AVIS DE SOUTENANCE DE THESE
DE DOCTORAT

Le **22-11-2019**
A **14h** Amphi Salle Minatec

CEA Grenoble
17 rue des Martyrs
38054 Grenoble

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

Antoine **LOISEAU**

Une thèse ayant pour sujet :

Implémentation légère et sécurisée pour la cryptographie sur courbes elliptiques pour l'IoT

MEMBRES DU JURY :

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

Rapporteurs :

Quisquater	Jean-Jacques	Professeur émérite	Ecole Polytechnique de Louvain
Goubin	Louis	Professeur	Université de Versailles

Examinateurs :

Fournier	Jacques	HDR	CEA Leti
Vitse	Vanessa	Maître de Conférence	Université de Grenoble
Clavier	Christophe	Professeur	Université de Limoges
Tria	Assia	HDR	CEA Leti

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

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

Résumé

Cette thèse traite des problématiques relatives aux implémentations de la cryptographie sur les courbes elliptiques dans un environnement contraint tel que l'Internet des Objets (IoT).

Les courbes elliptiques sont largement déployées au sein d'applications cryptographiques. Ces implémentations sont généralement basées sur le standard du NIST. Cependant, de nombreuses avancées en termes de performance et de sécurité ont été faites depuis l'élaboration de ce standard.

Nous nous proposons dans cette thèse de construire un nouvel ensemble de courbes elliptiques pour le modèle de courbes binaires d'Edwards. Ces nouvelles courbes intégreront dès leur conception un certain nombre d'optimisations. L'efficacité de ce modèle de courbes réside dans l'utilisation de coordonnées différentielles. Cependant, nous verrons que cette représentation est difficilement intégrable au sein des protocoles de signatures. Nous proposerons alors deux solutions pour pallier à cette problématique.

Par ailleurs, les contraintes fortes en termes de sécurité face aux attaques par canaux auxiliaires nous mèneront à l'évaluation de notre implémentation face à un ensemble d'attaques physiques. De cette étude, nous proposerons une nouvelle attaque physique mêlant attaque par faute et attaque par canaux auxiliaires.

Les attaques par profilages feront l'objet d'une étude particulière. Nous montrerons comment nous pouvons utiliser ces attaques pour retrouver une clef en une seule trace d'attaque, malgré l'utilisation de contremesures. Pour cela, nous utiliserons les méthodes de réduction de dimensions (PCA, LDA). Nous proposerons alors une nouvelle contremesure pour se prémunir de ce genre d'attaque.

Antoine LOISEAU, CMP