SEC² project

IMT –Télécom ParisTech, Mines Saint-Etienne

Jean-Luc Danger
jean-luc.danger@telecom-paristech.fr
0682035957

Targeted topics

All Topics requiring Secure and Safe embedded systems as:

SU-DS03-2019-2020: *Sub-topic 1:* Protecting citizens' security, privacy and personal data protection

SU-DS03-2019-2020: *Sub-topic 2:* Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs): defenders

SU-DS05-2018-2019: *Sub-topic a (2019):* Digital security and privacy in multimodal transport

SU-DS05-2018-2019: *Sub-topic b (2019):* Digital security and privacy in healthcare ecosystem

SU-INFRA01-2018-2019-2020: Combined physical and cyber threats

SU-INFRA02-2019: Security for smart and safe cities, including for public spaces

Institut Mines-Télécom

TELECOM ParisTech

Une école de l'IMT

Project idea: SEC²
"SECurity leveraged by Semi-Conductors"

Security and Safety are two major challenges in all future applications, but if we look at device level:

- ❑ **Attacks always improve:** cyber but also physical attacks
- ❑ **Root-of-Trust** to ensure End-to-End security must be seriously protected in the device.
- ❑ **Device Reliability** decreases in recent technologies

What can we do at device level ?

Institut Mines-Télécom

TELECOM ParisTech

Une école de l'IMT

SEC²

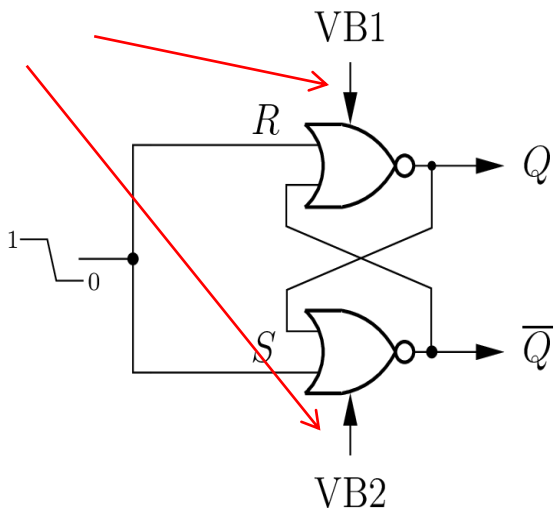
Main Goal: Deep **analyzis** of security and reliability of applications using new semiconductor technologies to propose novel **methods** and architectures **to enhance security and reliability**

Technical Objective: Use **intrinsic features** of new Semiconductors technologies like FD-SOI , MRAM, PCM Ram, 3D … to **leverage the security**, compensate reliability flaws and turn weaknesses into strength

FD-SOI new property: Back-Biasing

- BB allows to get **Steady and Unique** elements: Robust Physically Unclonable Function **PUF** as **Root of Trust**
- The other **unstable** elements: High quality **Randomness** => Robust True Random Number Generator **TRNG** for Crypto

FD-SOI Body Biasing

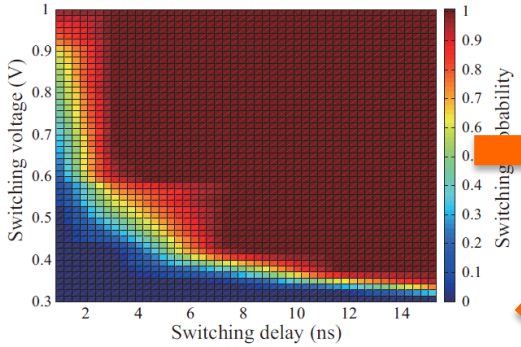


Institut Mines-Télécom

TELECOM ParisTech

Une école de l'IMT

MRAM new property: Stochastic switching behavior



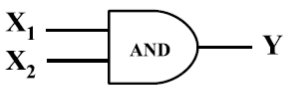
Stochastic

Unpredictable

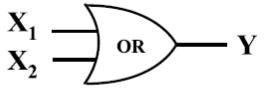
Inexact

2. Stochastic computing

X_1: 0101101100 $P_{x1} = 0.5$ X_2: 001010110 $P_{x2} = 0.4$

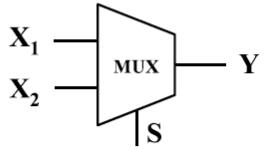


$P_Y = P_{x1} . P_{x2} = 0.2$



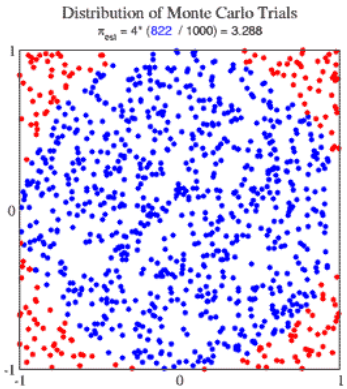
$P_Y = P_{x1} + P_{x2} - P_{x1} . P_{x2} = 0.7$

$P_Y = P_{x1} + P_{x2} - 2P_{x1} . P_{x2} = 0.5$



$P_Y = P_{x1} . P_S + P_{x2} . (1-P_S) = 0.45$

1. True random number generator



3. Approximate computing

SEC²

National Partners

Télécom ParisTech (academics)
Mines St-Etienne (academics)
ST Microelectronics (Big SC company)
Secure-IC (SME)
CEA Tech

Looking for Partners :

For security/safety use cases
International, already interested :

- TU Delft
- INL Braga

Looking for relevant H2020 calls :

SEC² is basically a technological subject which could be part of an applicative H2020 project