

Optimal Fully Homomorphic Encryption Approach

Problem

- Achieve *Fully Homomorphic Encryption* (FHE)
- Without noise + low computation

Purpose

- Support the operations of the cipher-text on remote servers
- Without knowing the plaintext

Why FHE?

- Against both insider and outsider threats

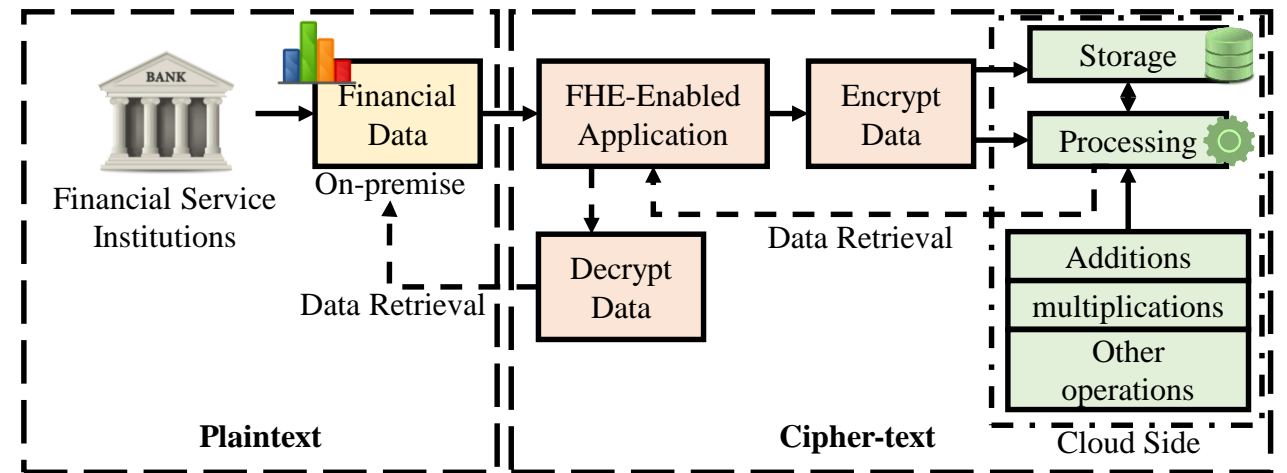
Mathematical Expression

$$f(x_1, x_2, \dots, x_n) = Dec(f(En(x_1), En(x_2), \dots, En(x_n))))$$

Where each x_i is an input plain text, $i \in 2 [1; n]$; function $f(\cdot)$ refers to any operations; $En(x_i)$ is an encryption function; $Dec()$ is a decryption function.

Methods

- Mainly consists of 4 algorithms
 - Encryption, decryption, homomorphic addition, & homomorphic multiplication
- Use Kronecker Products (KP) law



Architecture of KP-FHE Applied for Financial Service Institutions

Accuracy Evaluation

