Hardware implementation of Ascon authenticated cipher based on CMOS/STT-MRAM

CryptArchi 2022

Nathan Roussel, Olivier Potin,
Jean-Baptiste Rigaud and Jean-Max Dutertre

nathan.roussel@emse.fr

May 30 - May 31

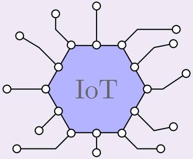
Outline

1. Introduction
    - Context
    - What is MRAM ?
    - Targeted CMOS technology
    - LightWeight Cryptography (LWC): Ascon
2. Benefits of hybridization
    - What does hybridization mean ?
    - Case 1: Sudden power failure
    - Case 2: Sleep mode
3. Non-volatile implementation of Ascon
    - What we can expect to hybridize ?
    - Flow overview
    - Non-volatile flip flop (NVFF)
    - Electrical simulation
    - Layout description
    - Liberty file
    - Logical model
    - Synthesis
    - Power estimation
4. Futur works and conclusion
5. References

Context

Context

- Tremendous growth of Internet of Things objects
- These objects must be reliable, low power consuming and secure [1]
- LightWeight Cryptography (LWC) algorithms to protect IoT
- Secure implementation of LWC to face physical attacks



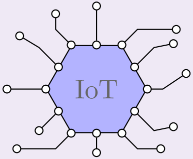
Issue

How to strengthen LWC algorithms with the lowest energy impact ?

Context

Context

- Tremendous growth of Internet of Things objects
- These objects must be reliable, low power consuming and secure [1]
- LightWeight Cryptography (LWC) algorithms to protect IoT
- Secure implementation of LWC to face physical attacks



Issue

How to strengthen LWC algorithms with the lowest energy impact ?

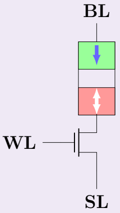
Proposal

Hardware implementation of LWC algorithm based on CMOS/STT-MRAM: MISTRAL project (ANR-19-CE39-0010) [2]

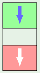
What is MRAM ?

Spin Transfer Torque MRAM (STT-MRAM)

- Magnetic Tunnel Junction (MTJ)
  - Reference Layer
  - Oxyde
  - Storage Layer (Free Layer)



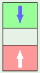
Storage



$R_P \simeq 2k\Omega$

Logic state **0**

State **P**



$R_{AP} \simeq 6k\Omega$

Logic state **1**

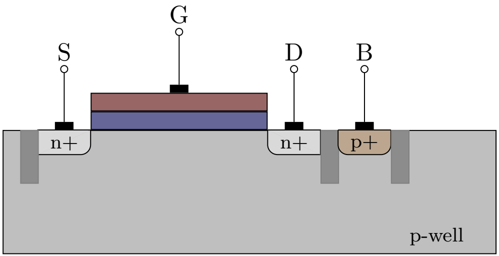
State **AP**

- P: Parallel
- AP: Anti-Parallel

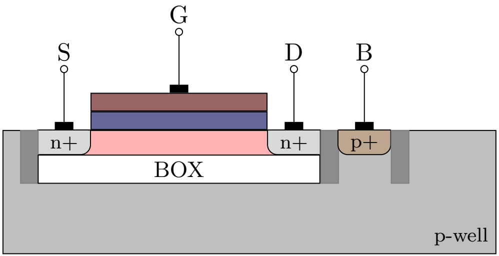
Targeted CMOS technology

CMOS technology

- Project choice: low power technology, mature node
- CMOS 28nm Fully Depleted Silicon On Insulator (FD-SOI) from STMicroelectronics [3]



Bulk



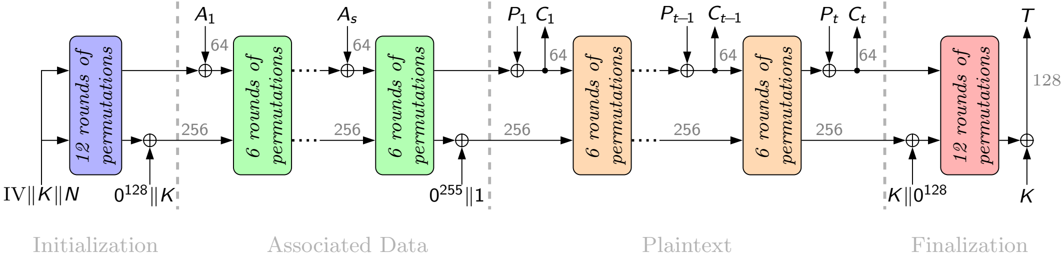
UTBB FD-SOI

LightWeight Cryptography (LWC): Ascon

Authenticated Encryption

CONFIDENTIALITY
INTEGRITY
AUTHENTIFICATION

- **Ascon**, authenticated encryption with associated data
- Part of the final phase of NIST LWC contest [4]



K: Key (**128 bits**)

N: Nonce (**128 bits**)

IV: Initialized vector (**64 bits**)

A: Associated data (Block of **64 bits**)

P: Plaintext (Block of **64 bits**)

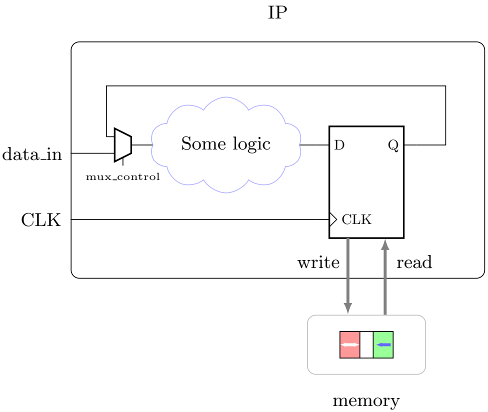
C: Ciphertext (Block of **64 bits**)

T: Tag(**128 bits**)

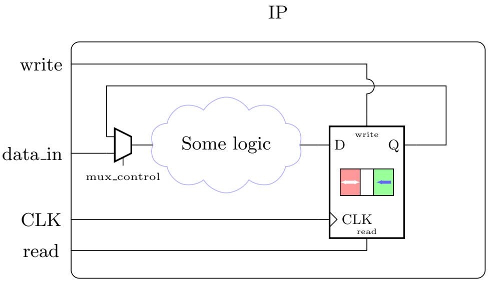
1. Introduction
    - Context
    - What is MRAM ?
    - Targeted CMOS technology
    - LightWeight Cryptography (LWC): Ascon
2. Benefits of hybridization
    - What does hybridization mean ?
    - Case 1: Sudden power failure
    - Case 2: Sleep mode
3. Non-volatile implementation of Ascon
    - What we can expect to hybridize ?
    - Flow overview
    - Non-volatile flip flop (NVFF)
    - Electrical simulation
    - Layout description
    - Liberty file
    - Logical model
    - Synthesis
    - Power estimation
4. Futur works and conclusion
5. References

What does hybridization mean ?

Classic circuit

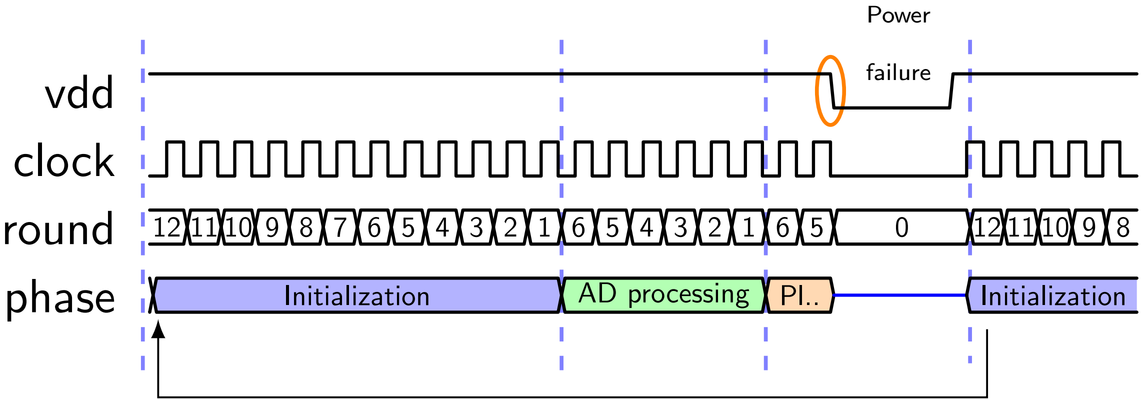


Hybridized circuit



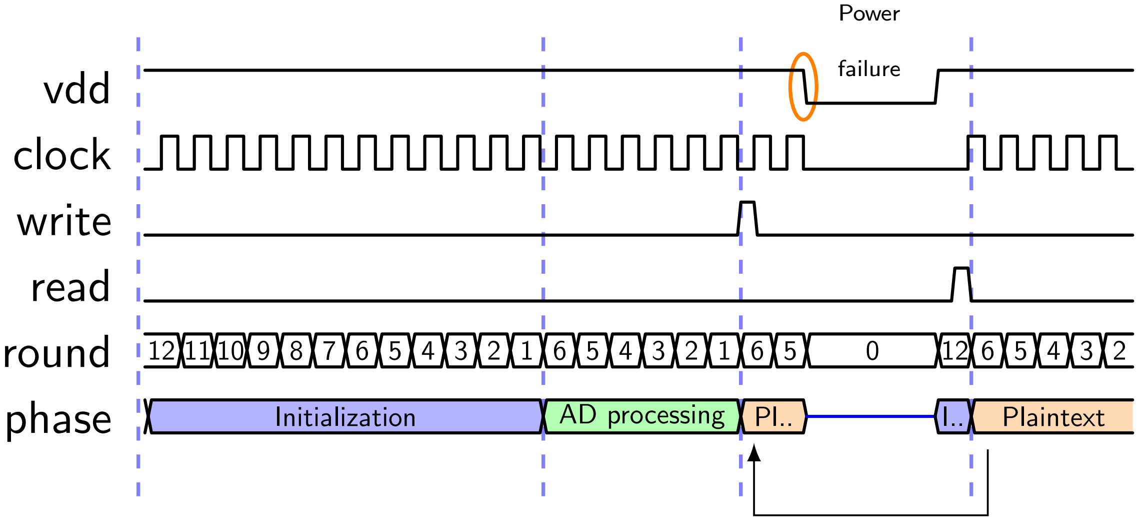
Case 1: Sudden power failure

Ascon CMOS



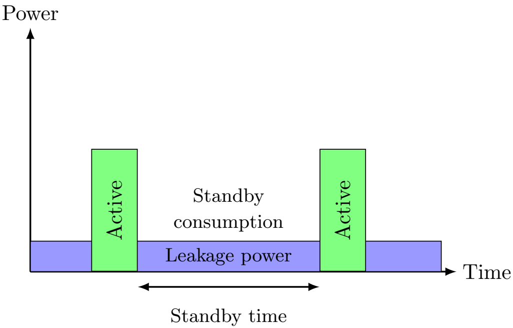
Case 1: Sudden power failure

Ascon CMOS/MRAM

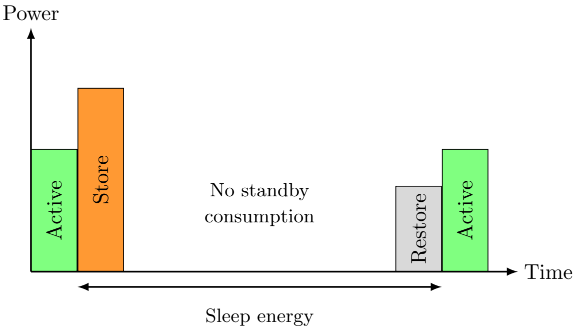


Case 2: Sleep mode

CMOS consumption

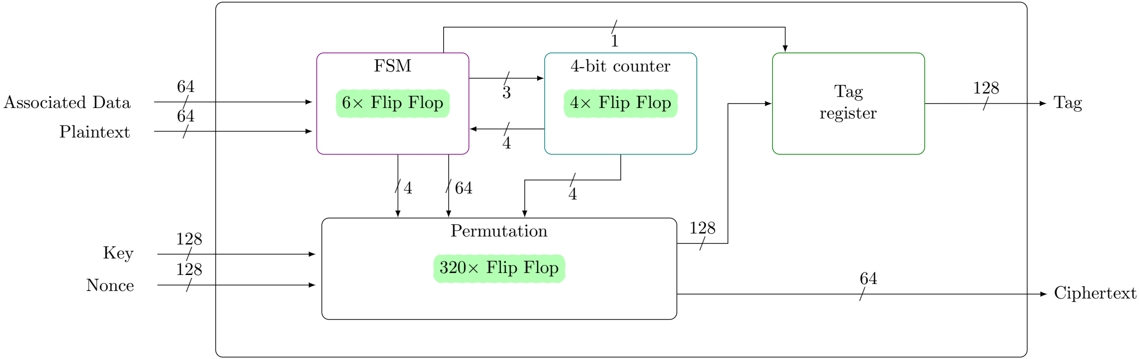


CMOS/MRAM consumption



1. Introduction
   - Context
   - What is MRAM ?
   - Targeted CMOS technology
   - LightWeight Cryptography (LWC): Ascon
2. Benefits of hybridization
   - What does hybridization mean ?
   - Case 1: Sudden power failure
   - Case 2: Sleep mode
3. Non-volatile implementation of Ascon
   - What we can expect to hybridize ?
   - Flow overview
   - Non-volatile flip flop (NVFF)
   - Electrical simulation
   - Layout description
   - Liberty file
   - Logical model
   - Synthesis
   - Power estimation
4. Futur works and conclusion
5. References

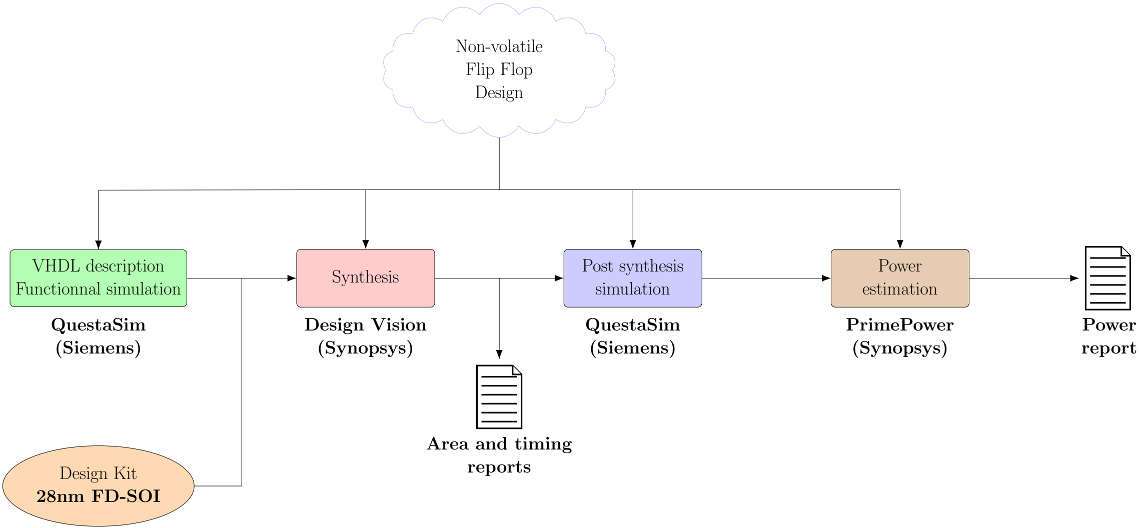
What we can expect to hybridize ?



Operating conditions

- Ascon-128 / One round computation in a single clock cycle
- Frequency 100MHz, Voltage 1V

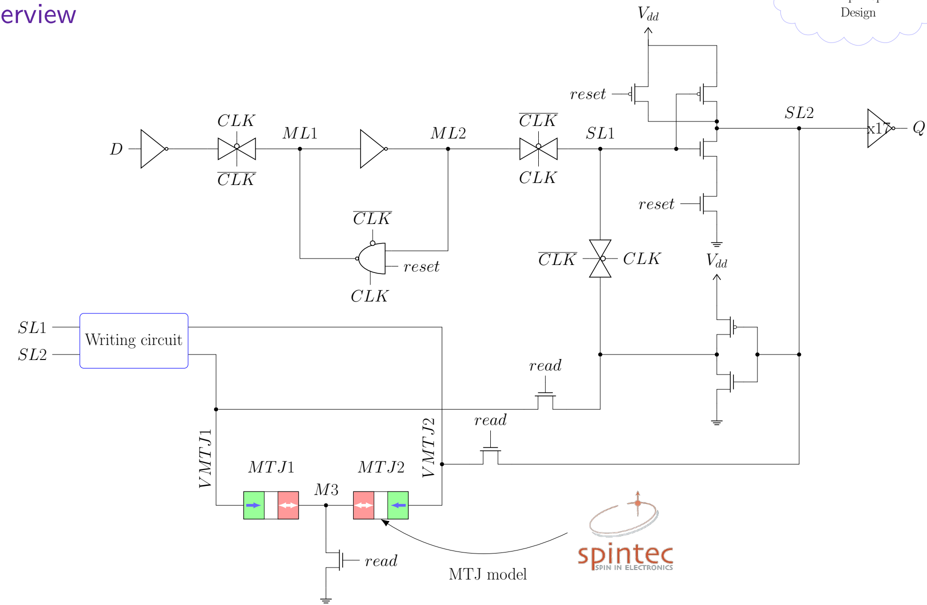
Flow overview



Non-volatile flip flop (NVFF)

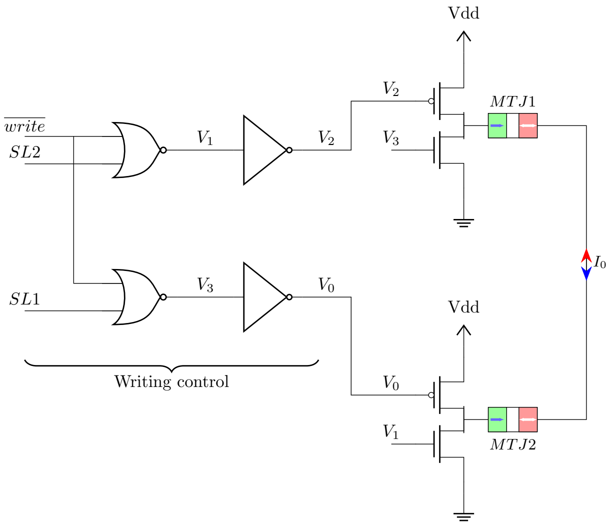
Circuit overview

Non-volatile
Flip Flop
Design

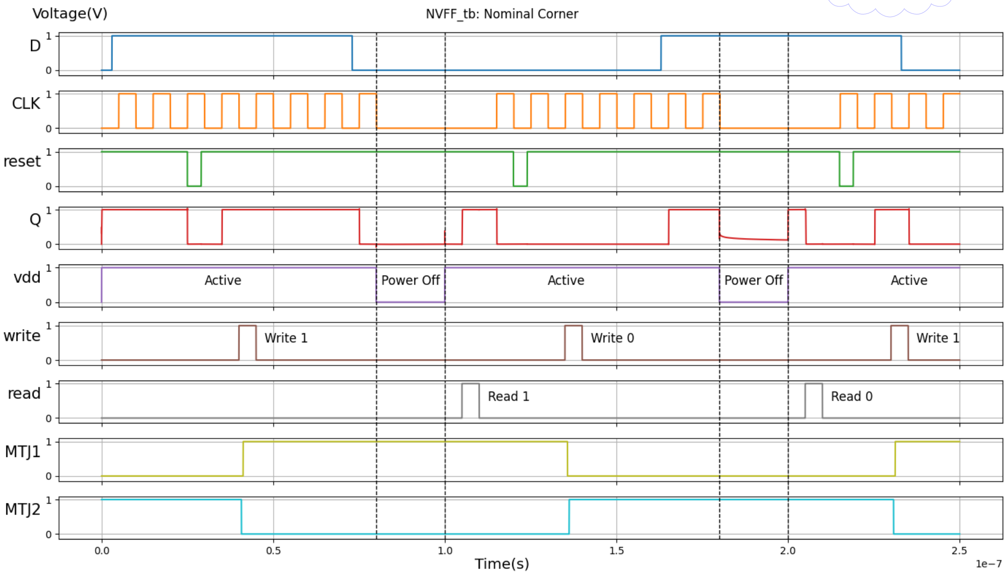


Non-volatile flip flop (NVFF)

Writing circuit



Electrical simulation



Layout description

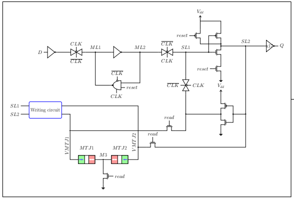
Layout considerations

- Creating the layout of non-volatile flip flop is a difficult task
- Producing a layout as optimized as the layout from ST Design Kit is impracticable at our level

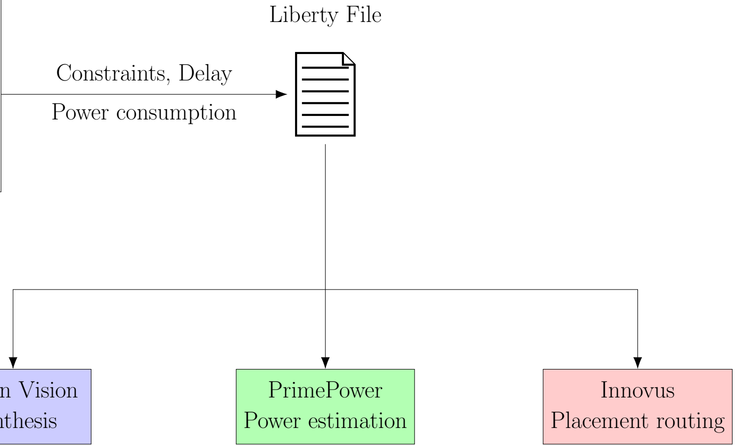
Layout specifications

- Considering non-volatile flip flop area equals to ST flip flop area $+$ 20 %
- Seems fair regarding transistor sizing

Liberty file



Non-volatile Flip Flop



Liberty File

Constraints, Delay

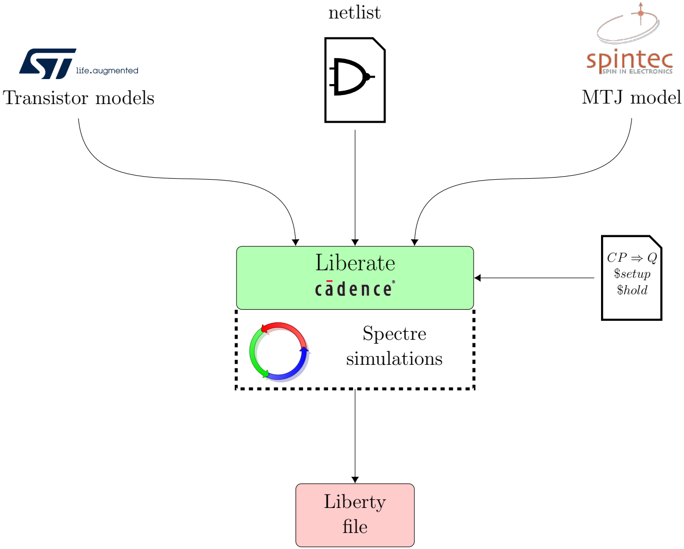
Power consumption

Design Vision
Synthesis

PrimePower
Power estimation

Innovus
Placement routing

Liberty file



Transistor models

Spectre netlist

MTJ model

Liberate
cadence

Spectre simulations

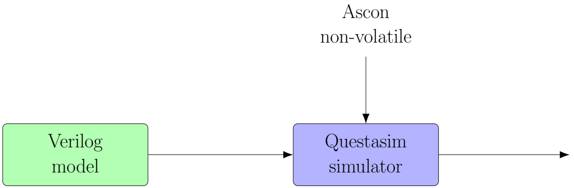
$CP \Rightarrow Q$
$\$setup$
$\$hold$

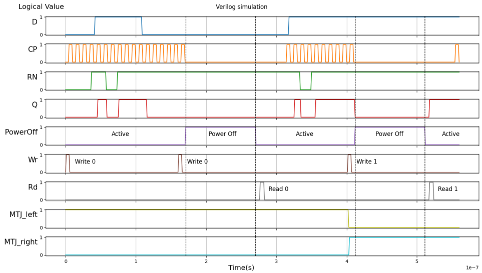
Liberty file

Logical model

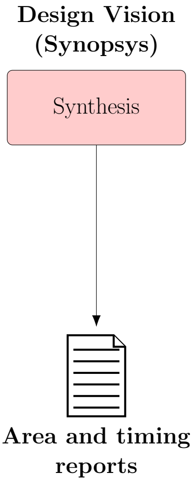
Verilog model for RTL/Post synthesis simulation

- Primitives describing the MTJ and the NVFF
- Delay/Constraint statements for SDF matching





Synthesis



Design Vision (Synopsys)

Synthesis

Area and timing reports

- No synthesis issues encountered as the liberty file is correctly generated

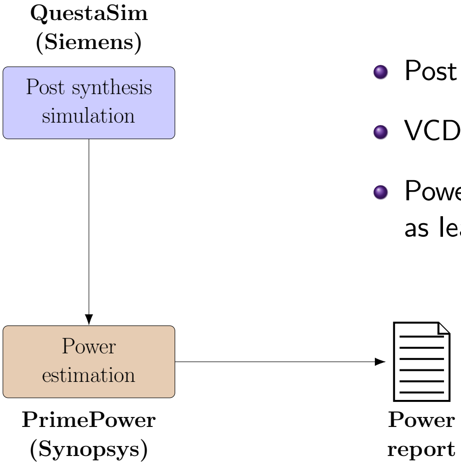
Area :

	Ascon	Ascon non-volatile
Area (μm^2):	**4970.75**	**5235.95** (×1.05)
Area (GE):	**10153**	**10694** (×1.05)

Timing :

	Ascon	Ascon non-volatile
Path Slack (ns):	**1.52**	**1.62** (×1.07)

Power estimation


QuestaSim (Siemens)

Post synthesis simulation

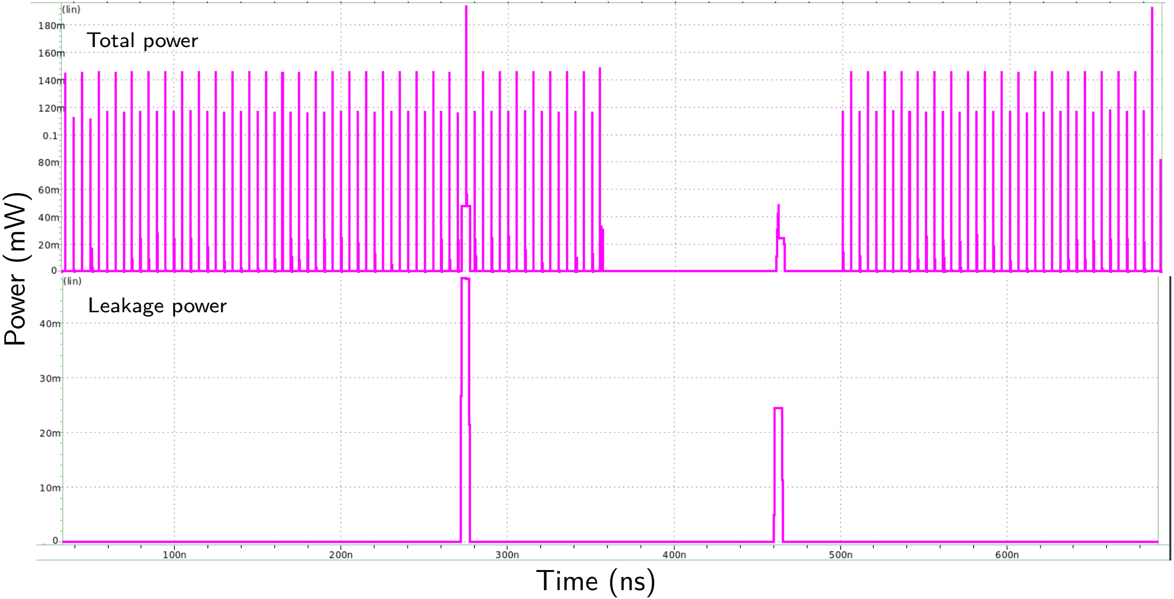
Power estimation

PrimePower (Synopsys)

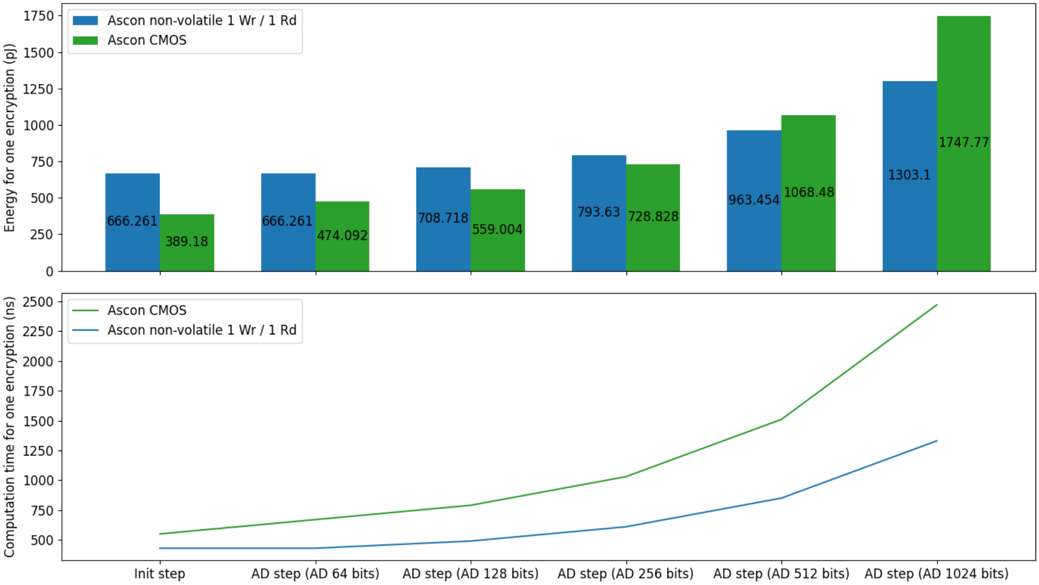
Power report

- Post synthesis simulation with SDF back-annotation
- VCD file produced by simulation tool
- Power consumption of non-volatile parts must be reported as leakage power in Liberty file

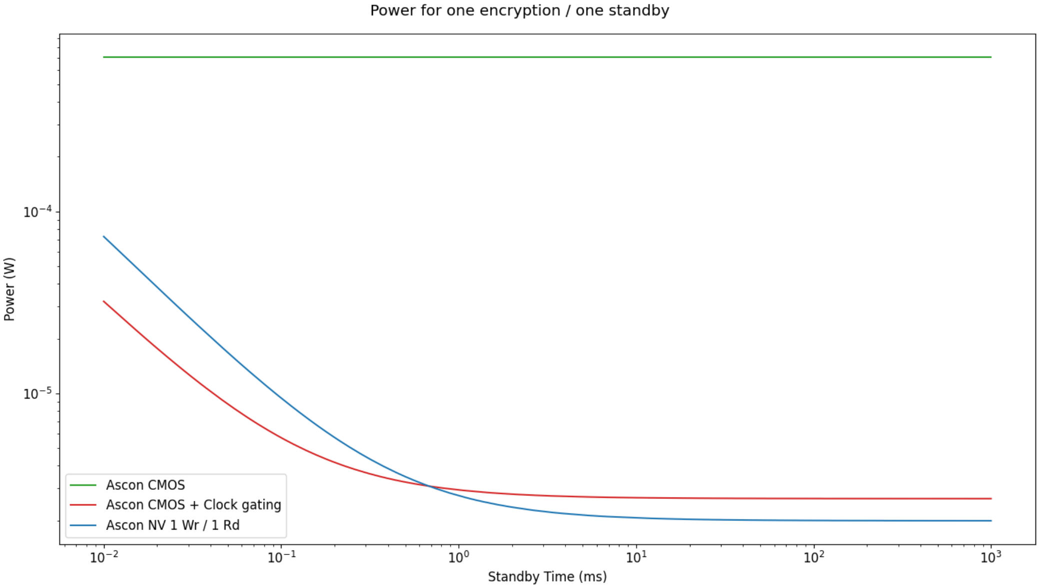
Power estimation



Case 1: Sudden power failure



Case 2: Sleep mode



1. Introduction
    - Context
    - What is MRAM ?
    - Targeted CMOS technology
    - LightWeight Cryptography (LWC): Ascon
2. Benefits of hybridization
    - What does hybridization mean ?
    - Case 1: Sudden power failure
    - Case 2: Sleep mode
3. Non-volatile implementation of Ascon
    - What we can expect to hybridize ?
    - Flow overview
    - Non-volatile flip flop (NVFF)
    - Electrical simulation
    - Layout description
    - Liberty file
    - Logical model
    - Synthesis
    - Power estimation
4. **Futur works and conclusion**
5. References

Futur works and conclusion

Conclusion

- Hardware implementation of Ascon with non-volatile flip flop
- Set up a design flow for hybridization

Futur works

- Placement routing and parasitic extraction steps
- Study the impact of non-volatile circuit for security aspects (side-channel and fault-based attacks)

1. Introduction
    - Context
    - What is MRAM ?
    - Targeted CMOS technology
    - LightWeight Cryptography (LWC): Ascon
2. Benefits of hybridization
    - What does hybridization mean ?
    - Case 1: Sudden power failure
    - Case 2: Sleep mode
3. Non-volatile implementation of Ascon
    - What we can expect to hybridize ?
    - Flow overview
    - Non-volatile flip flop (NVFF)
    - Electrical simulation
    - Layout description
    - Liberty file
    - Logical model
    - Synthesis
    - Power estimation
4. Futur works and conclusion
5. References

References I

[1] Kostas Mathioudakis et al. “Short Paper: IoT: Challenges, Projects, Architectures”. In: *2015 18th International Conference on Intelligence in Next Generation Networks*. IEEE, 2015.

[2] ANR. *Sécurisation d’algorithmes cryptographiques par hybridation MRAM/CMOS – Projet MISTRAL*. Feb. 2020. URL: https://anr.fr/Projet-ANR-19-CE39-0010.

[3] STMicroelectronics. *28nm FD-SOI Technology Catalog*.

[4] *NIST LWC*. URL: https://csrc.nist.gov/projects/lightweight-cryptography.