UNIVERSITE CLAUDE BERNARD – LYON I

DIPLÔME NATIONAL DE DOCTORAT (Arrêté du 25 mai 2016)

Date de la soutenance : **27 Janvier 2017**

Nom de famille et prénom de l'auteur : **Marie PAINDAVOINE**

Titre de la thèse : « Méthodes de Calculs sur les données chiffrées. »

RESUME DE LA THESE

L'annonce de l'essor du chiffrement des données se heurte à celle de l'avènement du « big data ». Il n'est maintenant plus suffisant d'envoyer et de recevoir des données, il faut pouvoir les analyser, les exploiter ou encore les partager à grande échelle. Or, les données à protéger sont de plus en plus nombreuses, notamment avec la prise de conscience de l'impact qu'ont les nouvelles technologies (smartphones, internet of things, cloud, …) sur la vie privée des utilisateurs. En rendant ces données inaccessibles, le chiffrement bloque a priori les fonctionnalités auxquelles les utilisateurs et les fournisseurs de service sont habitués. Pour rétablir ces fonctionnalités, il est nécessaire de savoir calculer des fonctions de données chiffrées, et cette thèse explore plusieurs pistes dans ce sens.

Dans une première partie, nous nous intéressons au chiffrement totalement homomorphe qui permet de réaliser des calculs arbitraires sur les données chiffrées. Ce type de chiffrement est cependant particulièrement coûteux, notamment à cause de l'appel souvent nécessaire à une procédure très coûteuse : le réamorçage. Nous prouvons ici que minimiser le nombre de réamorçages est un problème NP-complet et donnons une méthode pratique pour approximer ce minimum.

Dans une seconde partie, nous étudions des schémas dédiés à une fonctionnalité donnée. Le premier cas d'usage considéré est celui de la déduplication vérifiable de données chiffrées. Il s'agit pour un serveur de stockage externe d'être assuré qu'il ne conserve qu'un seul exemplaire de chaque fichier, même si ceux-ci sont chiffrés, ce qui lui permet d'optimiser l'usage de ses ressources mémoires. Ensuite, nous proposons un schéma de chiffrement cherchable permettant de détecter des intrusions dans un réseau de télécommunications chiffrés. En effet, le travail d'inspection du réseau par des moteurs d'analyse est actuellement entravé par la croissance du trafic chiffré. Les résultats obtenus permettent ainsi d'assurer la confidentialité des échanges tout en garantissant l'absence d'intrusions malveillantes dans le trafic.