DIPLÔME NATIONAL DE DOCTORAT

(Arrêté du 25 mai 2016)

Date de la soutenance : **09 juillet 2021**

Nom de famille et prénom de l'auteur : **Monsieur HAMDI Adel**

Titre de la thèse : *Chiffrement fonctionnel pour le traitement de données externes en aveugle*

Résumé

Le besoin croissant d'externalisation des services numériques et l'augmentation notoire de la quantité d'informations disponibles se heurtent aux différentes questions de la protection des données. Il est devenu crucial de s'appuyer sur des méthodes cryptographiques suffisamment avancées pour concilier fonctionnalité et sécurité. Cette thèse s'articule autour du chiffrement fonctionnel qui permet, grâce à un chiffré et une clef dite fonctionnelle, de déléguer en externe et de manière très fine une fonctionnalité spécifique. En particulier, nous explorons plusieurs pistes et proposons différents modèles formels pour résoudre des problématiques concrètes. D'abord, nous étudions l'interactivité durant la phase de génération de clefs fonctionnelles et identifions des cas d'usages où la protection des spécificités de la fonctionnalité est pertinent. Pour ce faire, nous introduisons une notion d'aveuglement, proposons une transformation générique l'atteignant ainsi qu'une construction efficace ad-hoc pour le produit scalaire.

Additionnellement, nous traitons du problème de ré-identification d'individus dans une base de données et établissons des liens entre confidentialité différentielle et sécurité du chiffrement. Partant d'une base chiffrée, nous développons une variante du chiffrement fonctionnel pour des requêtes linéaires aléatoires compatibles avec ce besoin. Notre approche permet de bénéficier en même temps de la délégation fine d'un calcul mais aussi de l'anonymisation du résultat obtenu.

Finalement, nous déployons un protocole pratique respectant la vie privée de ses utilisateurs et permettant l'agrégation de données mobiles. Notre proposition modifie une variante du chiffrement fonctionnelle dans un contexte multi-utilisateurs couvrant ainsi notre cas d'usage. En outre, la technique utilisée permet de garantir une tolérance aux pannes, où nous permettons aux utilisateurs de renoncer pendant l'exécution du protocole.