SCATTER

1- Résumé du Projet

Ce projet consiste en une étude de recherche et développement dans le domaine de la sécurité des implémentations cryptographiques, et plus précisément dans le domaine des attaques par canaux auxiliaires.

Nom	Développement d'une librairie d'analyse d'algorithmes de cryptographie
Acronyme	SCATTER
Porteur	Eshard (<20 salariés) - Hugues THIEBEAULD (Président)
Date	Mai 2018 à Mai 2020
Consortium	Eshard - XLIM (Université de Limoges)
Financement	DGA RAPID (Régime d'appui aux PME pour l'innovation duale)
TRL	6 - Prototype ou modèle de la technologie (sous-)système fonctionnant en environnement représentatif

Cette étude va permettre d'étudier en profondeur une nouvelle technique d'attaque, visant à retrouver un secret au sein de mesures physiques sans savoir exactement quand il est manipulé par l'appareil ciblé. Cela s'applique donc à tout algorithme de cryptographie présent dans un élément embarqué (puce sécurisée, objet communiquant, etc.). Un des objectifs principaux est de mettre en place une libraire d'analyse pour évaluer de façon efficace la sécurité des implémentations cryptographiques face à cette menace. Cela permettra d'évaluer l'impact de la nouvelle attaque sur les produits existants. Ensuite, des travaux seront menés pour créer des contremesures et développer une implémentation de référence d'algorithmes résistants. Ces travaux concerneront les industries pour lesquelles la sécurité embarquée est essentielle : le paiement, la défense, le contenu sécurisé, l'internet des objets…

2- Verrous Technologiques Sous-jacents

Les principaux verrous technologiques sont bien identifiés:

- **L'impact de la technique :** être en mesure d'estimer la menace que représente l'attaque sur la sécurité de produits jusqu'alors résistants.
- **Le caractère innovant :** s'assurer que les technologies développées ne font pas partiellement partie d'un état de l'art existant.
- **Les contremesures :** trouver les bonnes protections algorithmiques pour se prémunir contre les nouvelles attaques.
- **Les performances du logiciel :** l'attaque doit s'exécuter de façon rapide et efficace.

3- Pistes de Recherche et Méthodologie

Afin de bien étudier l'impact réel sur différentes produits, le premier lot de ce projet de recherche se focalise sur l'analyse d'impact sur un panel de produits. L'objectif est de comparer notre méthode à d'autres techniques existantes.

Par ailleurs un travail de formalisation mathématique et statistique doit être mené afin de mieux comprendre les nouveaux aspects apportés par la technique. Ce travail de recherche devrait permettre par la suite d'en améliorer les performances, ainsi que d'aboutir sur des contremesures spécifiques.