AVIS DE SOUTENANCE DE THESE
DE DOCTORAT

Le **11-04-2017**
A **10h** Amphi

Centre Microélectronique de Provence Georges
880 route de Mimet
13120 Gardanne

Soutiendra en vue de l'obtention du titre de Docteur de l'Ecole Nationale Supérieure des Mines de Saint-Etienne dans la spécialité : MICROELECTRONIQUE

Ibrahima **DIOP**

Une thèse ayant pour sujet :

Méthodologie et outils pour la mise en pratique des attaques par collision et attaques horizontales sur l'exponentiation modulaire.

MEMBRES DU JURY :

Président
(Le président est désigné le jour de la soutenance)

Rapporteurs :

CLAVIER	Christophe	Professeur	Université de Limoges
LEVEUGLE	Régis	Professeur	Grenoble INP - Phelma

Examinateurs :

GUILLEY	Sylvain	Full professor	TELECOM-ParisTech
LINGE	Yanis	Docteur/Cryptologue	STMicroelectronics
LIARDET	Pierre-Yvan	Expert en Cryptologie	STMicroelectronics
MAURINE	Philippe	Maitre de Conferences	Université Montpellier 2

Thèse préparée dans le centre CMP-GC à l'Ecole Nationale Supérieure des Mines de Saint-Etienne.
Travail co-encadré par : MAURINE Philippe

LIARDET Pierre-Yvan

Destinataires : DR, Accueil, SCIDEM, DREC, Centre,
D.CORTIAL « Le Progrès », 24 rue de la robotique – 42000 Saint-Etienne

Résumé :

Dans cette thèse, nous étudions deux sous-familles d'attaques par canaux cachés sur l'exponentiation modulaire appelées respectivement attaques par collision et attaques horizontales.

Cette étude est faite selon deux axes : leurs mises en pratique et les possibles contremesures.

Dans un premier temps, nous étudions les attaques par canaux cachés sur un simulateur développé.

Ce simulateur permet de vérifier la bonne implémentation d'une attaque avant sa mise en pratique dans un environnement réel.

Dans un deuxième temps, nous étudions les attaques par collision dans un environnement réel.

Pour cela, nous nous sommes intéressés à l'automatisation de la détection effective de collision.

Ainsi, nous proposons un nouveau critère de détection de collision.

Dans un troisième temps, nous étudions l'estimation du rapport signal à bruit d'un jeu de traces dans le contexte des attaques par canaux cachés.

Ainsi, nous proposons une nouvelle façon d'estimer le rapport signal à bruit lors d'une attaque par canaux cachés.

En outre, nous montrons que cette estimation du rapport signal à bruit peut être exploitée pour l'analyse des fuites mais aussi pour effectuer un filtrage adaptatif.

Dans un quatrième temps, au travers d'une étude détaillée des principales étapes d'une attaque horizontale, nous montrons les problèmes pouvant intervenir dans la pratique et comment les résoudre.

Nous proposons finalement de possibles contremesures aux attaques horizontales.

Ibrahima DIOP