

Cahier des charges relatif au travail de fin d'études de

Thomas ANIZET, inscrit en 2^{ème} Master, orientation électronique

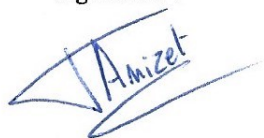
- Année académique : 2018-2019
- Titre provisoire : Contre-mesure pour les attaques par canaux cachés
- Objectifs à atteindre :
Étant un acteur majeur dans le domaine de la *Défense*, Thales collabore étroitement avec de nombreux gouvernements. La *cybersécurité* est au centre des préoccupations actuelles. Le besoin en implémentations sécurisées se fait donc de plus en plus ressentir. L'objectif est de se prémunir contre des attaques classiques et des attaques plus bas niveau exploitant des caractéristiques physiques. Afin de se familiariser avec ce domaine, l'étudiant devra réaliser une recherche bibliographique de règles de bonnes pratiques pour de la programmation sécurisée hardware. Après en avoir étudié les tenants et aboutissants, l'étudiant réalisera (i) **une série de démonstrateurs permettant de mettre en évidence l'impact des failles non traitées** et (ii) **le gain en sécurité dû aux contre-mesures**.
- Principales étapes :
 - Recherches bibliographiques de règles de bonnes pratiques.
 - Implémentation de l'algorithme AES sur FPGA.
 - Réalisation d'une attaque CPA (*Correlation Power Analysis*).
 - Étude et choix de métrique(s) pour l'analyse de contre-mesures.
 - Développement d'une contre-mesure.
 - Analyse et conclusion sur la contre-mesure développée.

Fait en trois exemplaires à Tubize, le 22 Novembre 2018

L'étudiant

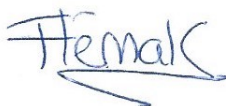
Nom – Prénom :
ANIZET Thomas

Signature :



Le tuteur

Nom – Prénom :
FLÉMAL CLÉMENTCE
Département/Unité :
Électronique
Signature :



Le promoteur

Nom – Prénom :
LERMAN Liran
Société :
Thales
Signature :

