team
   b) Context

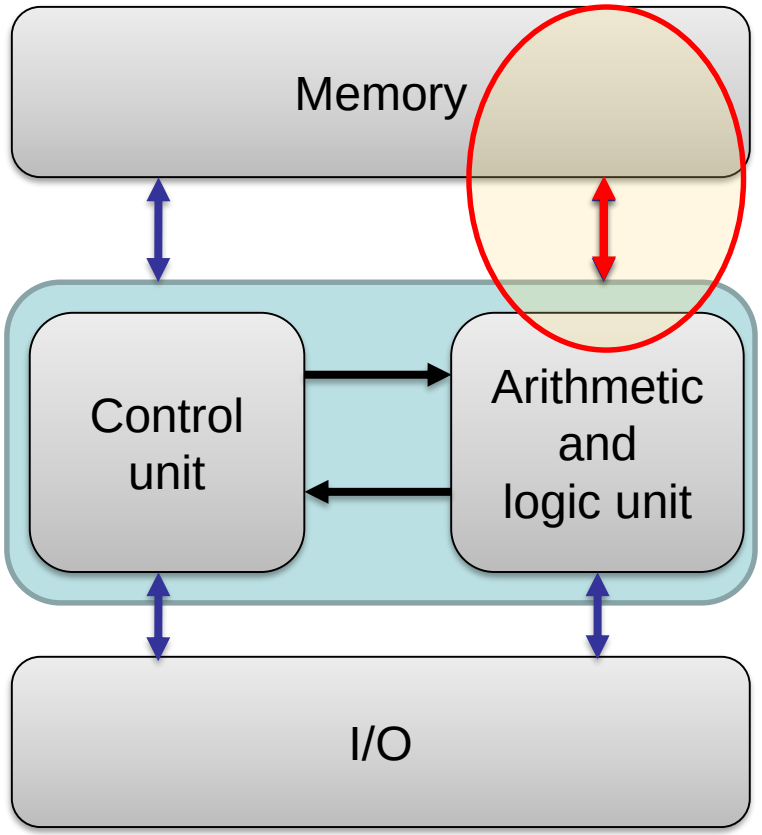
2. Exploring Logic-in-Memory based on FeFET
   a) FeFET technology and elementary logic gates
   b) Galois field operations
   c) TC-MEM and Sbox implementation

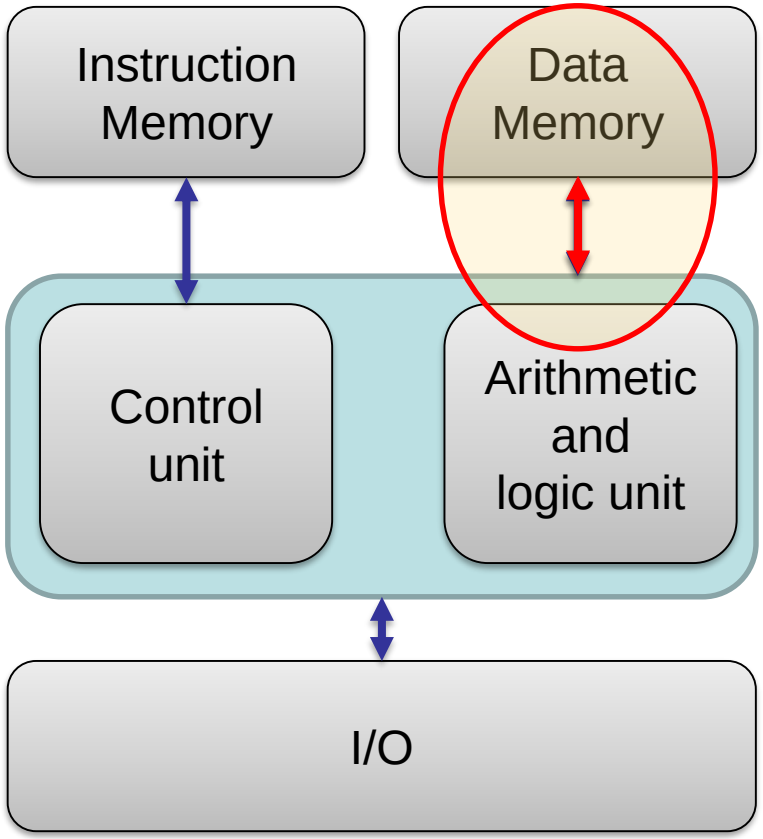
3. Platform and evaluation tool

4. Open challenge and future direction

Context (Classical computing architectures)

- Von Neumann Architecture/ Harvard Architecture
  - Data transfert congestion





Limit performances and energy efficiency

Data driven application and IoT

Edge

Data acquisition + computation

information (protected)

decision

communication + data fusion + computation

meta-information

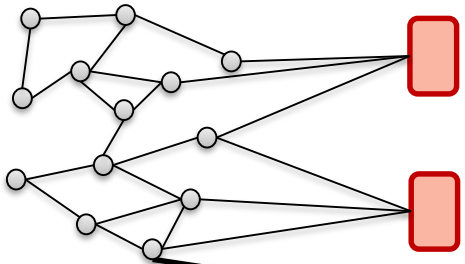
cloud

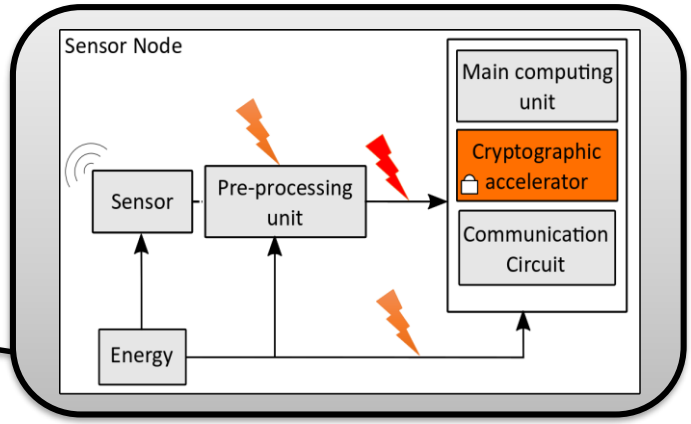
meta-processing

Logic in memory
In-memory computing

in-network computing

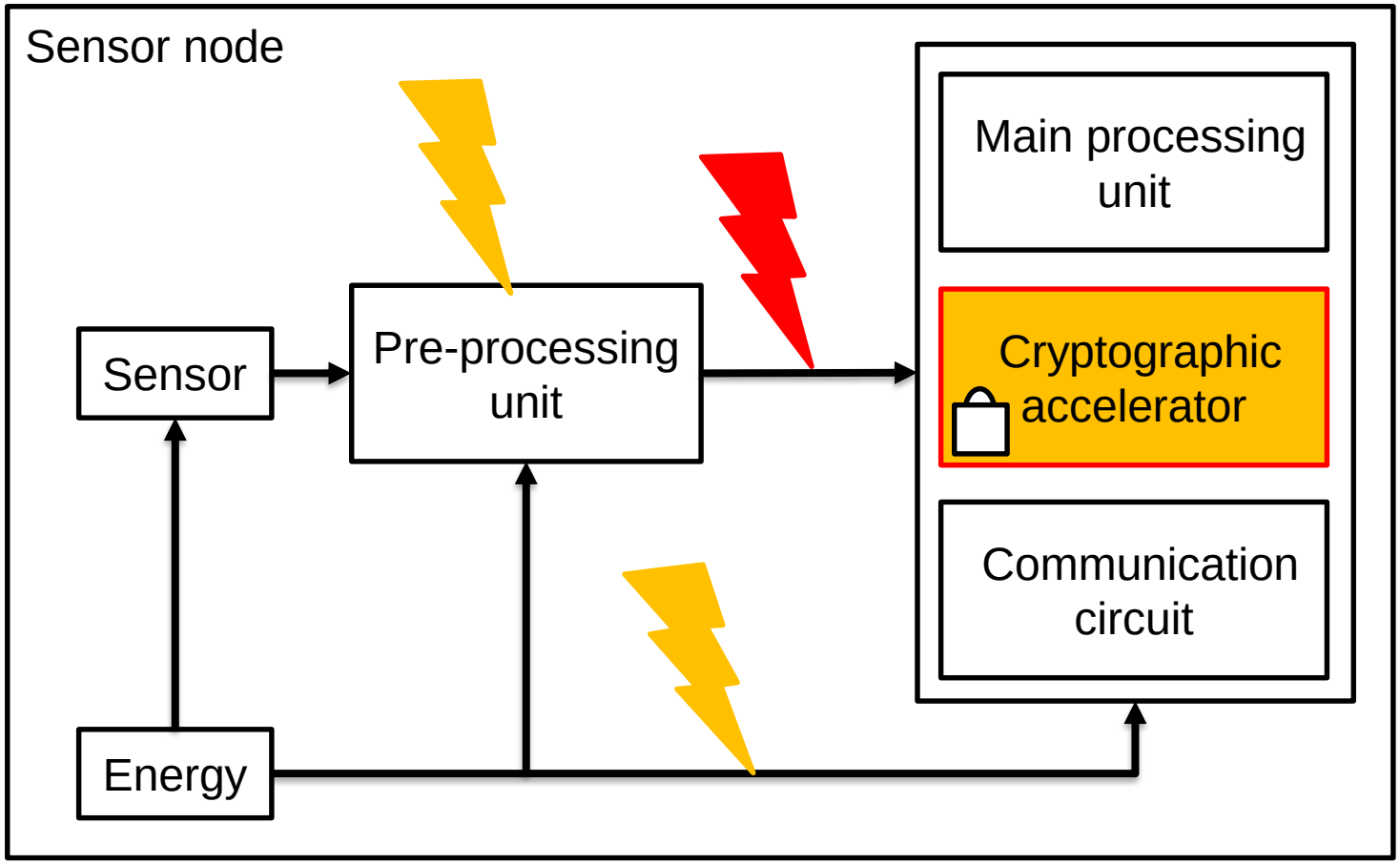
in-cloud computing



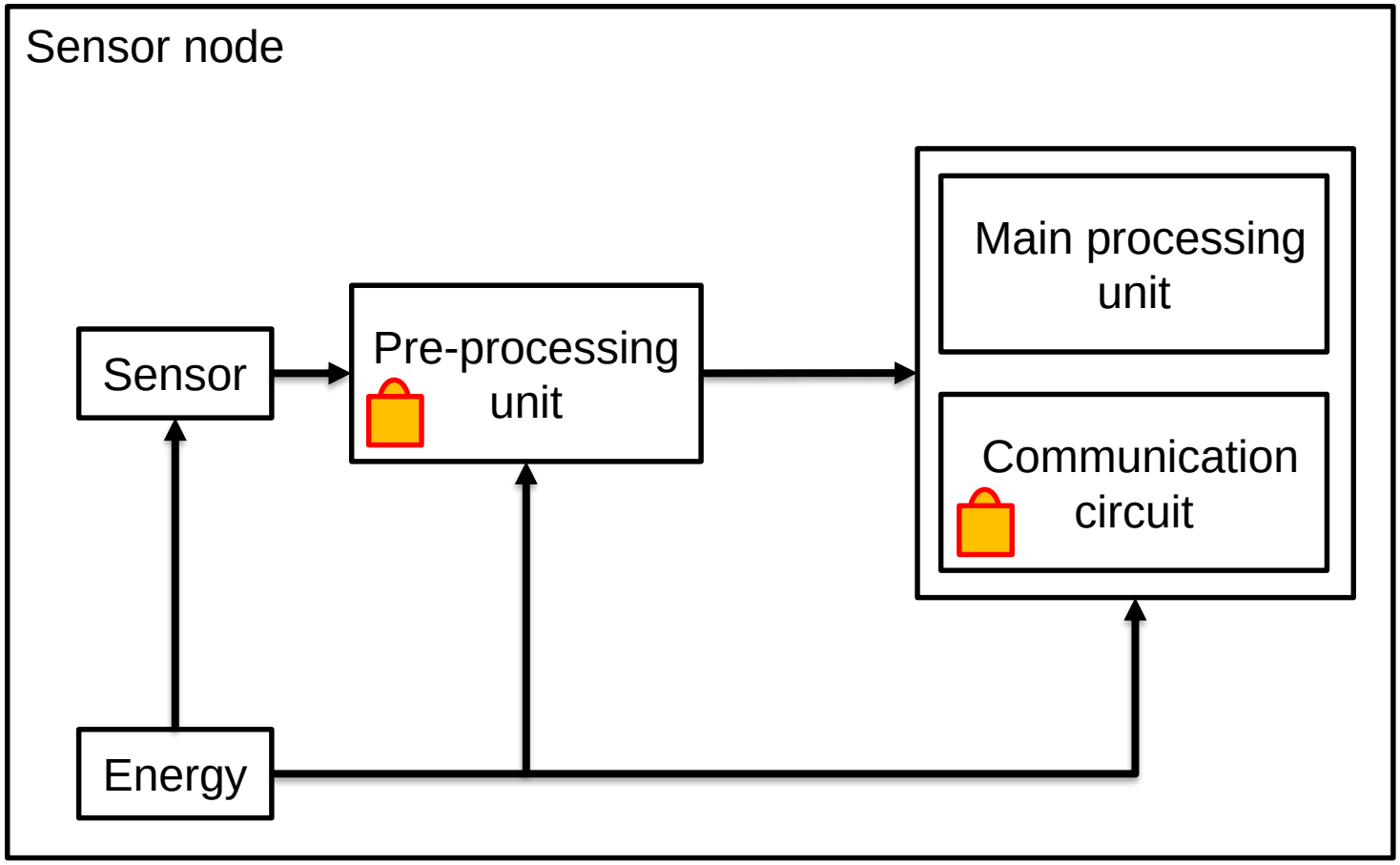


Need for a Secure and Highly energy efficient Computing platform

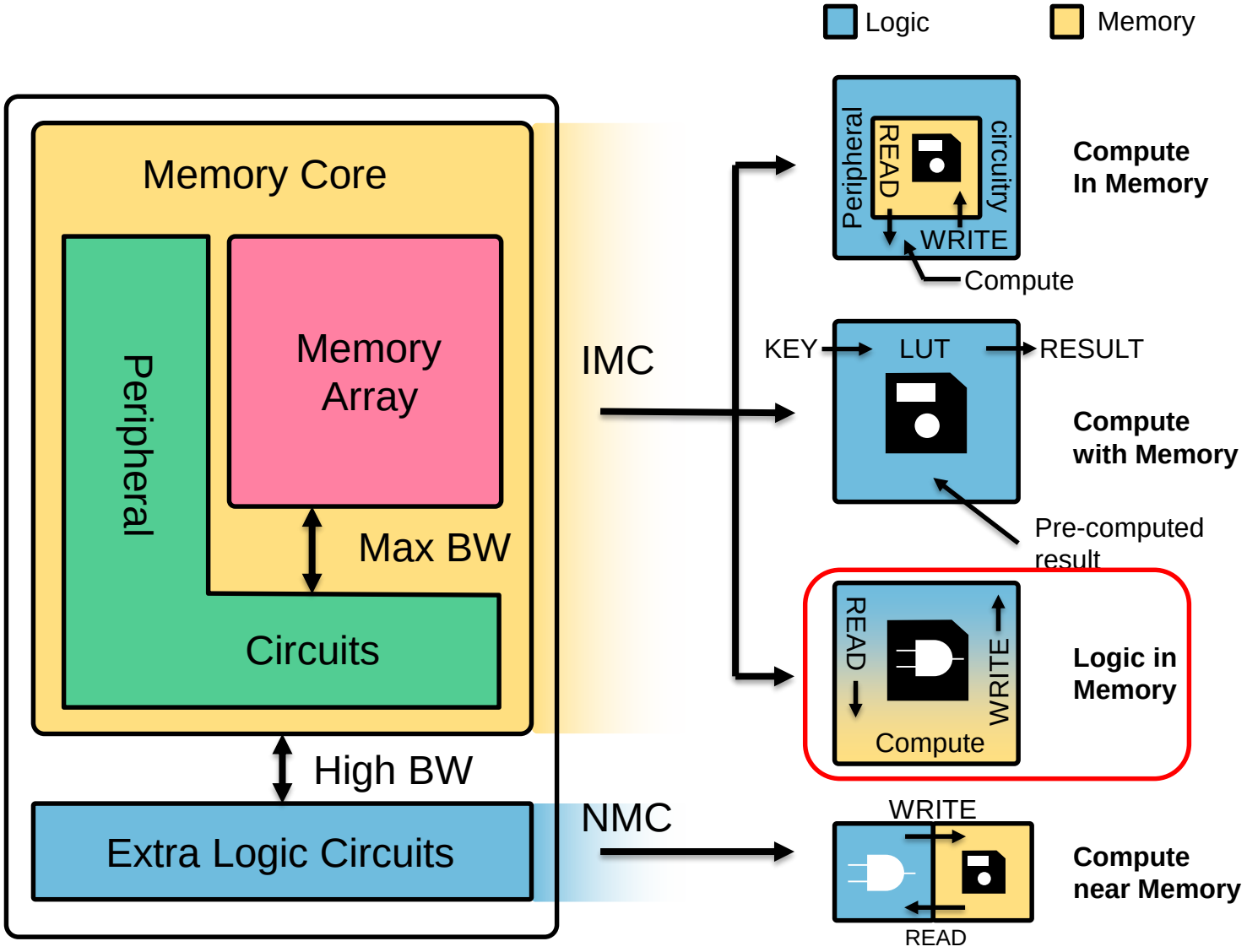
SECRET project



SECRET project



In Memory Computing solution



Agenda

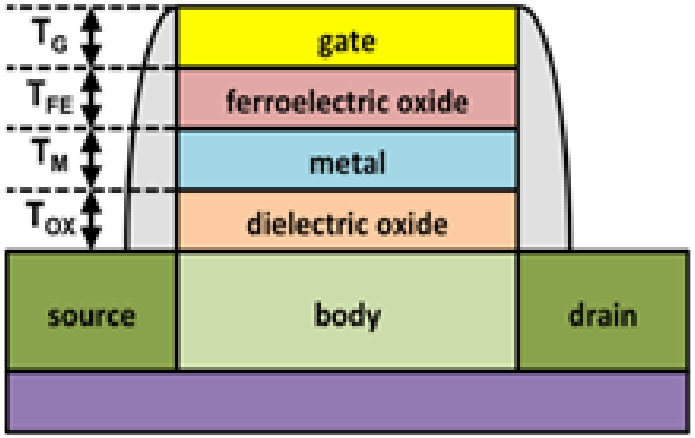
1. Introduction
   a) The INL and our team
   b) Context

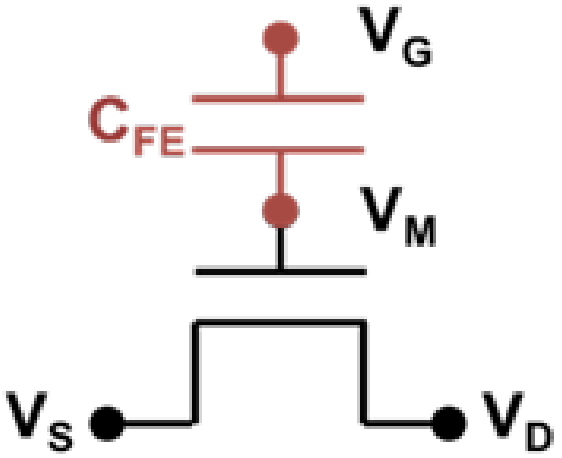
2. Exploring Logic-in-Memory based on FeFET
   a) FeFET technology and elementary logic gates
   b) Galois field operations
   c) TC-MEM and Sbox implementation

3. Platform and evaluation tool

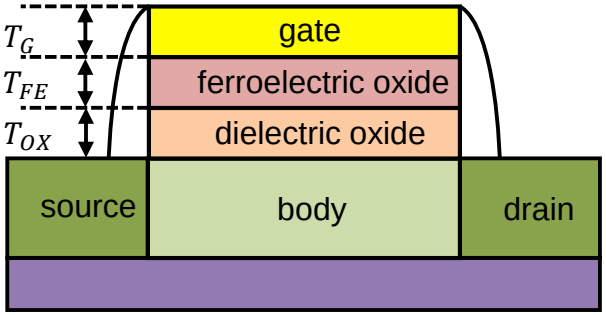
4. Open challenge and future direction

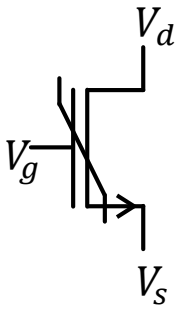
Ferroelectric Field Effect Transistor

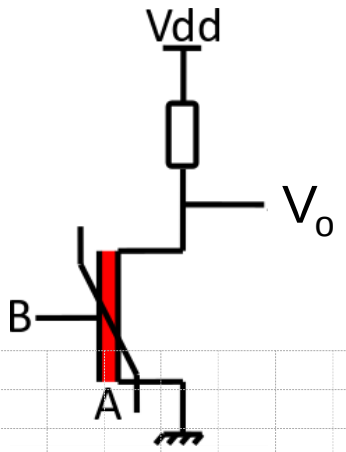


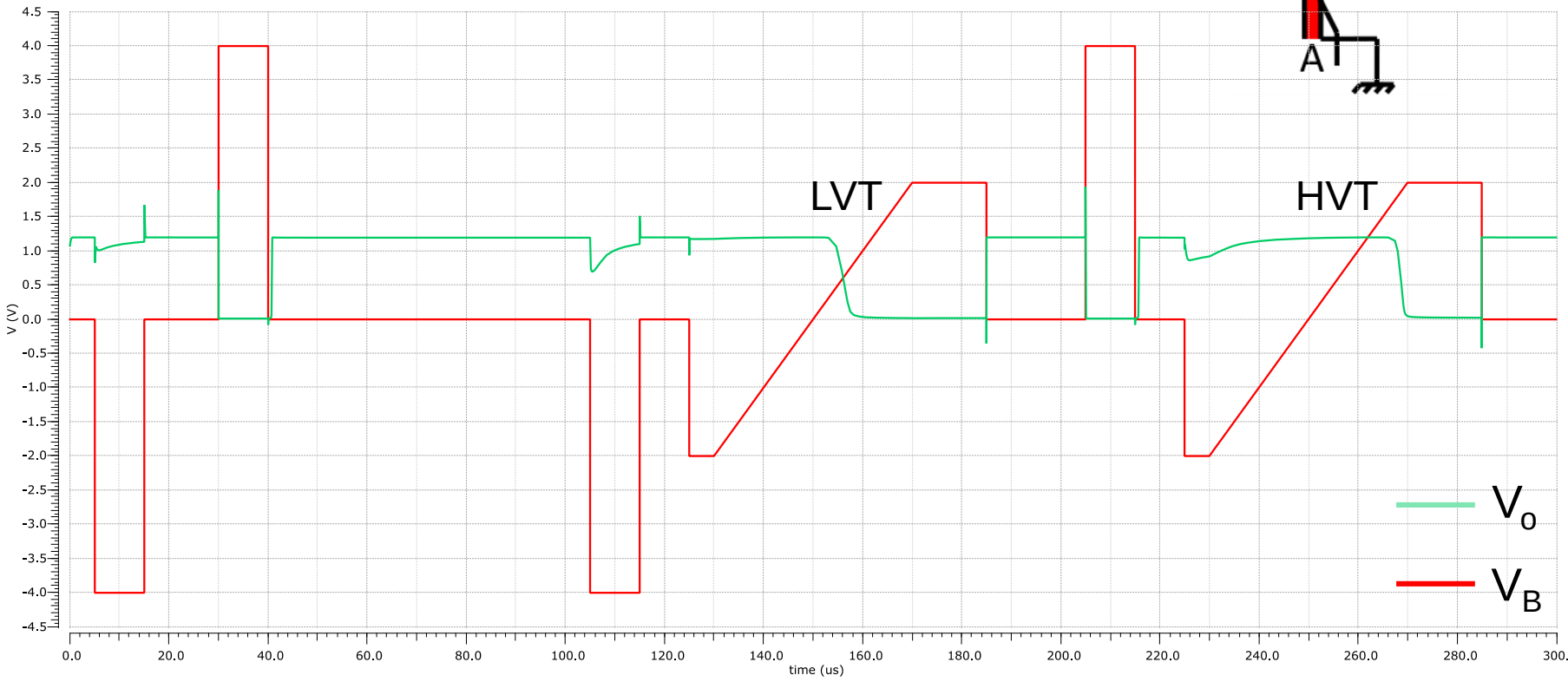


FeFET Logic in memory nand

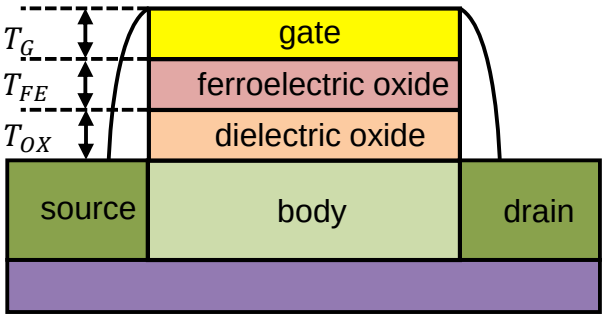


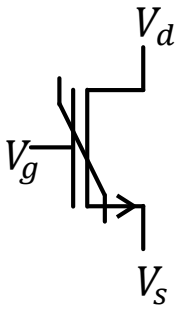


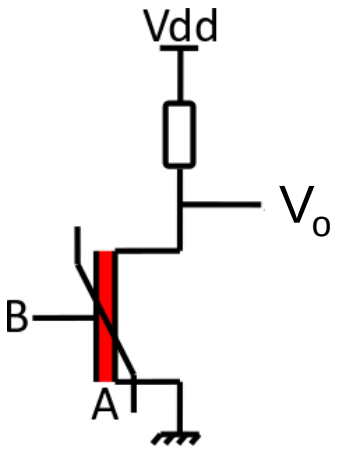


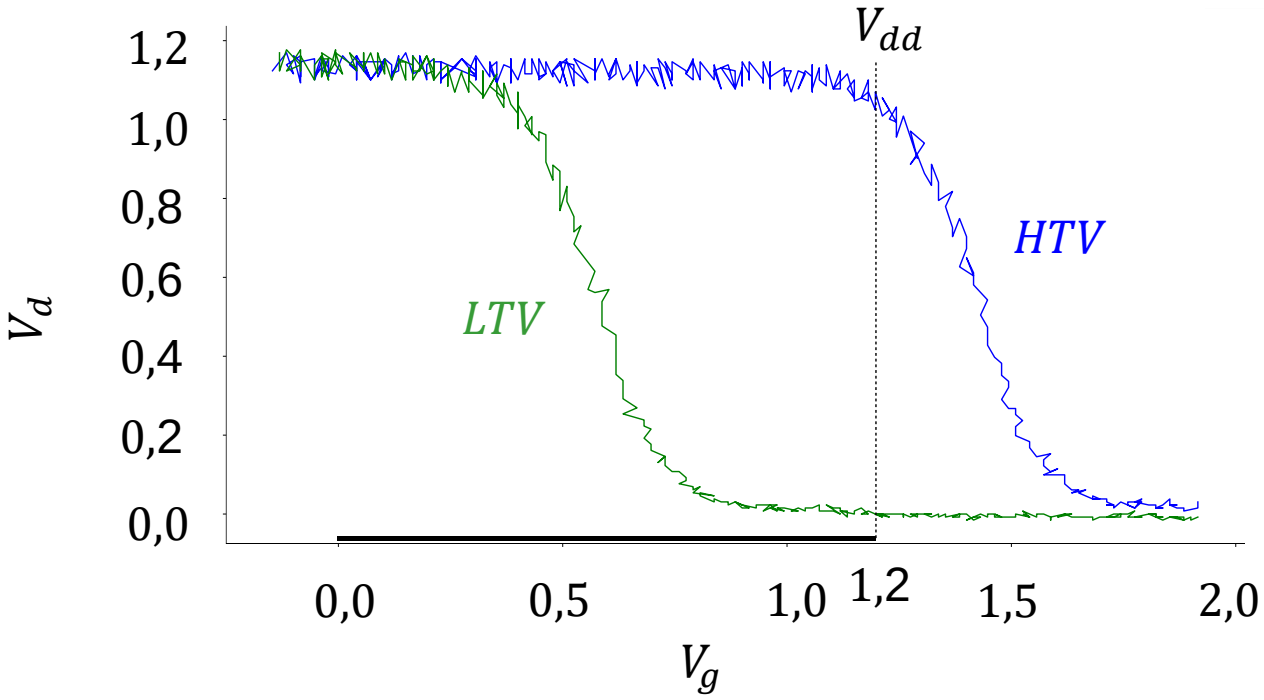


FeFET Logic in memory nand



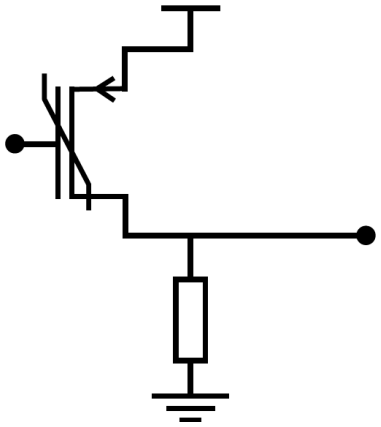


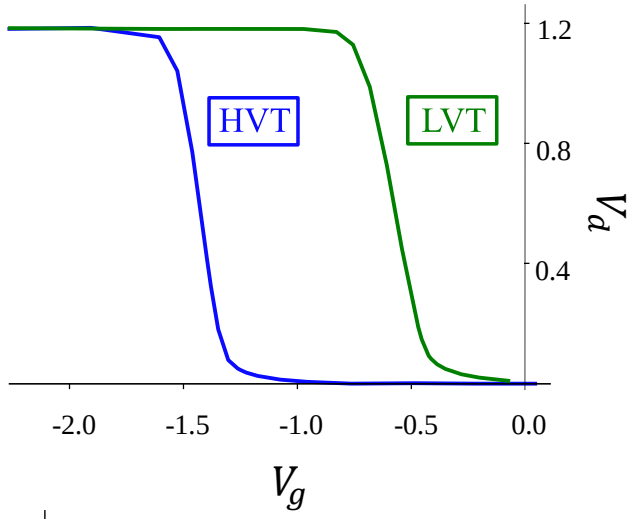




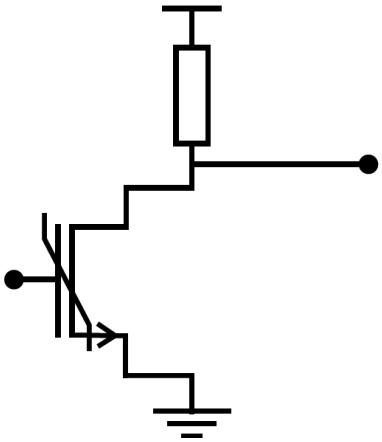
nFeFET vs pFeFET

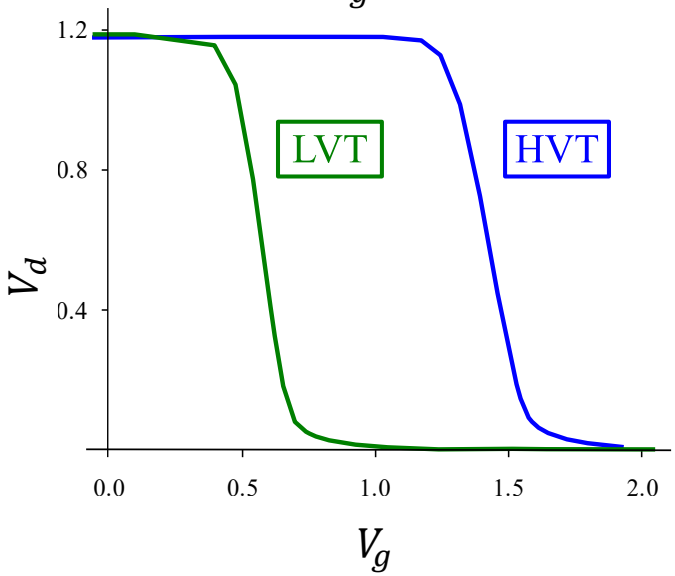
pFeFET



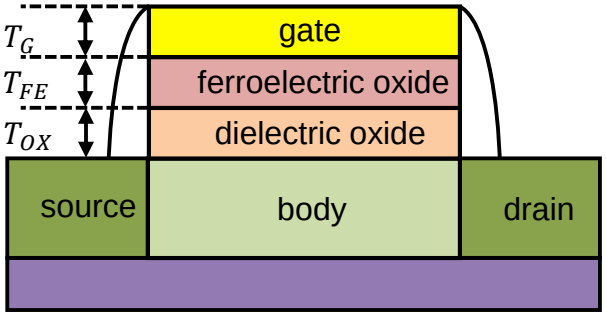


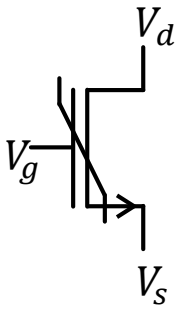
nFeFET

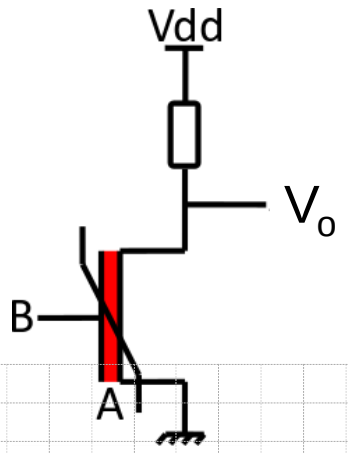


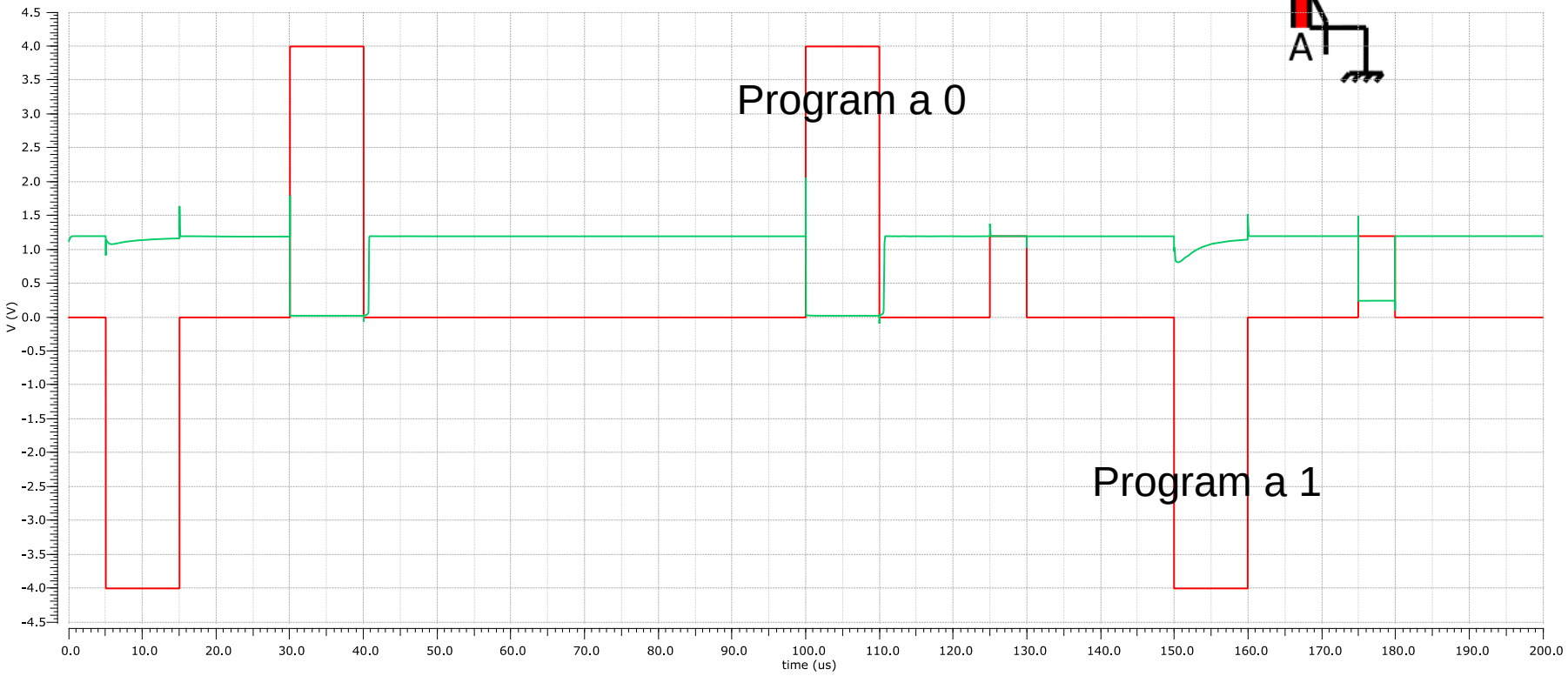


nFeFET Logic in memory NAND









Agenda

1. Introduction
   a) The INL and our team
   b) Context

2. Exploring Logic-in-Memory based on FeFET
   a) FeFET technology and elementary logic gates
   b) Galois field operations
   c) TC-MEM and Sbox implementation

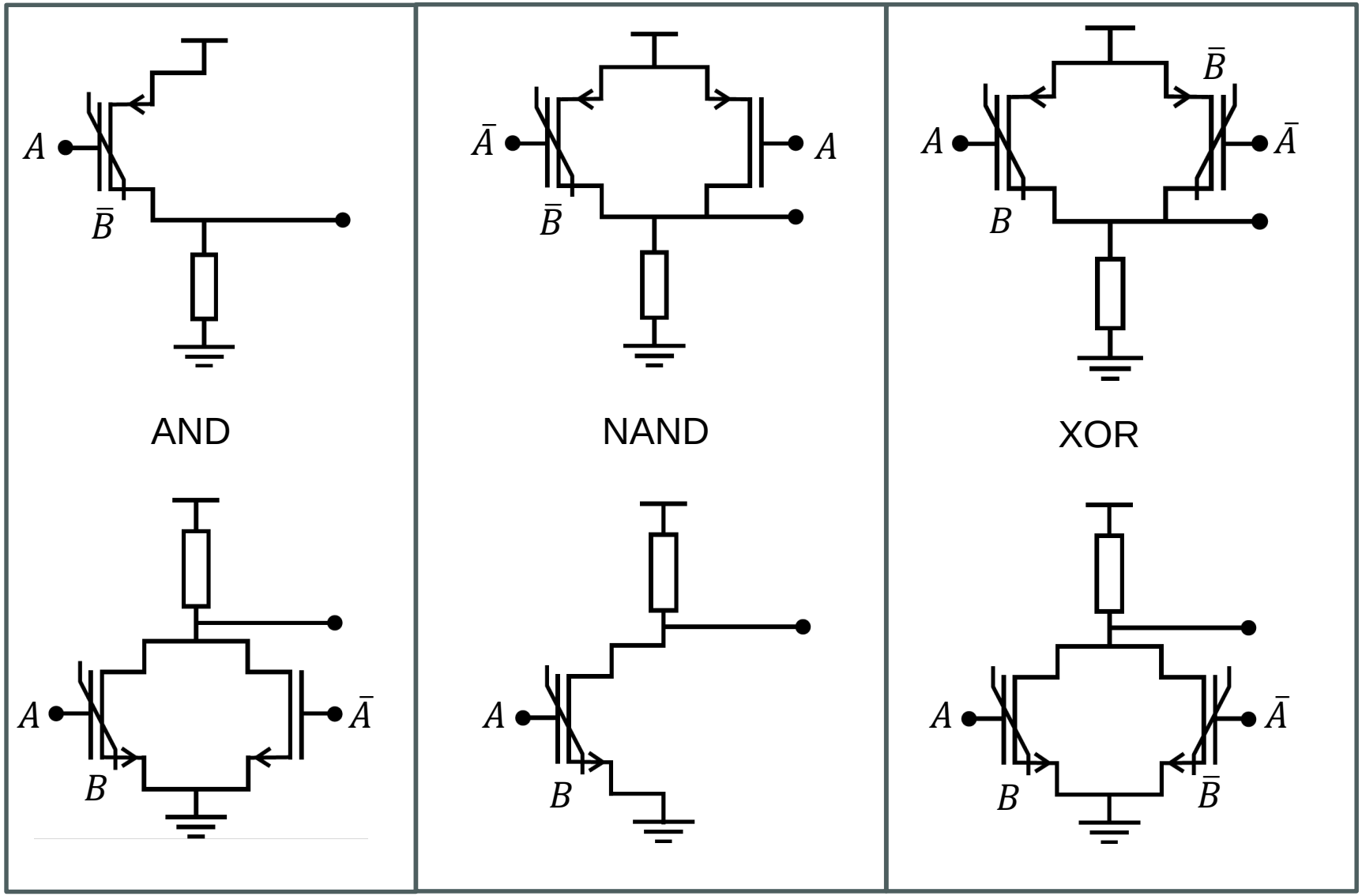
3. Platform and evaluation tool

4. Open challenge and future direction

FeFET complementary logic gates

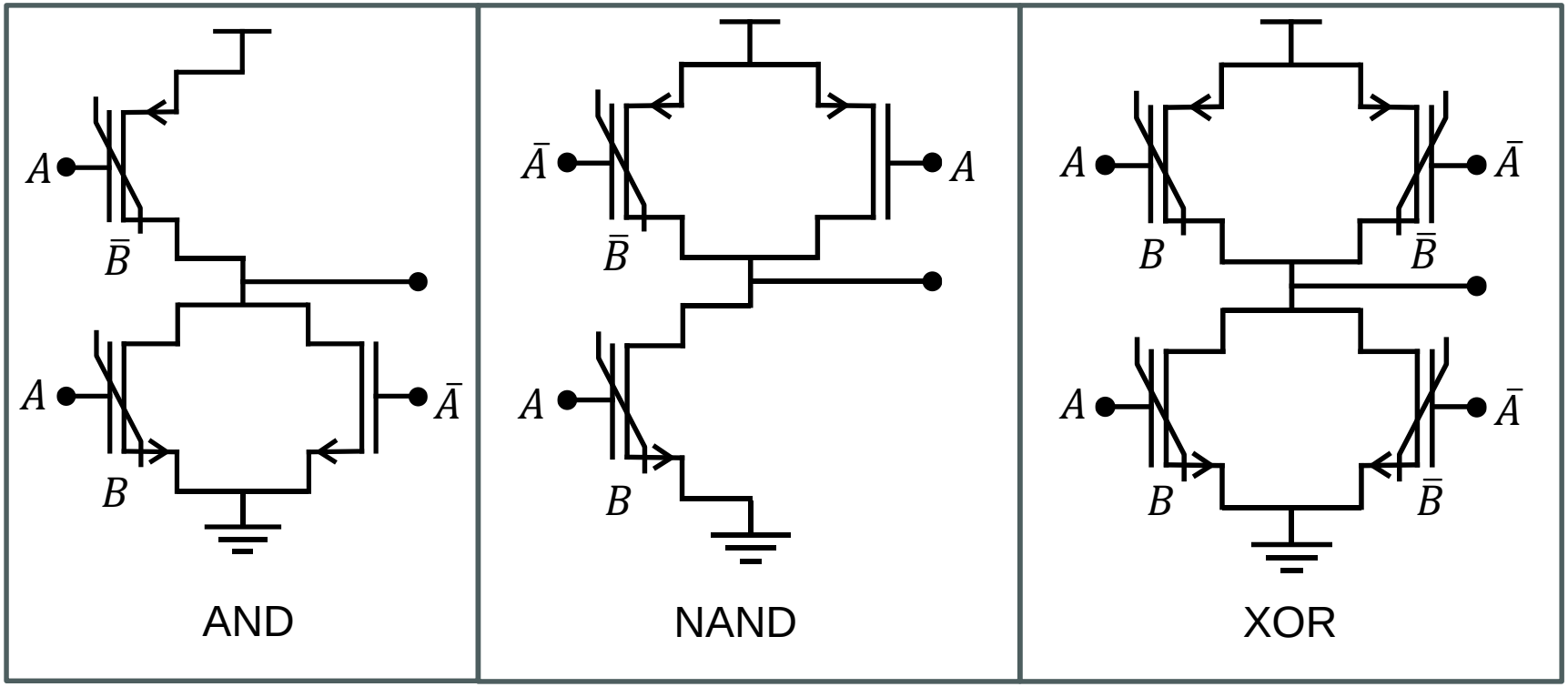
pFeFET

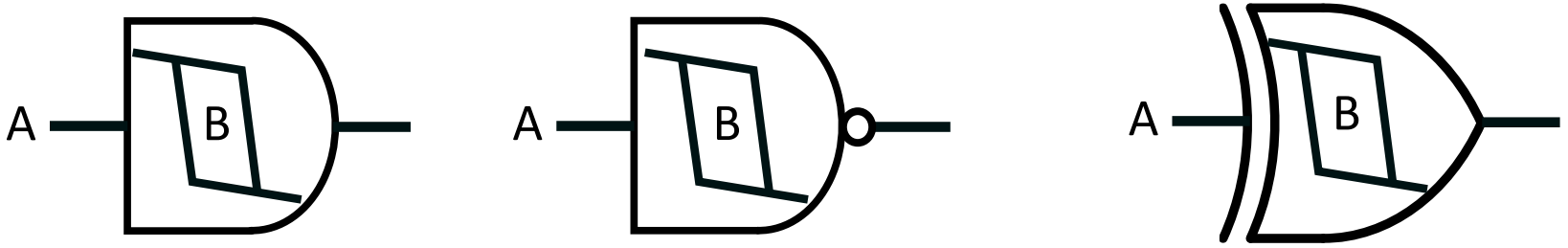
nFeFET



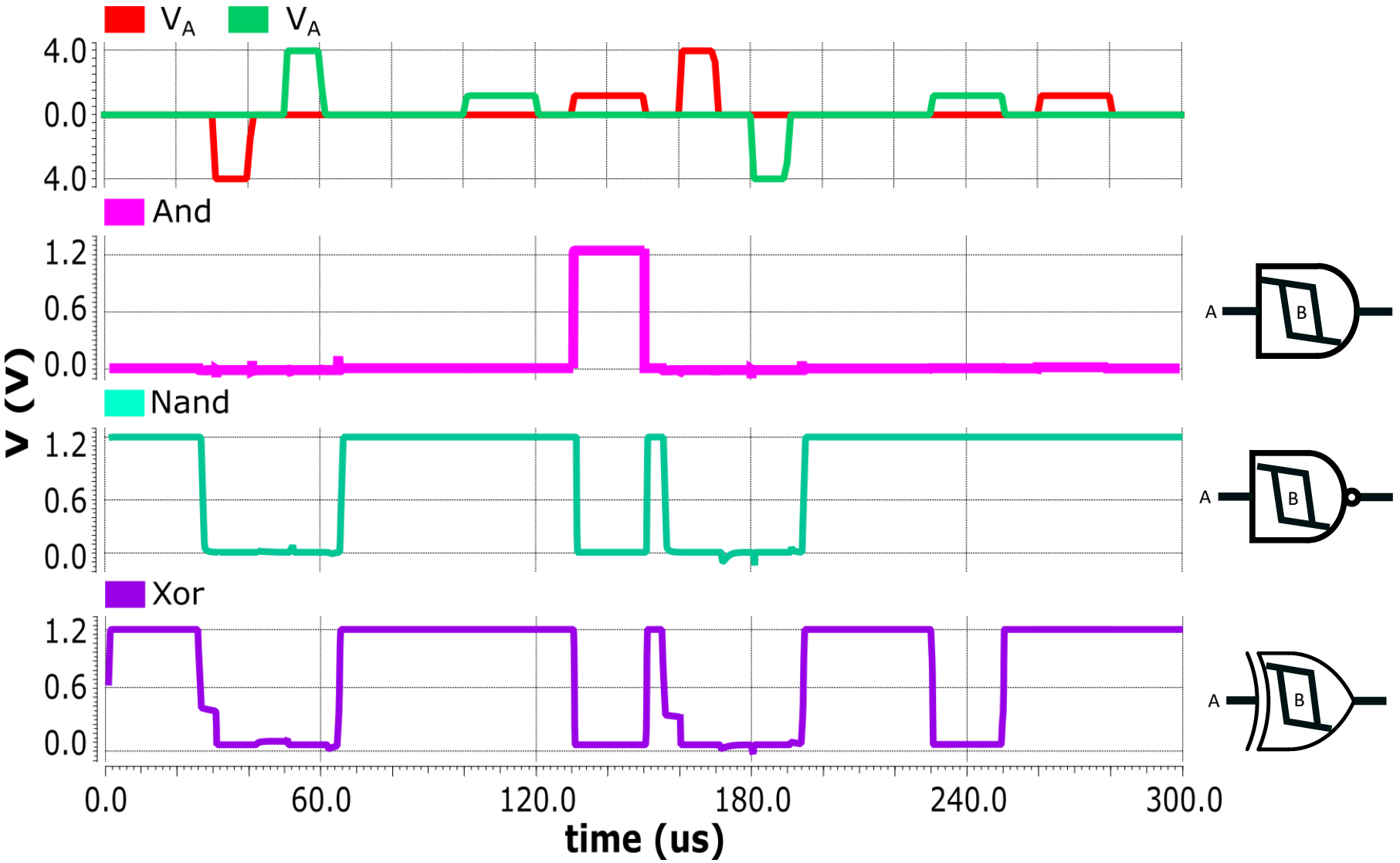
FeFET complementary logic gates

cFeFET



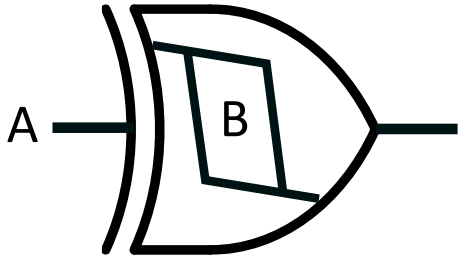


FeFET complementary logic gates



Non volatile operator for cryptography

- Finite field operation:
  - Addition = subtraction = exclusive OR

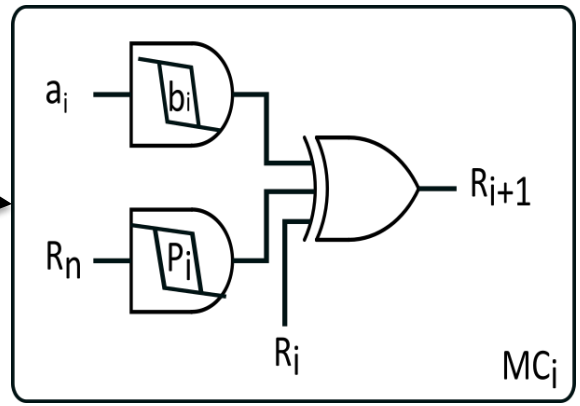


  - Multiplication using polynomial over the finite field
    - Need a reduction by an irreducible polynomial of the field if the result of the multiplication is outside the field
    - Easy for small fields (< GF(2^8))

and if multiplication are small

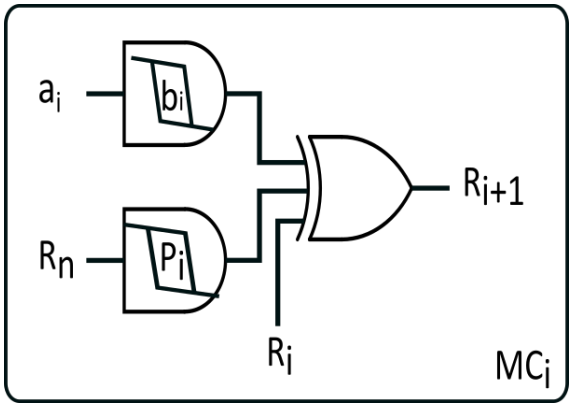
- Difficult for large fields

or if multiplication are large

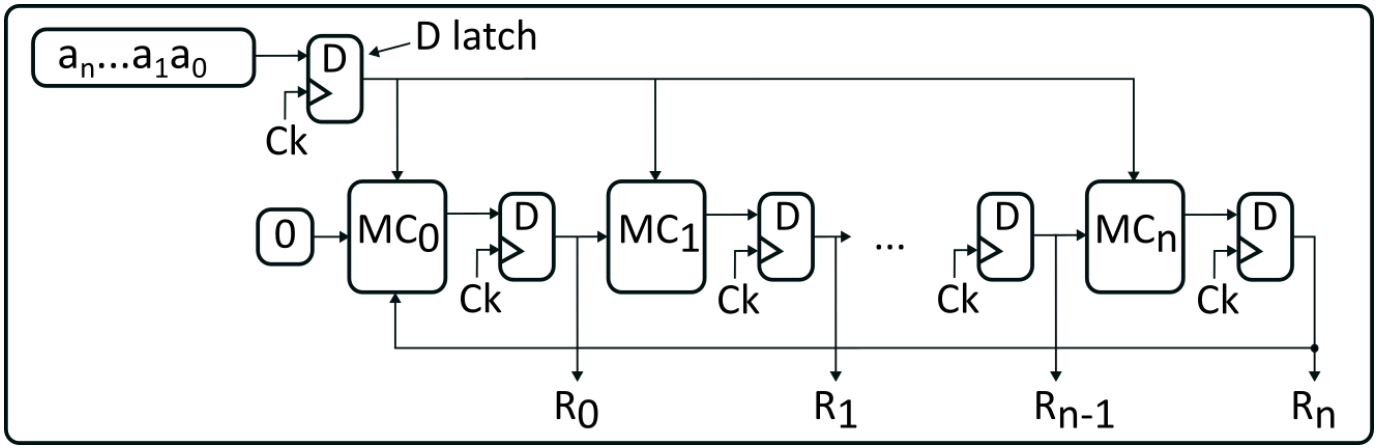


Non volatile Galois field multiplier

1-bit multiplication



n-bit multiplication



Agenda

1. Introduction
   a) The INL and our team
   b) Context

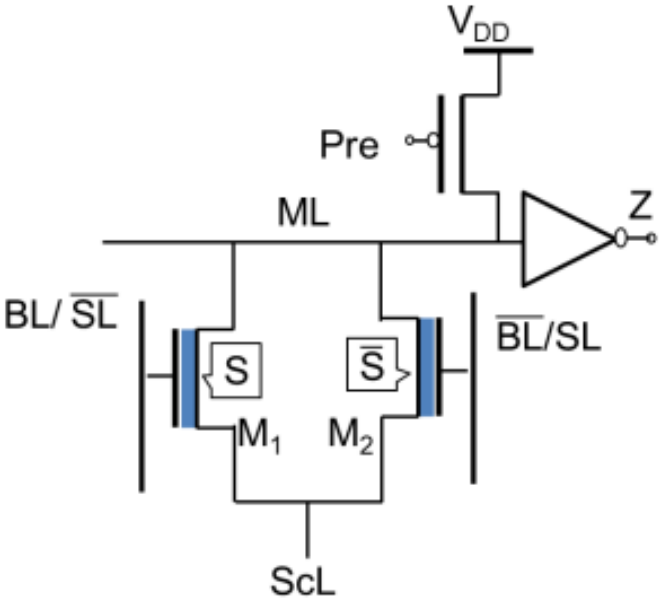
2. Exploring Logic-in-Memory based on FeFET
   a) FeFET technology and elementary logic gates
   b) Galois field operations
   c) TC-MEM and Sbox implementation

3. Platform and evaluation tool

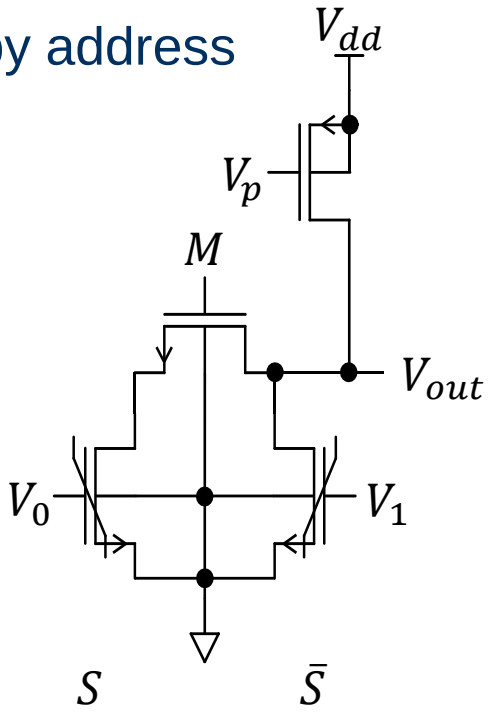
4. Open challenge and future direction

TC-MEM

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



TCAM[1]



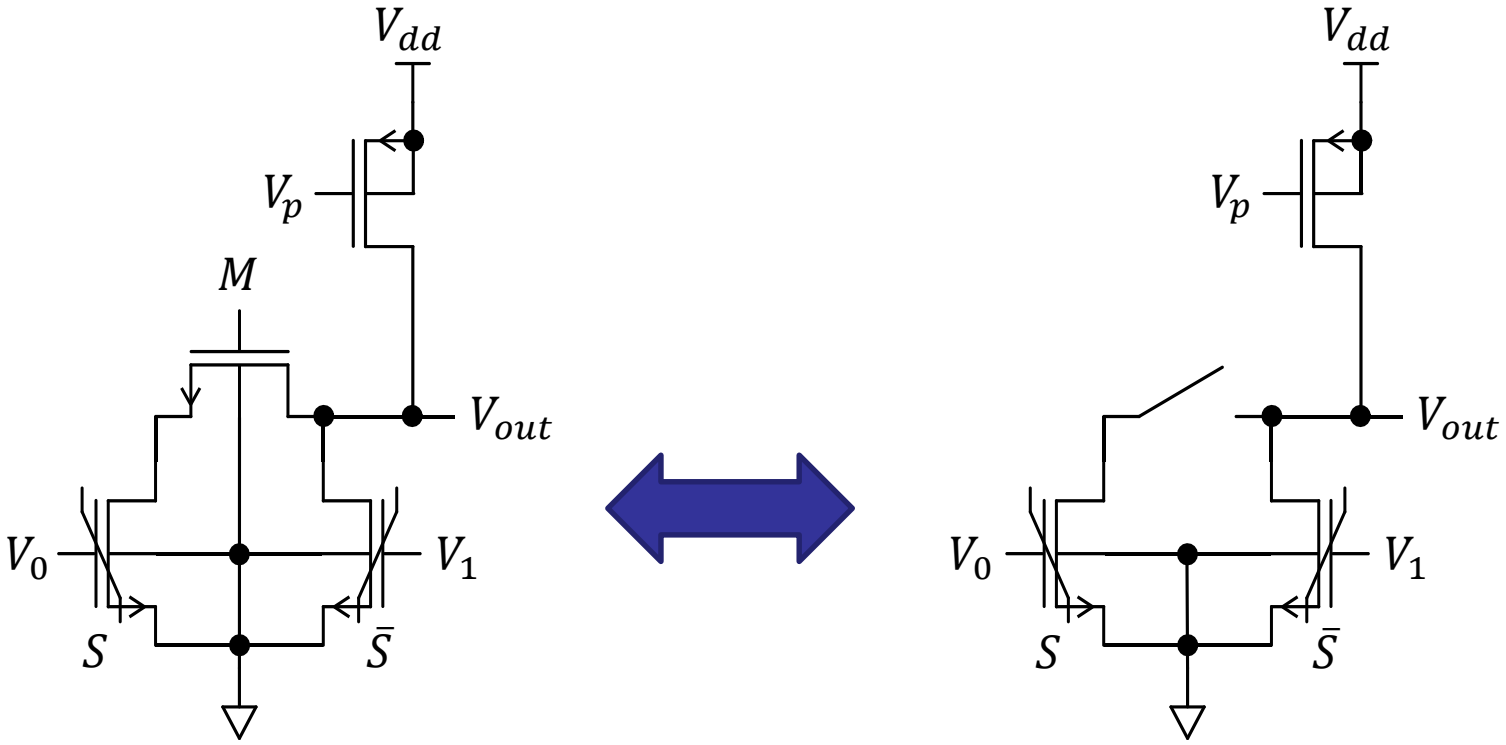
TC-MEM[2]

[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, doi: 10.1109/JXCDC.2022.3168057.

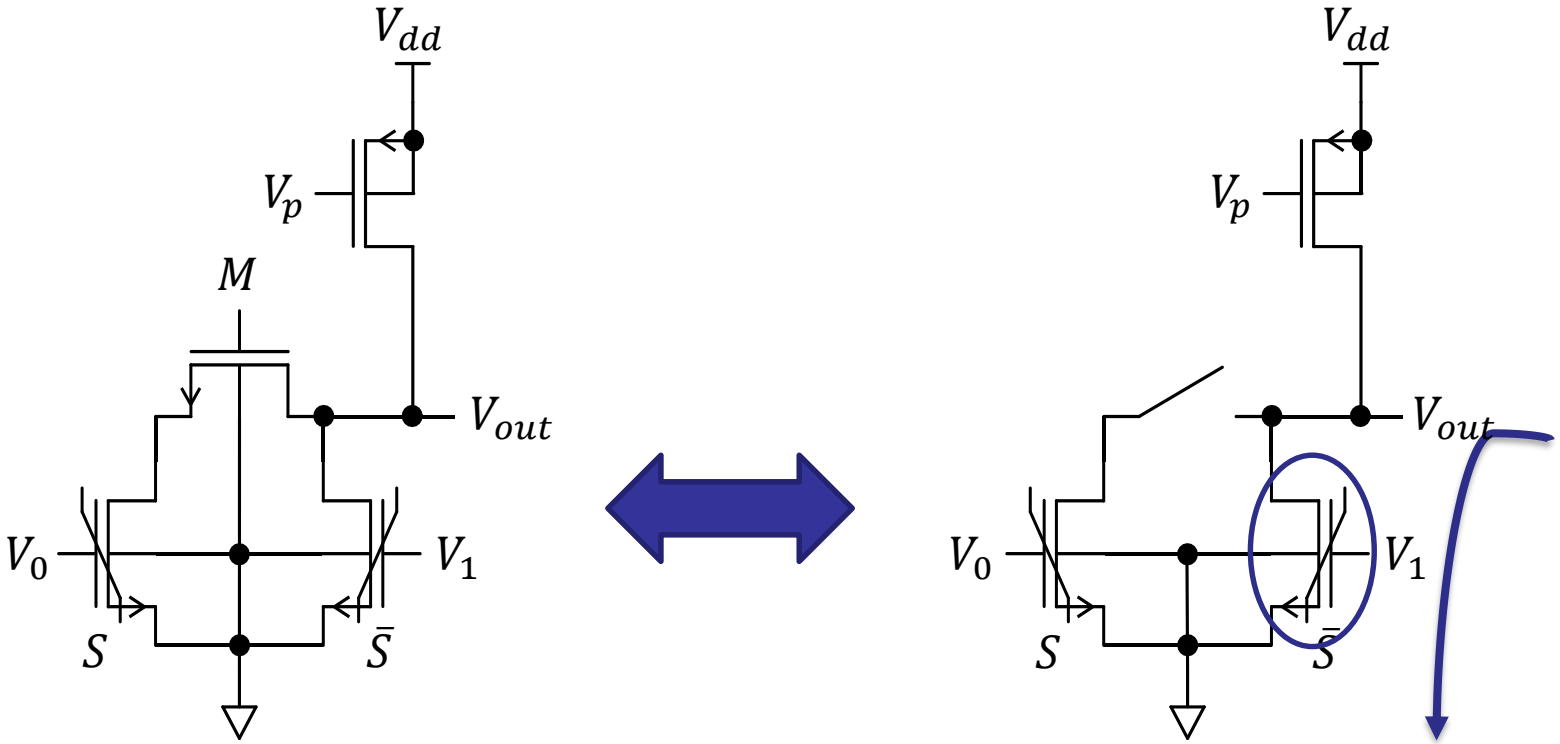
TC-MEM

- $M = 0$: Memory mode



TC-MEM

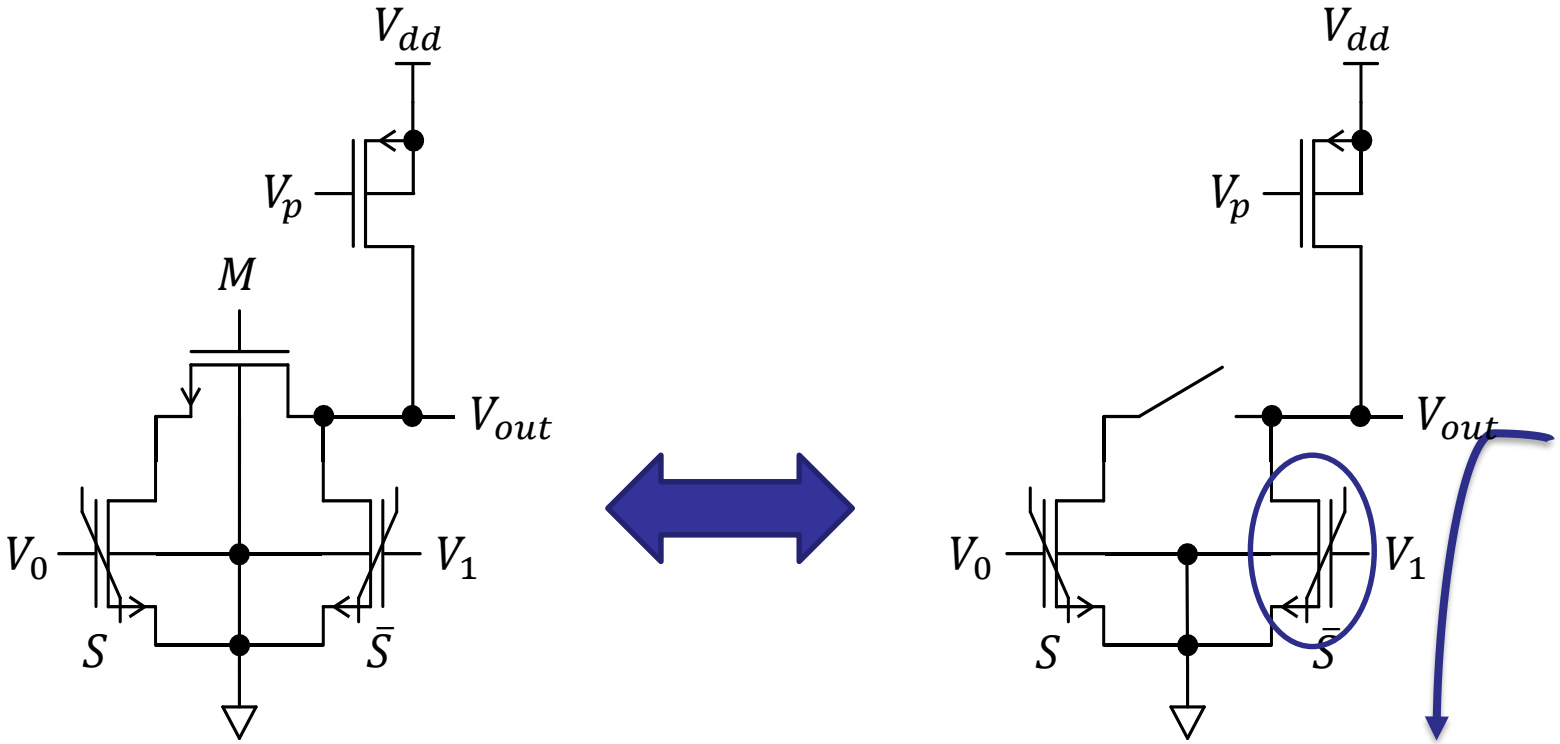
- $M = 0$: Memory mode



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

TC-MEM

- $M = 0$: Memory mode

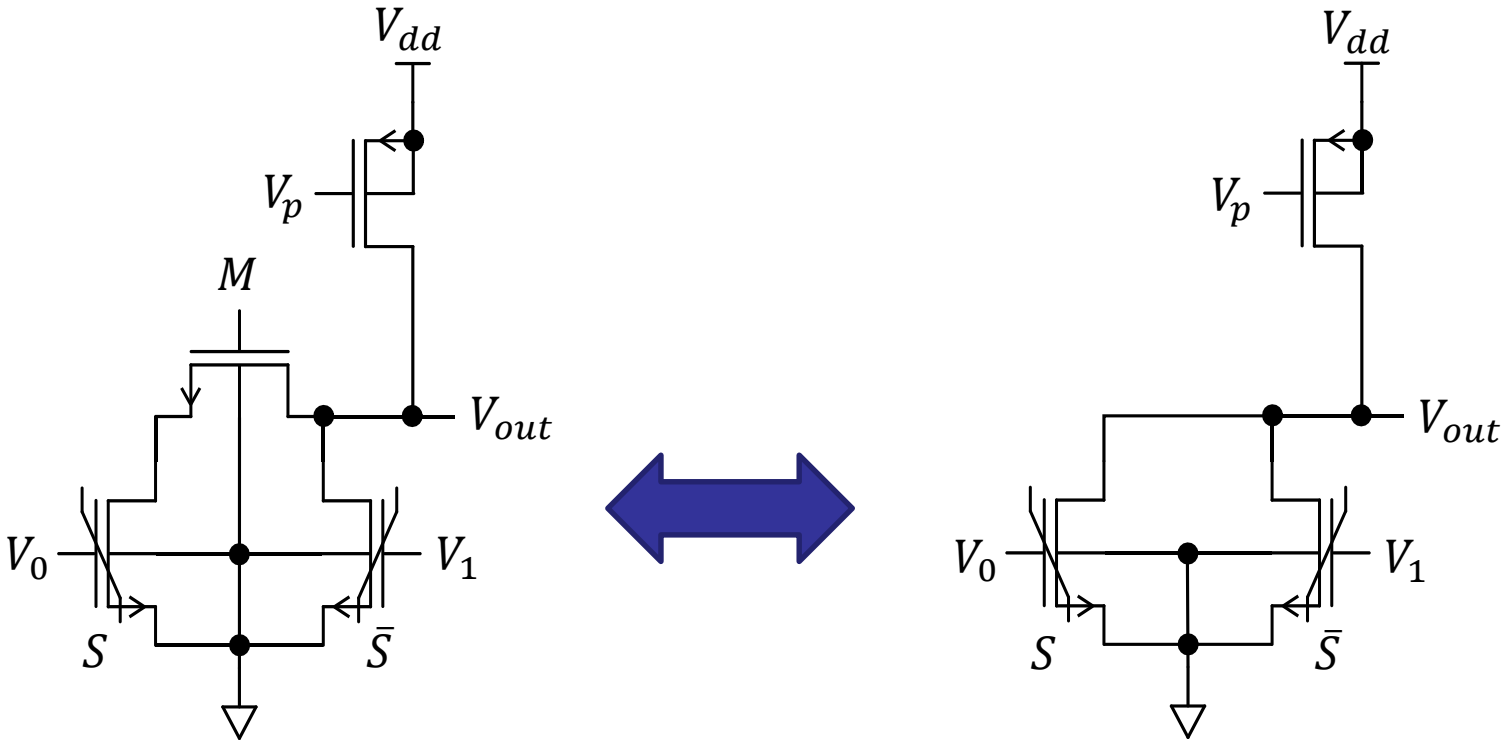


$$V_o = \overline{V_1 . \bar{S}}$$

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

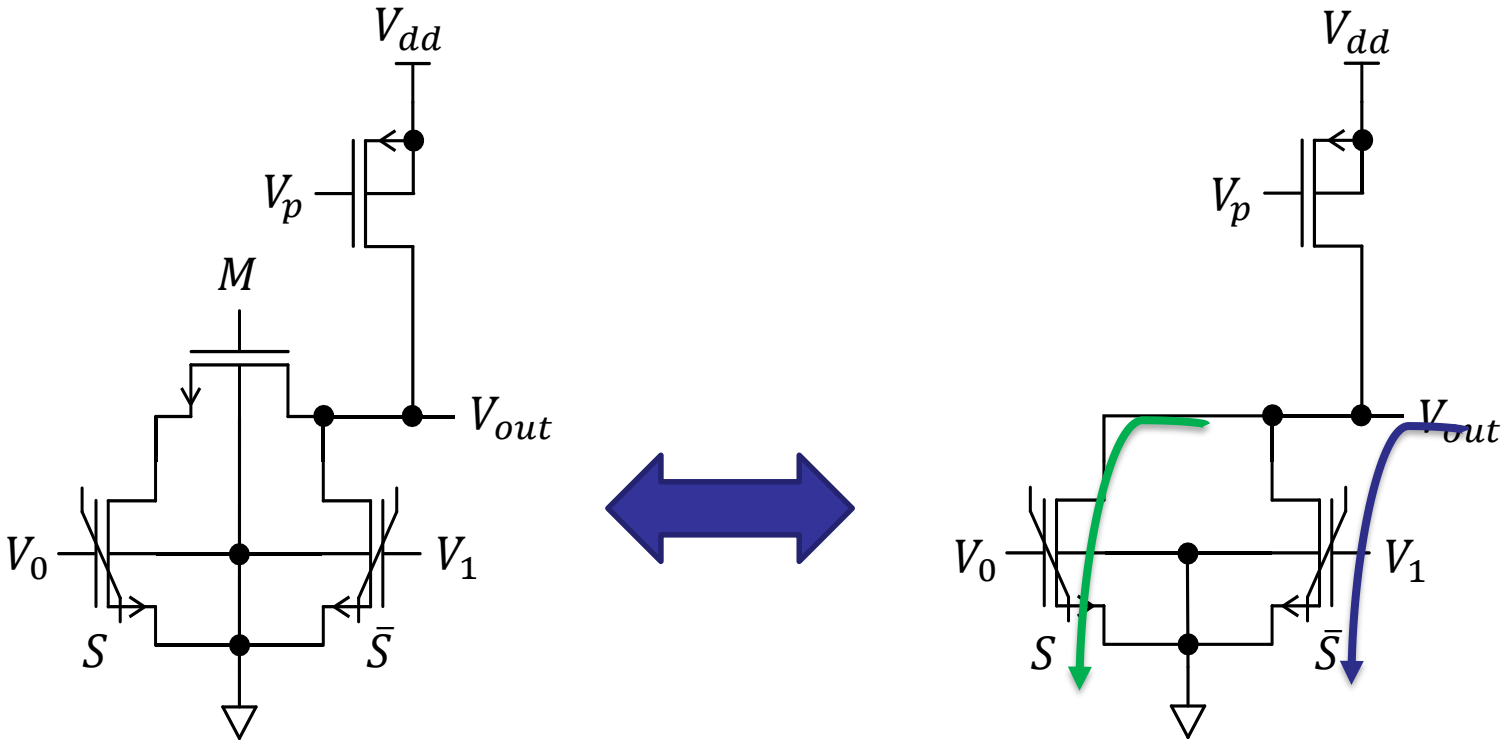
TC-MEM

- $M = 1$: TCAM mode



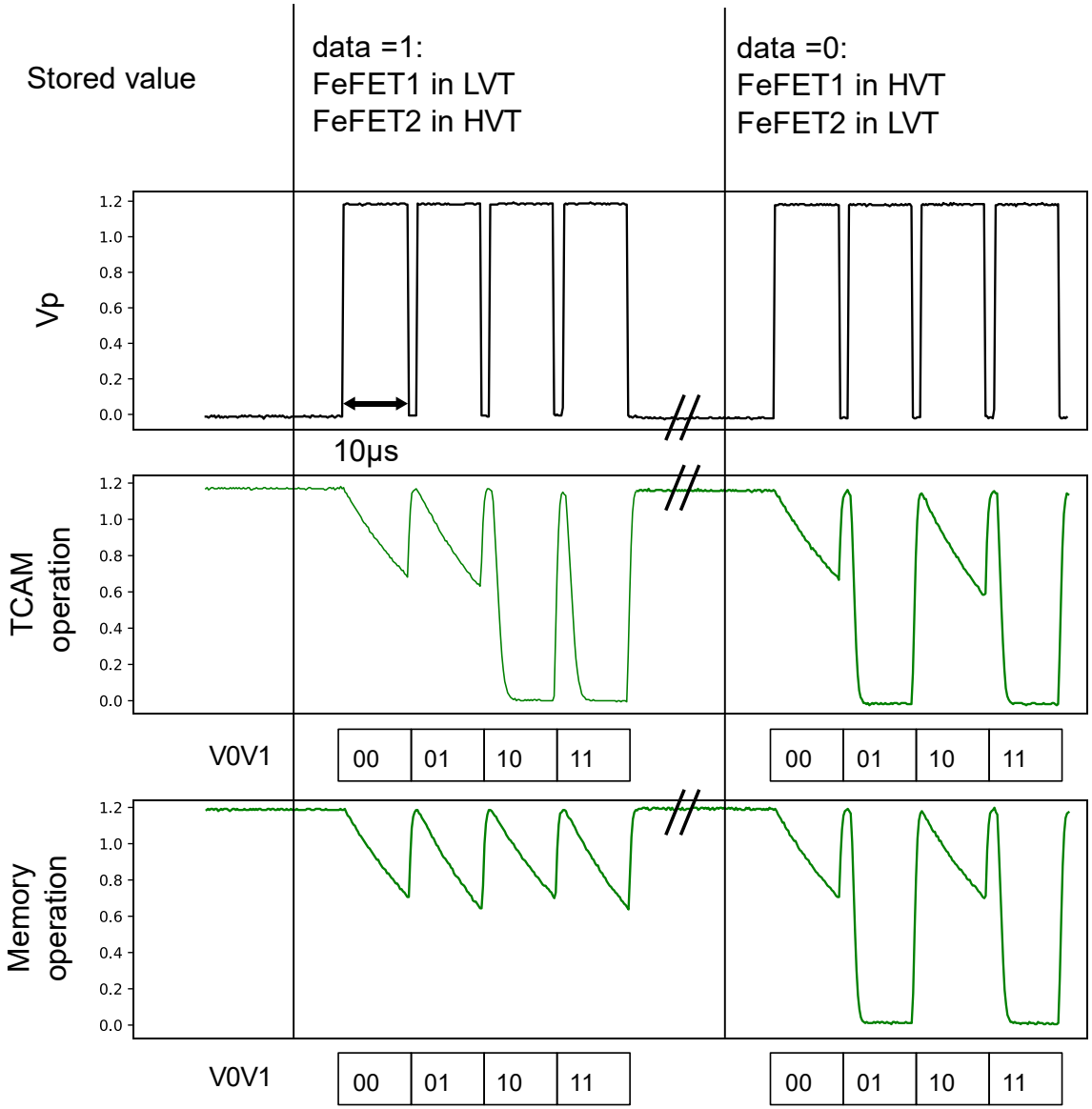
TC-MEM

- $M = 1$: TCAM mode

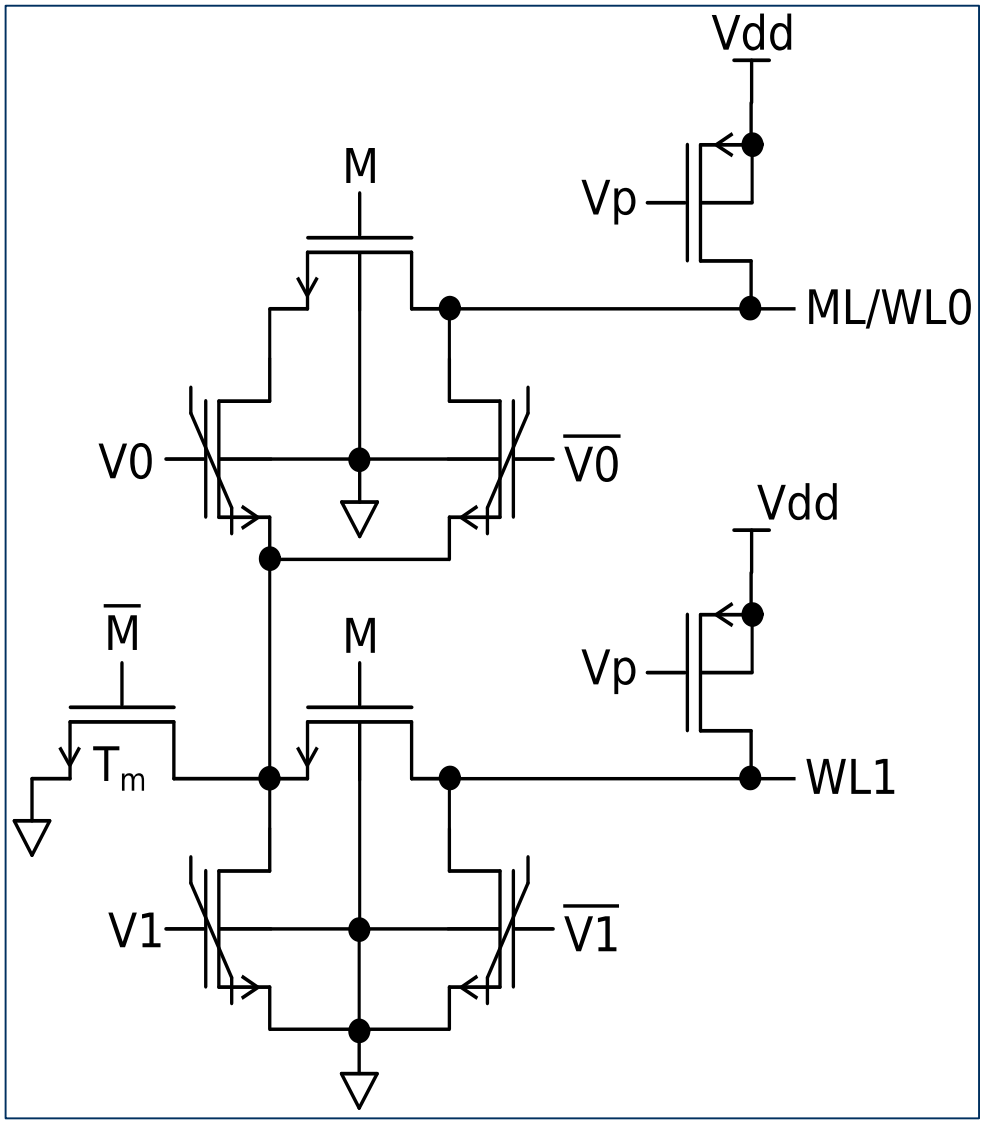


$$V_{out} = \overline{V_0.S}.\overline{V_1.\bar{S}}$$

TC-MEM (chip measurement)



TC-MEM 2-bit, 4-bit, …

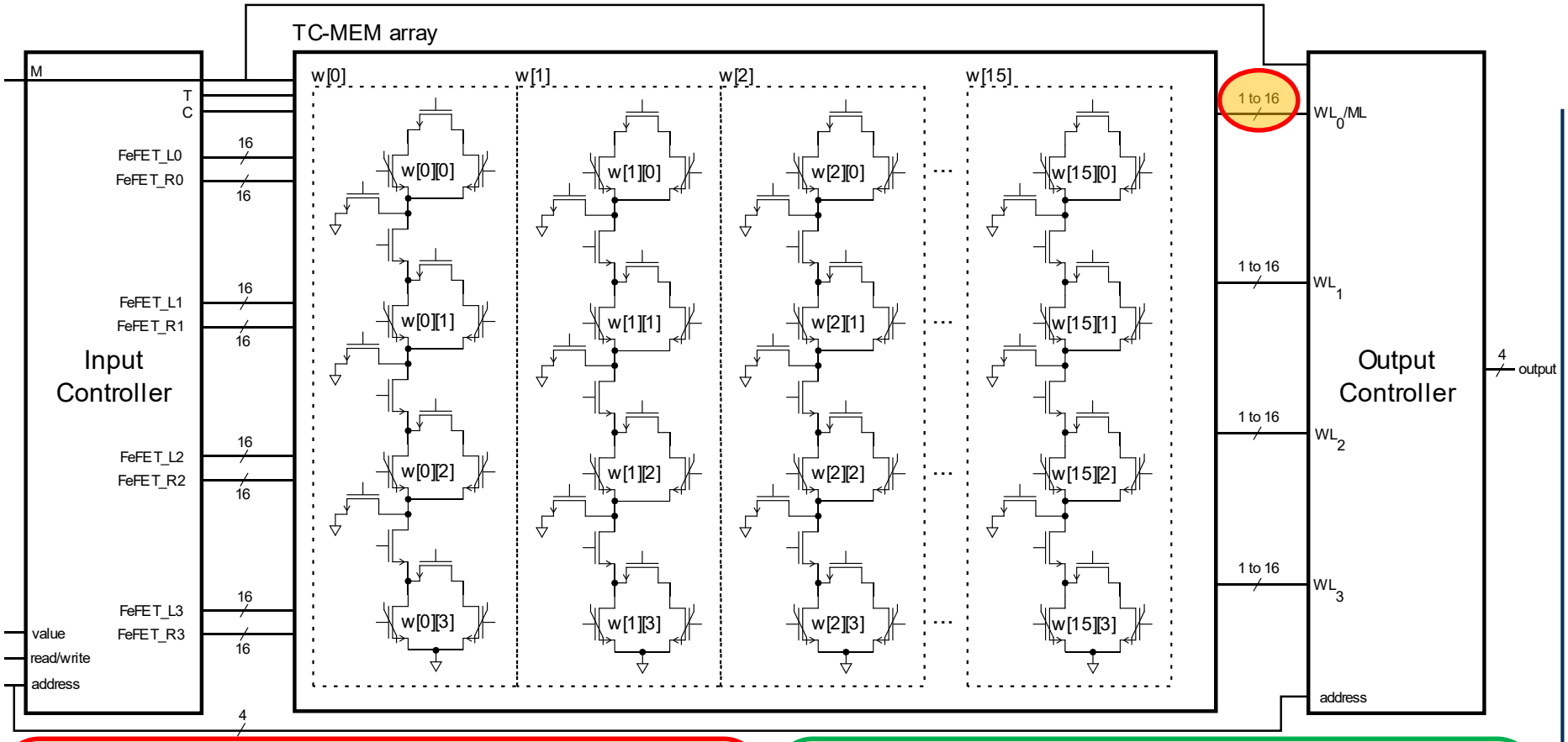


2-bit TC-MEM

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

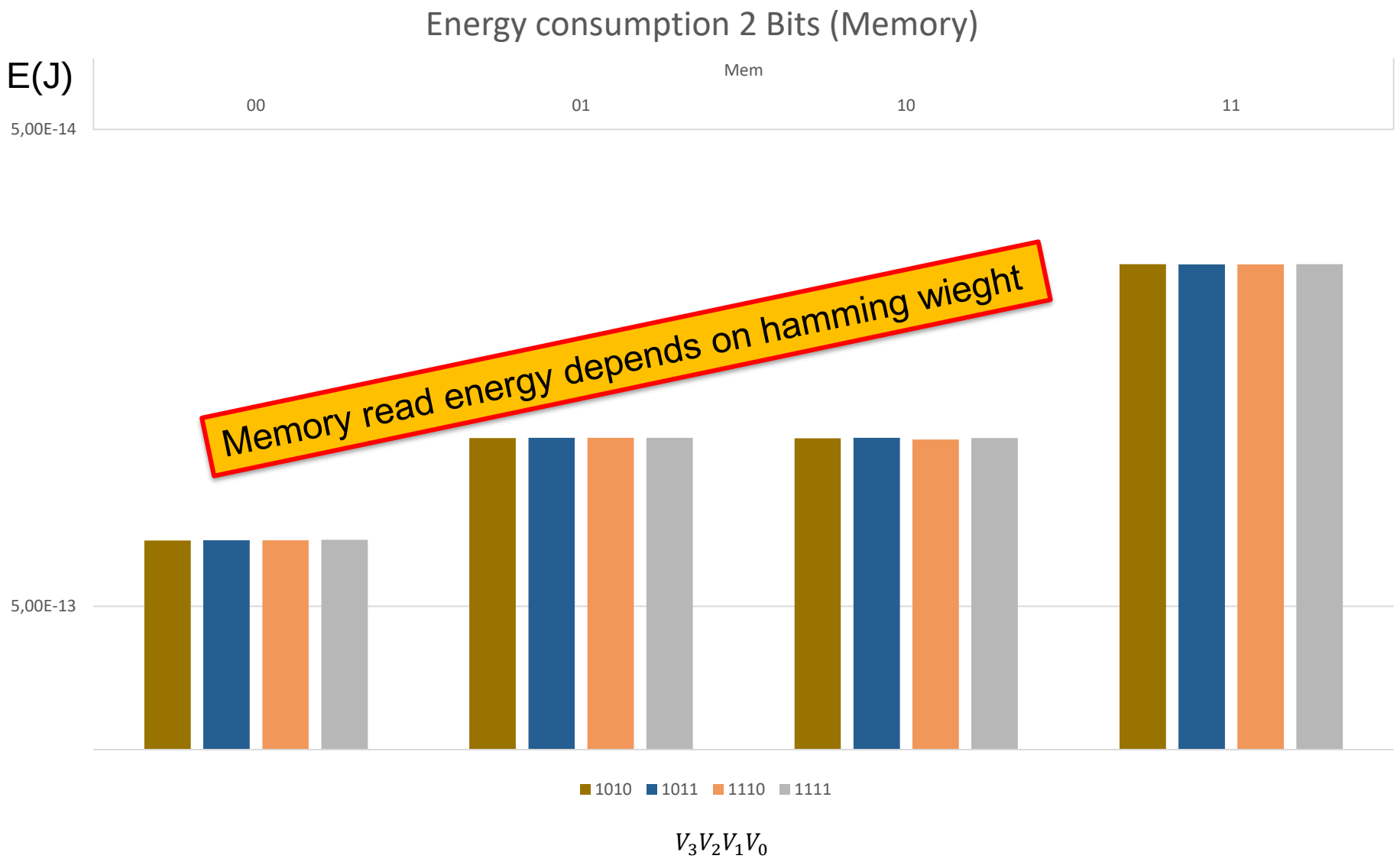
Sbox implementation 2:

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

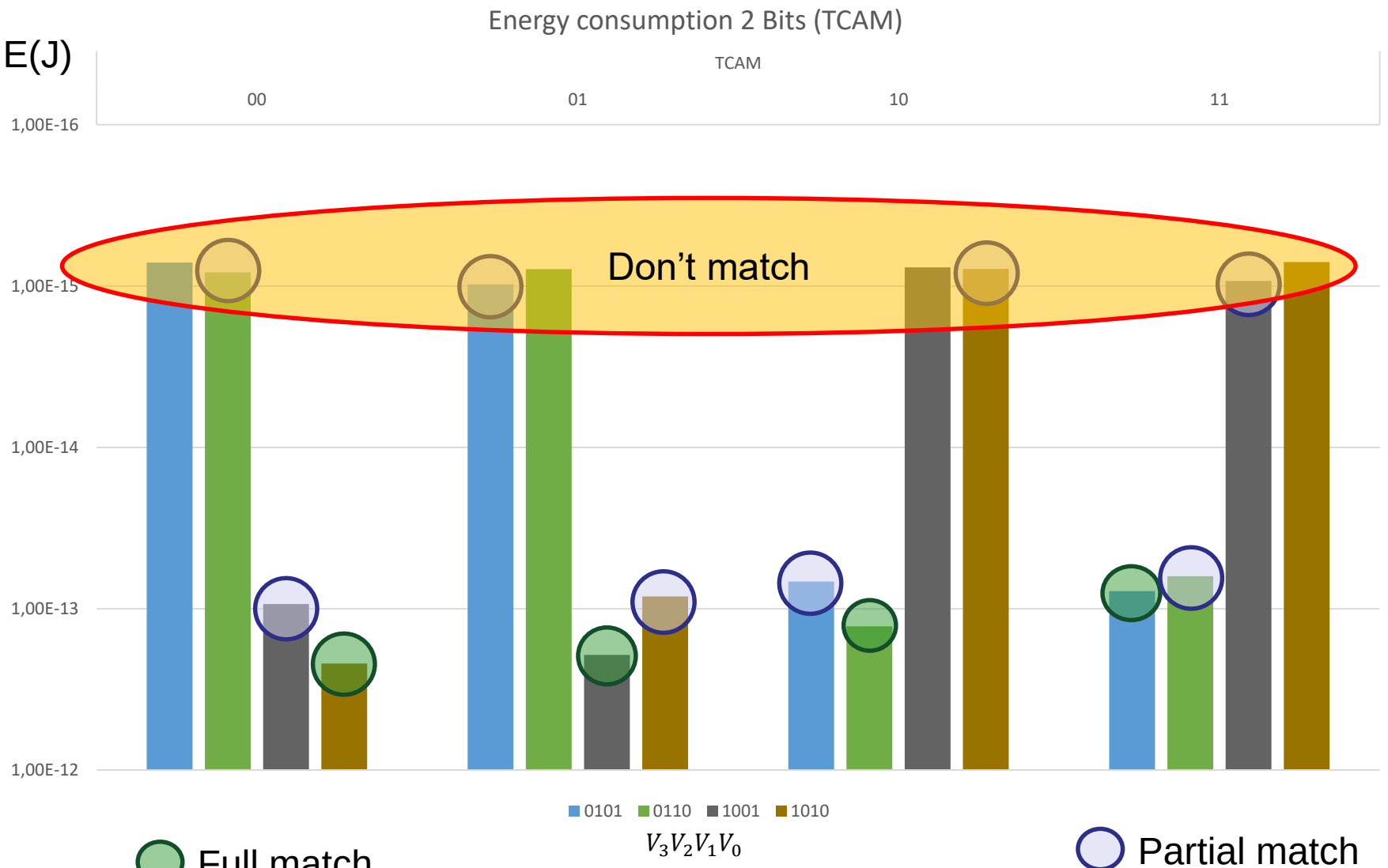
Shared vs separated match line

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

Energy consumption and side channel attacks



Energy consumption and side channel attacks



Agenda

1. Introduction
   a) The INL and our team
   b) Context

2. Exploring Logic-in-Memory based on FeFET
   a) FeFET technology and elementary logic gates
   b) Galois field operations
   c) TC-MEM and Sbox implementation

3. Platform and evaluation tool

4. Open challenge and future direction

Evaluation of non-volatile operators

1. Simulation (Cadence)

Precision	High
Scalability	Low
cost	Low

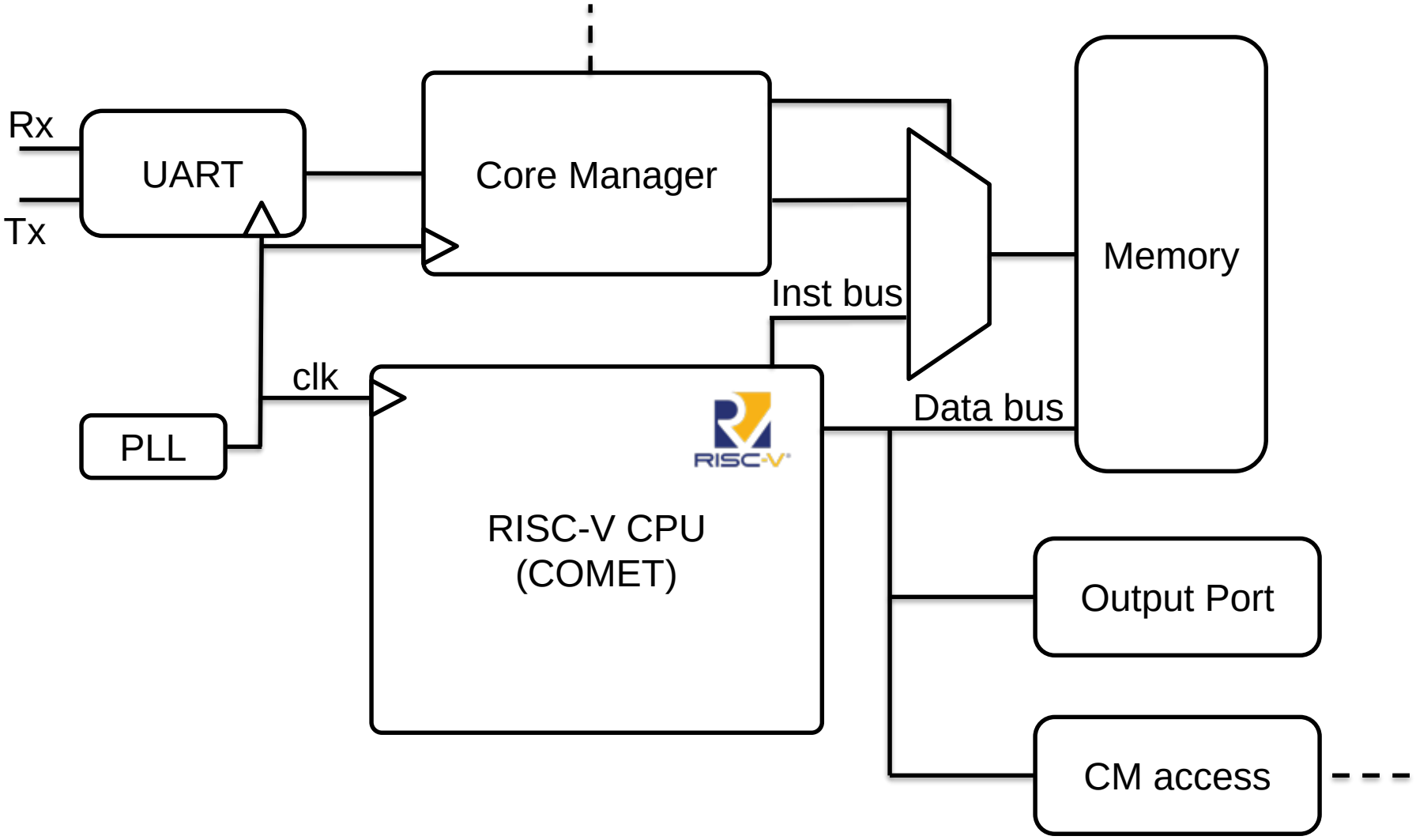
2. Demonstrator

Precision	Very High
Scalability	none
cost	Very high

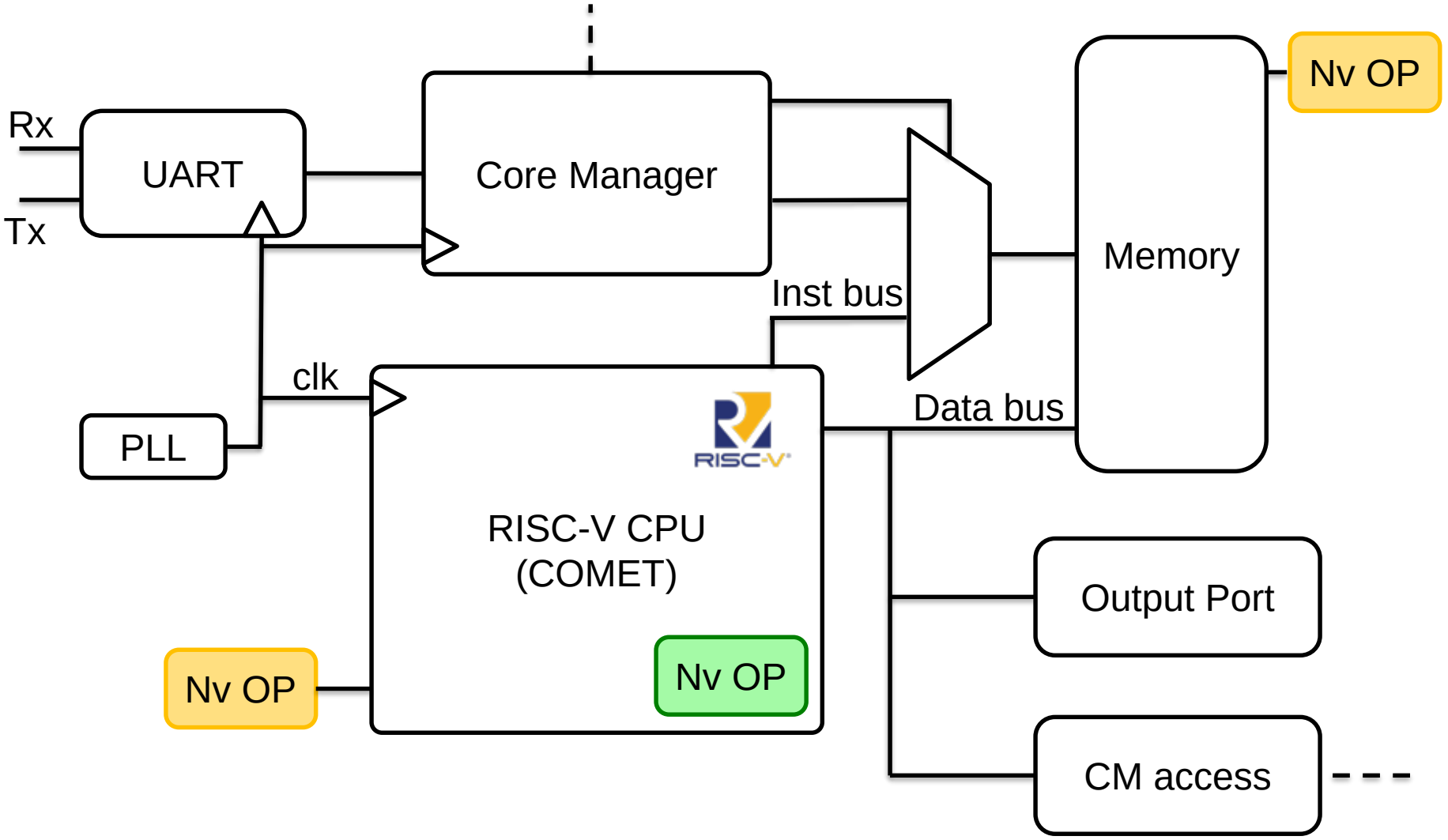
3. Emulation

Precision	variable
Scalability	Very high
cost	low

RISC-V based emulation platform



RISC-V based emulation platform

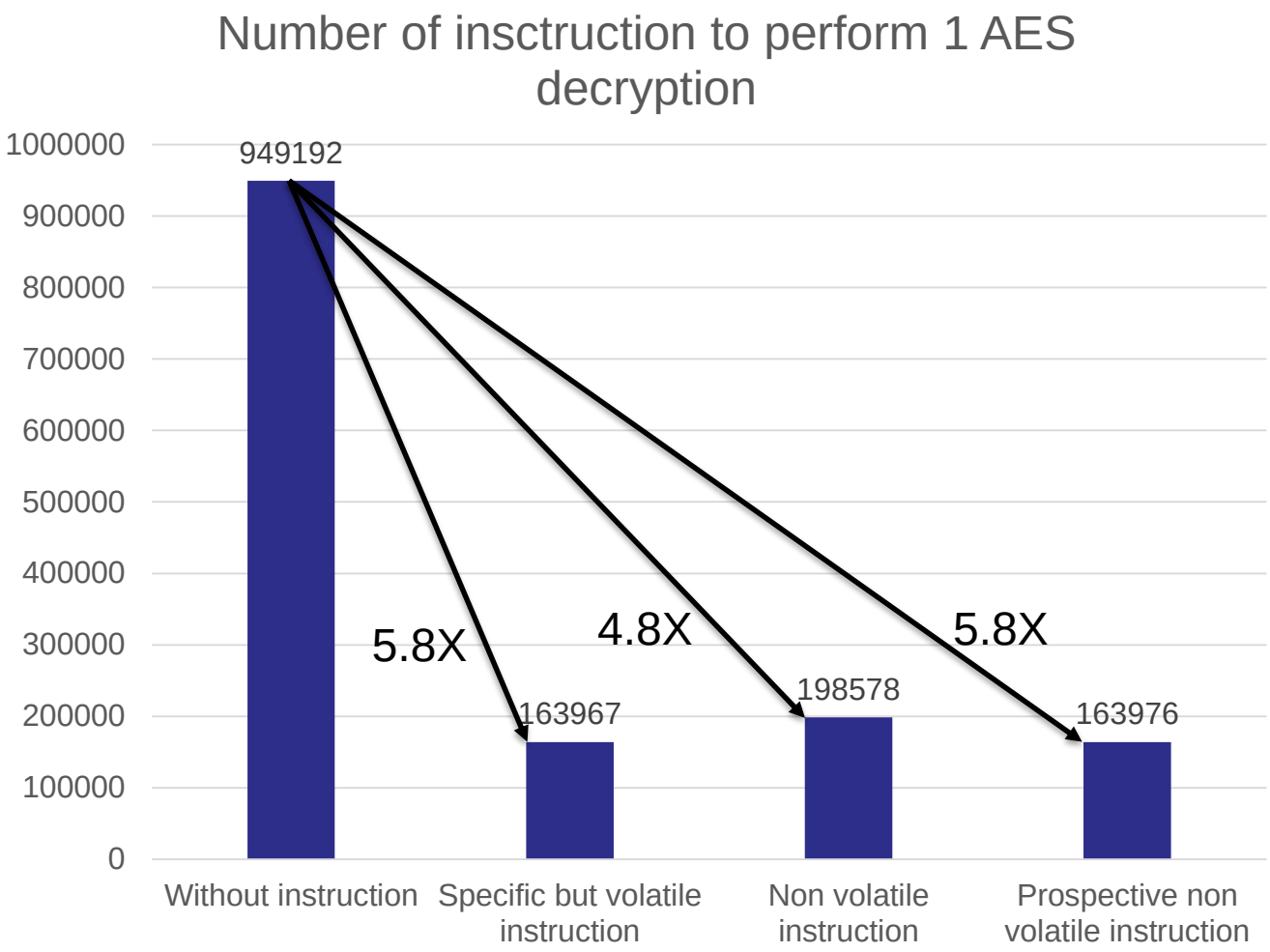


Evaluation of the Galois field multiplier

- Implementation of AES algorithm in the RISC-V core:
  1. Without using any specific instruction (Baseline)
  2. With a new and specific instruction (without FeFET)
  3. With the new, specific and non-volatile instruction (with FeFET)
     1. With 500nm*500nm FeFET (characterized using ASIC)
     2. With prospective values

- Why AES :
  - Standard cryptographic algorithm
  - Use a lot of constant for computation that are publicly available
  - Use multiplication many times
  - Worst case due to small finite field and small multiplication constants.

Evaluation of the Galois field multiplier



To go furhter

- Implementation of other instructions to perform other type of operations dedicated to cryptography:
  1. Design the FeFET based operator
  2. Evaluate it's characteristic (timing, energy, …)
  3. Integrate the new operator in form of new processor instruction

- Create the two different integration level in the platform.
- Manufacture a demonstrator integrating the non-volatile circuit and interfaced it with the platform:
  - Real measurement of timing, energy, …
  - Start to evaluate the security of each designed operator.

Agenda

1. Introduction
   a) The INL and our team
   b) Context

2. Exploring Logic-in-Memory based on FeFET
   a) FeFET technology and elementary logic gates
   b) Galois field operations
   c) TC-MEM and Sbox implementation

3. Platform and evaluation tool

4. Open challenge and future direction

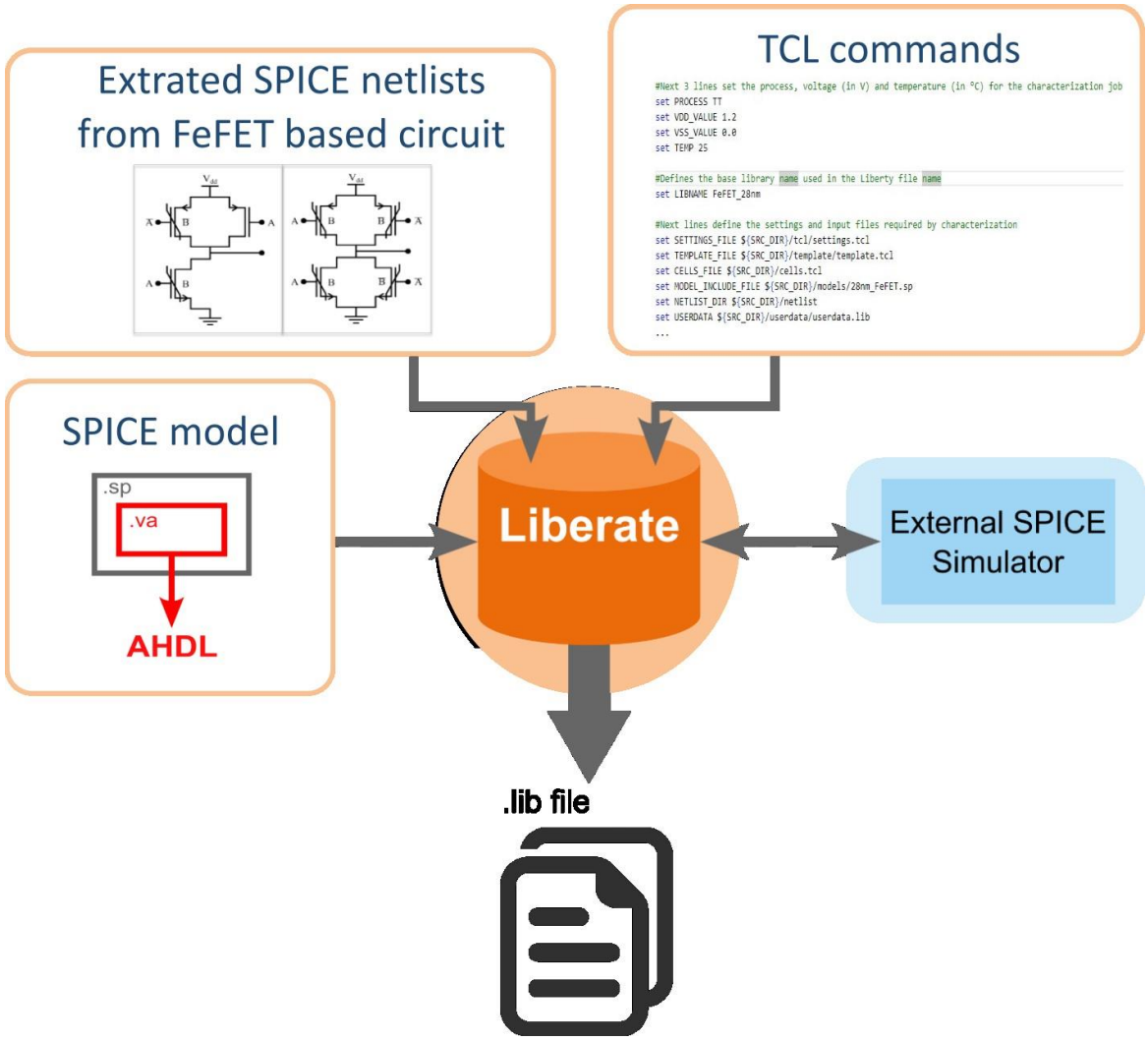
Creation of a standard library for logic synthesis

- Describe using hardware description language complex operation
- Ease the development of computing circuit based on FeFET

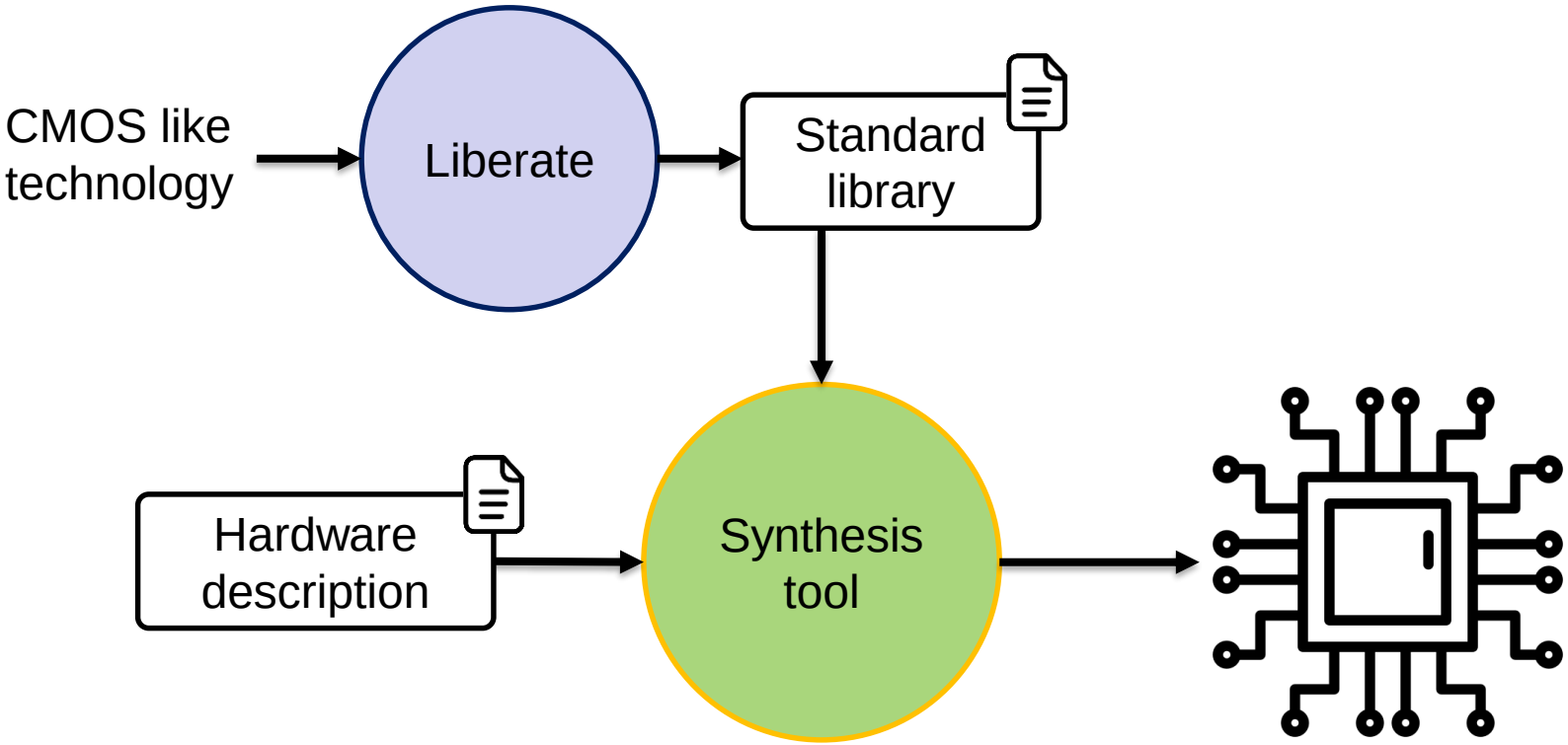
But

- Require a lot of simulations
- Mismatch between characteristic file and logic synthesis for non-volatile device.

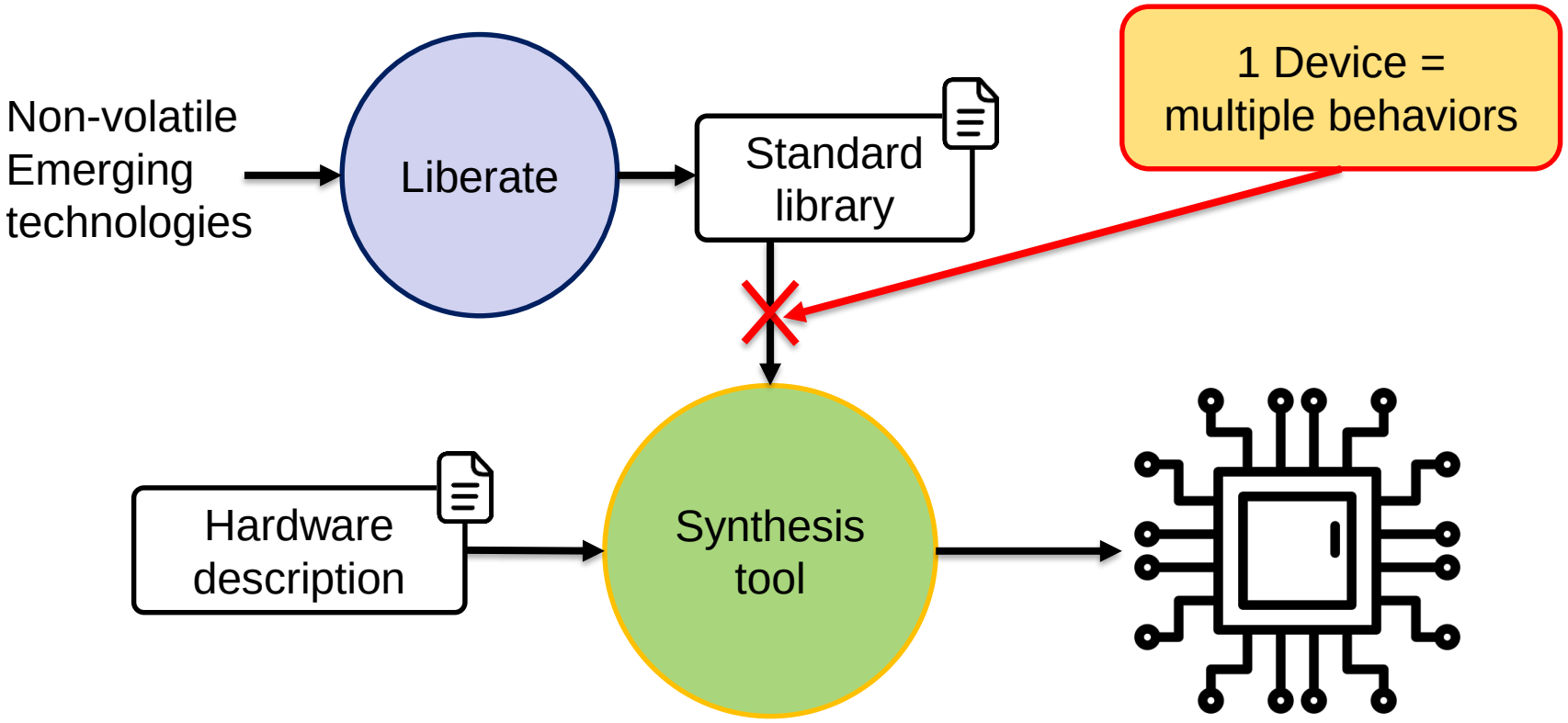
Automatic generation of liberty file



CMOS like emerging technologies



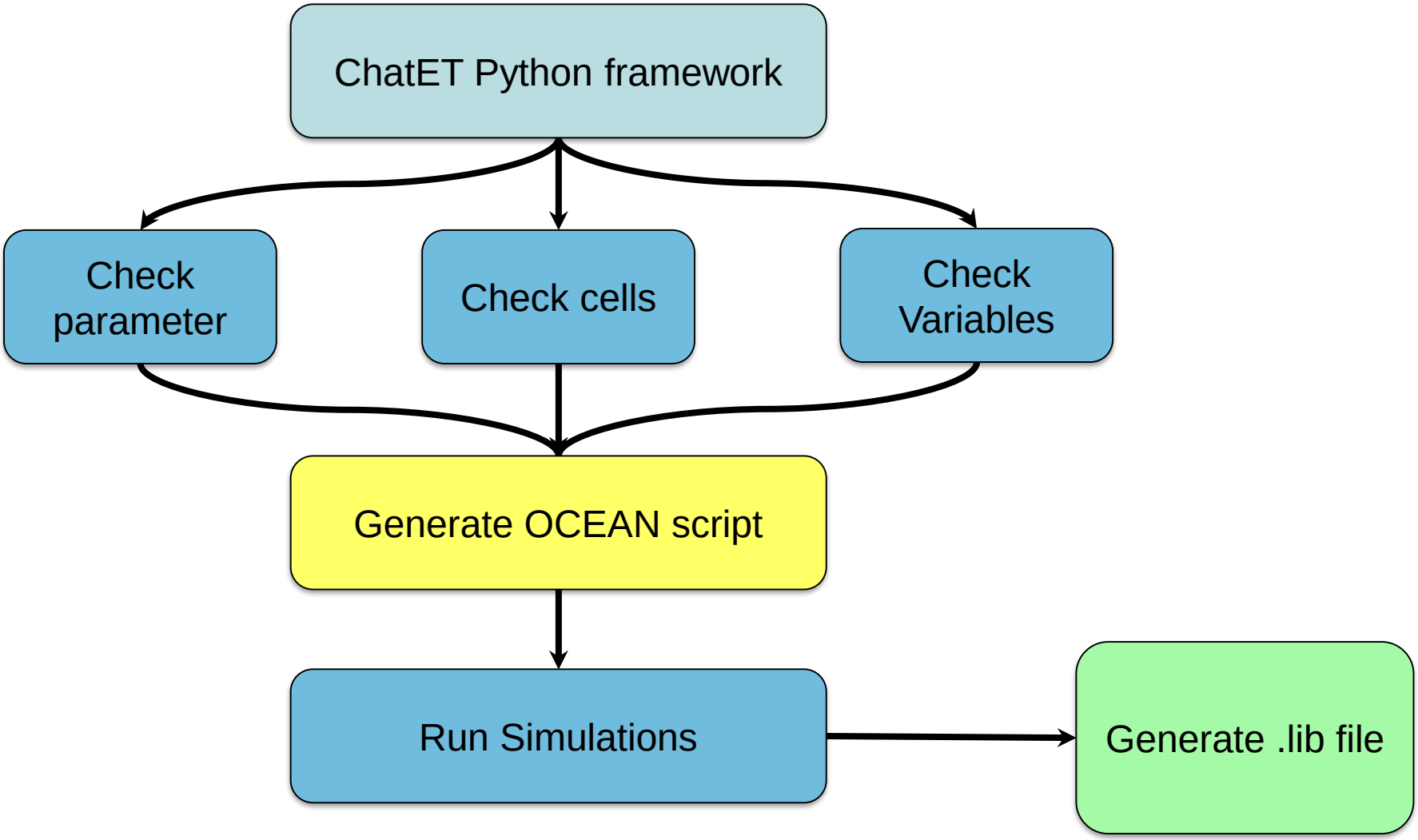
Non-volatile technologies



Main issues:

- FeFET model convergence is hard with liberate
- The 2 behaviors (characteristics) of the FeFET prevent standard analysis proposed with liberate

CharET framework proposition



Conclusion

- Up to now :

1. FeFET Design
   - Static logic gates have been designed using FeFET
   - Few and simple operation can be designed using cadence
2. Evaluation :
   - Possibility to integrate new instruction using model card to evaluate operation designed in NV-technologies

- For future :
  - Automate and make it possible to synthetize operation with FeFET (1 PhD candidate has started in October)
  - Add other evaluation in the RISC-V based platform
  - Manufacture demonstrator and interface it with our platform
  - Design other security primitives based on FeFET (1 PhD candidate has started in October)

Thank you for your attention

This work was 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.