AVIS DE SOUTENANCE DE THESE
DE DOCTORAT

Le **18-10-2018**
A **10h30** Amphi HS002 (GCP)

Campus Georges Charpak Provence
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

Benjamin **LAC**

Une thèse ayant pour sujet :

Cryptographie légère intrinsèquement résistante aux attaques physiques pour l'Internet des objets.

MEMBRES DU JURY :

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

Rapporteurs :

Clavier	Christophe	Professeur	Univ. de Limoges
Standaert	François-Xavier	Professeur	Univ. catholique de Louvain

Examinateurs :

Bossuet	Lilian	Professeur	Univ. Jean Monnet
Gérard	Benoît	Ingénieur	Dir. générale de l'armement
Goubin	Louis	Professeur	Univ. de Versailles
Canteaut	Anne	Dir. de recherche	INRIA
Fournier	Jacques	Resp. scientifique	CEA Grenoble
Sirdey	Renaud	Dir. de recherche	CEA Grenoble

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

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

Résumé

L'Internet des objets a de nombreux domaines applicatifs et offre ainsi un potentiel immense pour les entreprises, les industries et les utilisateurs.

Notre étude porte sur les besoins en cryptographie et les enjeux de sécurité des objets connectés, dont les particularités sont à la fois le nombre important de données qu'ils manipulent, et le fait qu'ils soient souvent en milieu hostile, accessibles physiquement à tout type d'attaquant potentiel.

Les attaques par observation et par perturbation sont les deux principales catégories d'attaques physiques.

Dans nos travaux de recherche, nous analysons ces différentes techniques d'attaques et les contre-mesures existantes, et nous introduisons deux nouveaux chemins d'attaques que nous avons validés expérimentalement en laboratoire sur une famille récente de chiffrements symétriques : les structures entrelacées.

Afin de répondre aux besoins en matière de sécurité et aux fortes contraintes de performances des objets connectés, nous proposons une nouvelle contre-mesure logicielle générique basée sur la redondance que nous avons nommée l'IRC.

Nous étudions donc le déploiement de l'IRC sur les schémas de chiffrement existants, et sa résistance face aux attaques physiques.

Finalement, nous introduisons GARFIELD : un nouveau chiffrement par blocs à bas coût adapté à l'IRC pour assurer un bon compromis entre sécurité et performance.

Nous vérifions sa résistance aux attaques mathématiques classiques et nous proposons des implémentations avec différents niveaux de sécurité face aux attaques physiques, pour les applications de l'Internet des objets, dont nous analysons les performances et la validité en pratique.

Benjamin LAC, CMP