Introduction to Homomorphic Encryption

1

Privacy in the Cloud

- Many individuals and companies are outsourcing their storage and computing needs to the cloud
- This developments raise many privacy issues
  - Clients no longer have direct control of their data
- Privacy issues
  - Data privacy
  - Function privacy
  - Query privacy
  - Server privacy
- Current encryption schemes only guarantee data privacy
  - Data becomes unusable

2

Homomorphism

- A homomorphism is a map (function) between two algebraic structures of the same type , that preserves the operation of the structures.

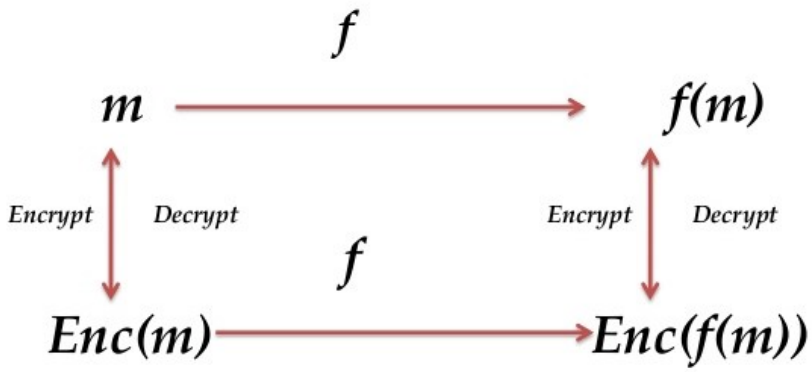
$$f : A \rightarrow B$$

$$f(x * y) = f(x) * f(y)$$

- The map ***f*** is a homomorphism or is said to preserver the operation *******

3

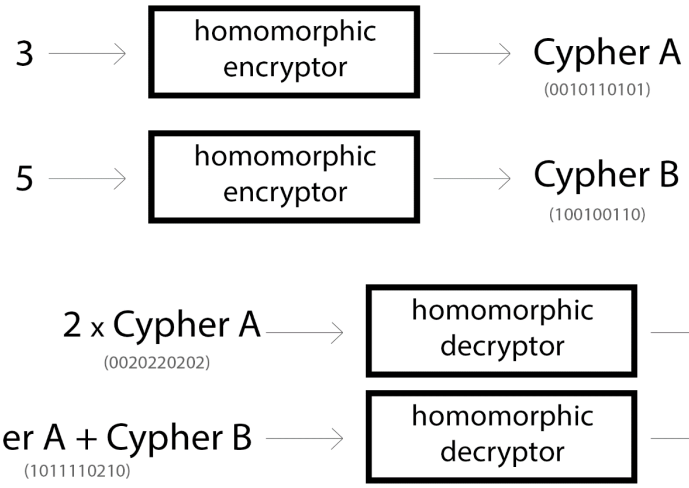
Homomorphic Encryption (HE)



- ENC() – Homomorphic Encryption function
- f() – Function that is preserved after the application of ENC()

4

Homomorphic Encryption

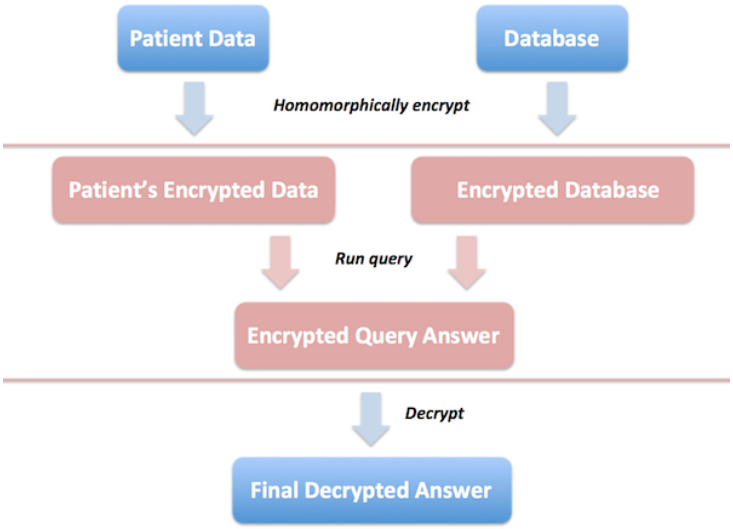


5

Homomorphic Encryption

6

Homomorphic Encryption – Use Case



7

Types of Homomorphic Encryption Schemes

- Partially Homomorphic Encryption (PHE)
  - Supports only addition or multiplication operations on plaintext
- Fully Homomorphic Encryption (FHE)
  - Supports any arithmetic operation including addition and multiplication on plaintext
- Somewhat Homomorphic Encryption
  - Fully homomorphic encryption is only possible for fixed number of calculations after which the system becomes unstable

8

Comparison of PHE Schemes

PHE Scheme	Supported Operations
RSA	Multiplication
ElGamal	Multiplication
Goldwasser-Micali	Addition
Parillier	Addition, Constant Multiplication

9

FHE Schemes

- First FHE scheme was proposed in 2009 by ***Craig Gentry***
  - PhD thesis at Stanford University
  - Scheme was based on Lattice-based cryptography
- In 2010 van Dijk et.al. proposed an improvement to Gentry's scheme
  - FHE over integers
  - Utilizes most of the ideas from Gentry's scheme but replaces Lattice-based algebraic structures with integers
- FHE schemes based on LWE (Learning with Errors)
  - Learning with errors is a problem in machine learning that is hard to solve

10

FHE Schemes

- Not very efficient
- Only practical on small amounts of data
- In Dec 2020 , IBM launched its homomorphic encryption service

11

Any questions?

???

12