Chiffrement Complètement Homomorphes

Team Aplha

Mars 2021

Contents

1 Définition

Chiffrement homomorphe ; est une forme de cryptage recente, permet d'effectuer des calculs(addition multiplication)sur un message chiffré au préalable par un algorithme de chiffrement. On a donc besoin d'un algorithme de Cryptage Asymétrique ; le rendu final est le même pour un message non chiffré.

Dsk(Cpk(n)+Cpk(m))=n+m Cette propriété s'appelle l'homomorphie additive
Dsk(Cpk(n)Cpk(m))=nm Cette propriété s'appelle l'homomorphie multiplicative

L'avantage principal apporté par le chiffrement homomorphique est la construite des protocoles respectant la vie privée des utilisateurs.

En effet, le chiffrement homomorphe peut aussi exercer une fonction évaluative du calcul sans avoir accès à la clé secrète.

On a deux type chiffrement homomorphe :
Le chiffrement partiellement homomorphe qui utilise soit opération arithmétique addition ou une multiplication afin de réaliser son chiffrement.
Et un chiffrement complètement homomorphe par contre lui il utilise l'addition et la multiplication.

Par ailleurs dans notre projet on va se contenter d'approfondire nous connaissances et on se basera plus sur le chiffrement completement homomorphe.

Les calculs sont représentés sous forme de circuit booléens ou arithmétiques.

2 Contraintes et exigences

2.1 Contraintes

-l'application utilise un cryptage asymétrique
-On doit avoir une interface graphique qui doit intéragir avec le client.
-On doit avoir une simulateur de serveur qui execute un CChomomorphe.
-On doit avoir une BDD qui est utilisé par le serveur pour le stocage de données.

2.2 Exigences fontionnelles et non fontionnelles

-exigences minime dans le cadres d'un projet d'etude.