# AVIS DE SOUTENANCE DE THESE
# DE DOCTORAT

Le **30-10-2019**
A **14h** Amphi HS01

Campus George Charpak Provence
880 Route de Mimet
13541 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

**Amina** **BEL KORCHI**

Une thèse ayant pour sujet :

Déploiement de la cryptographie homomorphe dans le cadre de l?IoT

**MEMBRES DU JURY** :

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

**Rapporteurs** :

| | | | |
|---|---|---|---|
| Cuppens | Nora | DR | IMT Atlantique - Mines Telecom |
| Urien | Pascal | Professeur | Telecom Paris Tech |

**Examinateurs** :

| | | | |
|---|---|---|---|
| EL MRABET | Nadia | Mcf - HDR | Campus George Charpak Provence |
| Tisot | Serge | Ingénieur | Kontron |
| Guilley | Sylvain | Pr | Telecom Paris Tech |

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

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

## Résumé

La technologie émergente des appareils mobiles permet aux utilisateurs d'accéder à un large éventail d'applications grâce à la connexion internet.

Comme ces applications exigent une puissance de calcul considérable, elles représentent un défi pour les appareils dont la puissance de calcul, la mémoire, le stockage et l'énergie sont limités. Cependant, un tel défi pourrait être surmonté par le cloud computing car celui-ci offre des ressources dynamiques pratiquement illimitées pour le traitement et le stockage des données.

Néanmoins, les utilisateurs mobiles hésitent encore à adopter cette technologie car les schémas de chiffrement classiques exigent le déchiffrement des données pour pouvoir être traités.

La cryptographie homomorphe est une solution potentielle pour permettre un calcul arbitraire des données chiffrées sans avoir à les déchiffrer. En pratique, le cloud peut calculer la somme et/ou le produit des textes chiffrés.

Le résultat est envoyé à l'émetteur qui peut déchiffrer avec sa clé secrète. Bien que la cryptographie homomorphe soit considérée comme une solution pour permettre d'effectuer des calculs sécurisés, son efficacité reste un obstacle à sa mise en œuvre.

L'inconvénient des schémas de chiffrement homomorphe est la taille des textes chiffrés.

L'objectif de cette thèse est d'appliquer un schéma de chiffrement homomorphe dans un cas d'usage industriel lié à l'IoT, afin de réaliser une implémentation efficace et optimale d'un protocole homomorphe.



**Amina Bel Korchi**