MISTRAL

Sécurisation d'algorithmes cryptographiques par hybridation MRAM/CMOS

anr agence nationale de la recherche

Appel : AAPG

Année : 2019

Instrument : PRC

Contact : rigaud@emse.fr

COORDINATEUR : Jean-Baptiste Rigaud

PARTENAIRES :
CEA-LETI/ IM2NP / Mines Saint-Étienne / SPINTEC

Résumé :
Le projet MISTRAL propose un approche innovante d'hybridation MRAM/CMOS pour la sécurisation des algorithmes de cryptographie légère face aux attaques matérielles.

CONTEXTE ET OBJECTIFS

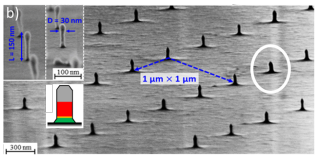
Les objets connectés ont été, jusqu'à présent, conçus avec de fortes contraintes en consommation et en coût. La sécurité des objets de l'IoT devient une problématique majeure. Pour y remédier, des solutions comme la cryptographie légère (LWC) et le développement de contre-mesures doivent être implantés afin de combler l'écart entre les besoins en sécurité et les contraintes de coût et de consommation.

MÉTHODOLOGIE

- Nano-fabrication de cellules STT-MRAM durcies contre injection laser et EM.
- Caractérisations (électrique et sécuritaire) et modélisation des effets pour adapter le flot de simulation.
- Spécification de protections contre les attaques en fautes tirant bénéfice de l'hybridation CMOS/MRAM pour des algorithmes de cryptographie légère (LWC).
- Conception jusqu'au placement-routage de différentes versions (CMOS, hybridé, robuste) d'un algorithme cible.
- Caractérisations par simulation (consommation et sécuritaire) pour quantifier l'apport des solutions proposées.

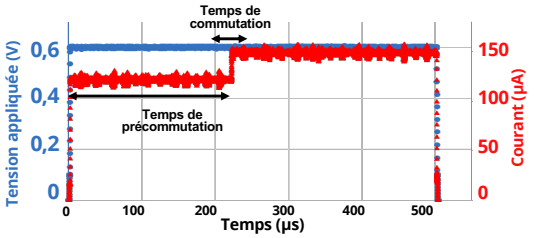
RÉSULTATS

- Fourniture et caractérisation électrique d'un premier lot de dispositifs élémentaires STT-MRAM.



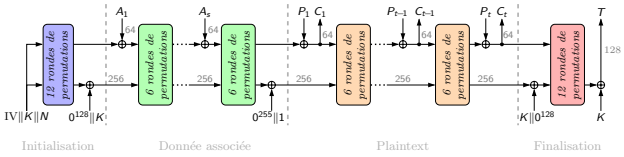
Nano-fabrication de réseau de Jonctions Tunnel Magnétiques à couple de transfert de spin (STT-MTJ)

- Acquisition dynamique de la commutation d'état.
- Modélisation de la dépendance des temps de précommutation et de commutation avec la tension appliquée et avec le diamètre de la JTM.



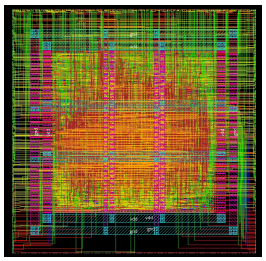
Acquisition dynamique de la commutation d'état d'une MTJ

- Choix de ASCON, finaliste du concours NIST sur la LWC, comme algorithme de référence.



ASCON-128 : chiffrement authentifié avec données associées

- Conception de la version CMOS de référence (28nm de STM). Analyse de consommation associée.
- Mise en œuvre d'une attaque SIFA sur le circuit placé-routé.



Vue *layout* du circuit ASCON (5000 μm^2, 790 μW)

DISSEMINATION

- Communications relatives au projet MISTRAL sur le site: https://mistral.wp.imt.fr

PERSPECTIVES

- Injection laser sur les cellules STT-MRAM
- Hybridation du circuit ASCON

leti ceatech — im2np — MINES Saint-Étienne, Une école de l'IMT — spintec SPIN IN ELECTRONICS