Modification Non Invasive de circuits intégrés avec des rayons X (MITIX)

Appel : ANR-20-CE39-0012

Année : 2020

Instrument : ESRF

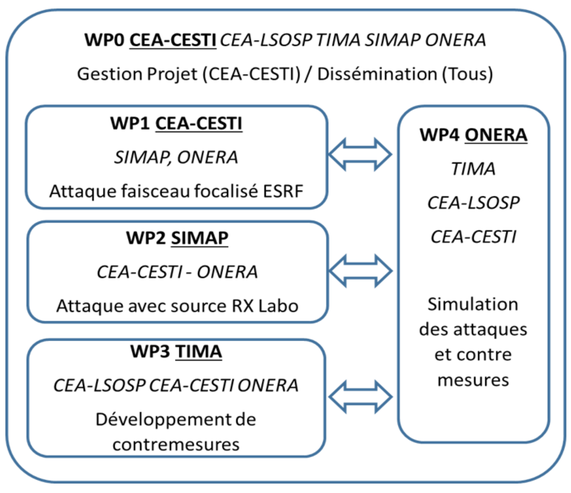
COORDINATEUR : Stéphanie Anceau

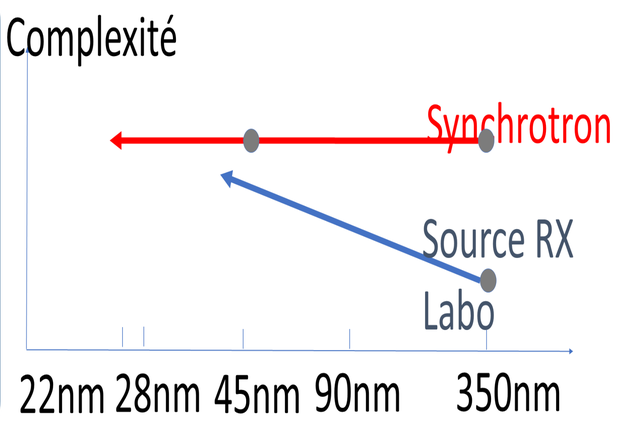
PARTENAIRES : CESTI, LSCO du CEA LETI, SIMAP, TIMA de l'UGA et L'ONERA

Afin d'évaluer le niveau de sécurité des composants en conservant toujours leur avance sur les fraudeurs, les ingénieurs et chercheurs sont en recherche constante de nouvelles techniques d'attaques. Récemment, les chercheurs du CESTI-LETI et du SIMAP ont exploré une nouvelle approche pour perturber des circuits électroniques avec un faisceau de rayons X nano-focalisé au synchrotron et sur un générateur de rayons X de laboratoire.

CONTEXTE ET OBJECTIFS

L'objectif de ce projet est de démontrer la pertinence des attaques de circuits intégrés par rayons X sur des technologies plus avancées, soit en utilisant un rayonnement synchrotron, soit avec des moyens d'attaques plus accessibles tels que des sources de rayons X de laboratoire. La simulation et la modélisation des mécanismes mis en œuvre permettront dans le cadre de ce projet le développement des contre-mesures logicielles et matérielles adéquates qui seront testées expérimentalement.





MÉTHODOLOGIE ET RÉSULTATS

Ci-dessous sont présentées les avancées du projets en fonction des WP. Comme prévu dans le planning le WP1 et WP2 ont bien commencé leurs tâches et les WP3 et WP4 sont en ordre de marche pour 2022 : le recrutement du thésard et du post doc ayant pris un peu plus de temps que prévu. Il reste l'accord de consortium à finaliser ainsi qu'un accord d'agrément pour le WP4. L'ensemble des recrutements prévus sont maintenant finalisés.

WP0 : CEA CESTI

- Mise en place d'un site web ANR
- Mise en place d'un espace de travail partagé sécurisé (tuleap)
- Rédaction de l'accord de consortium (en cours de finalisation)
- Réunion avec tous les partenaires
- Réunion avec certains partenaires

WP1 : CEA CESTI

- Recrutement ingénieur + stagiaire
- Choix des composants
- Préparation pour attaque
- Réflexion sur les expériences à l'ESRF ID16B : choix des créneaux
- Passage des programmes informatiques de contrôle VB à python
- Test programme sur composants

WP2 : SIMAP/ CEA CESTI

- Recrutement ingénieur
- Caractérisation du spectre de RX
- Réalisation des caches fixes sur ATMEGA
- Réalisation des caches amovibles pour ATMEGA et STM32
- Centrage des caches amovibles Attaques sur ATMEGA et STM32
- Publication dans CARDIS

WP3 : CEA LSCO / TIMA

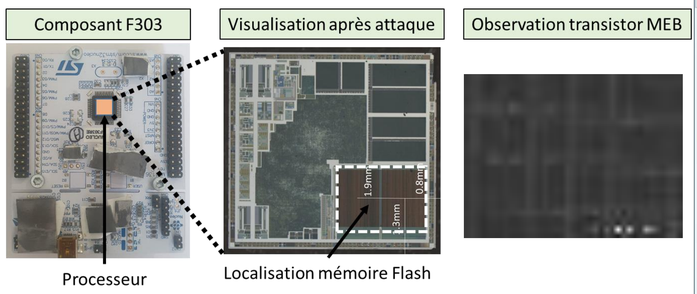
- Début du travail sur les contremesures matérielles
- Recrutement thésard (janv 2022)

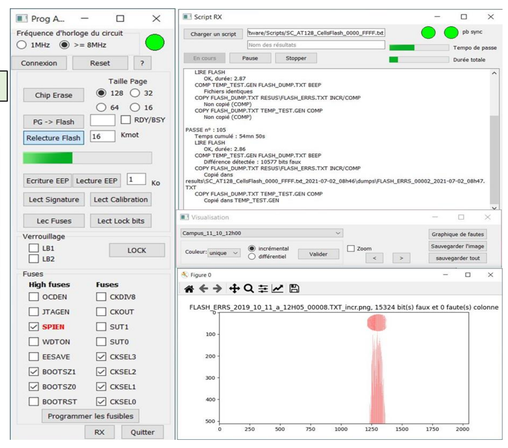
WP4 : ONERA / TIMA / CEA CESTI

- Négociation d'un accord d'agrément
- Recrutement post doc en cours
- Recrutement thésard (janv 2022)

Détail WP1 et WP2

Choix des composants MCU et préparation pour attaque: en plus des composants ATMEGA, nous avons opté pour des composants de la famille STM32. Nous avons pu identifier les zones d'intérêt (FLASH, RAM, Glue Logique) par préparation chimique et observation au MEB comme indiqué ci-dessous sur le composant F303. L'interface de programmation en python a été développée pour l'attaque des composants ATMEGA et STM32 dans la mémoire flash et la RAM. Une cartographie des fautes sur l'ATMEGA a pu être obtenue.

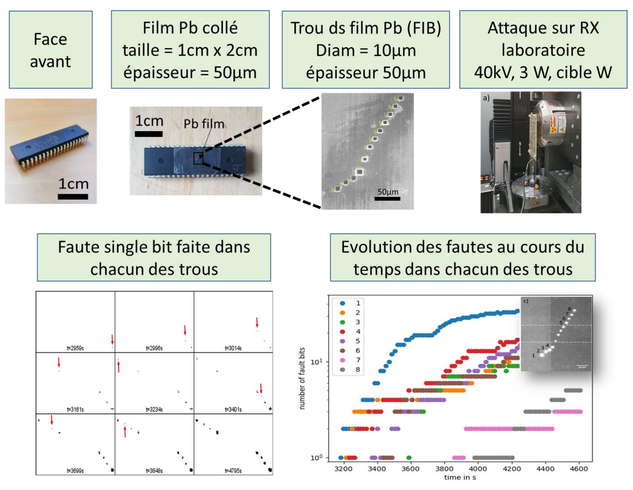


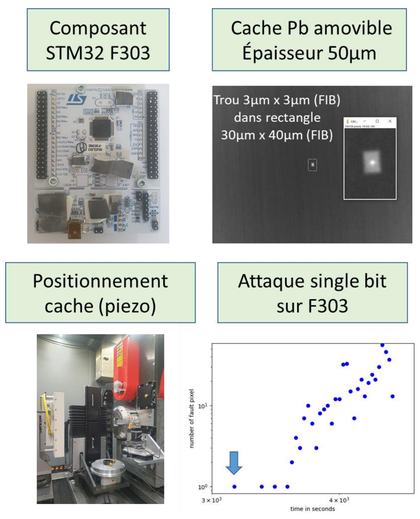


Dans le futur : cartographie mémoire FLASH (STM32), choix des composants les plus adaptés pour les expérience à l'ESRF sur ID16B.

Détail WP1 et WP2

Le spectre des rayons X de la source a été déterminé à l'aide d'un spectromètre et trouvé les bonnes conditions d'attaque (tension, courant, cible) sur les ATMEGA et STM32 F303. Des attaques en face arrière et face avant ont pu être mises en place sur les ATMEGA et ainsi que des attaques avec cache amovible sur les F303.





Publications : présentation orale et article dans CARDIS 2021

Dans le futur : attaque sur technologies avancées (90nm et 45 nm) avec cache fixe et amovible dans la FLASH . Attaque localisée dans la RAM et la Glue logique.