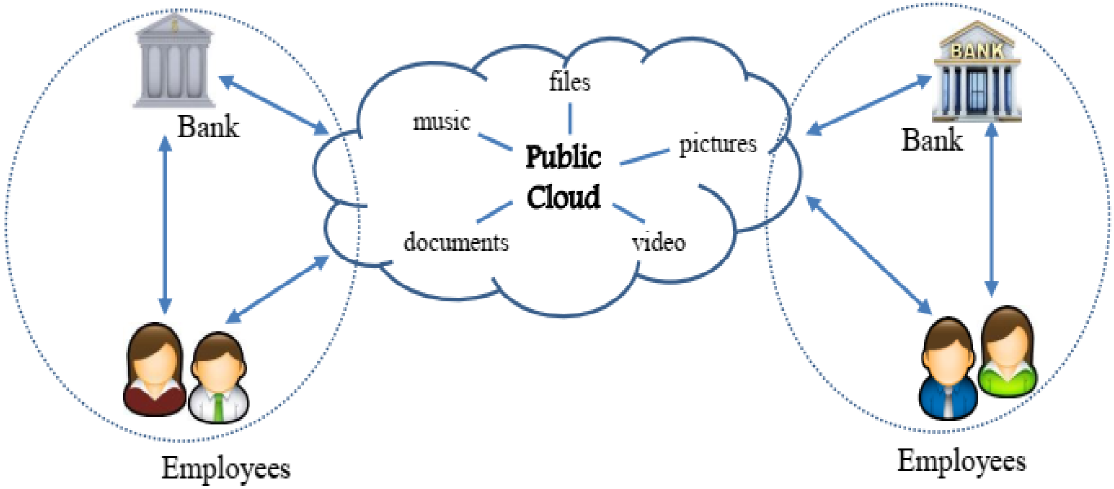
QSafe-Quantum Safe Encrypted Cloud Storage

by

Dr. P. Syam Kumar

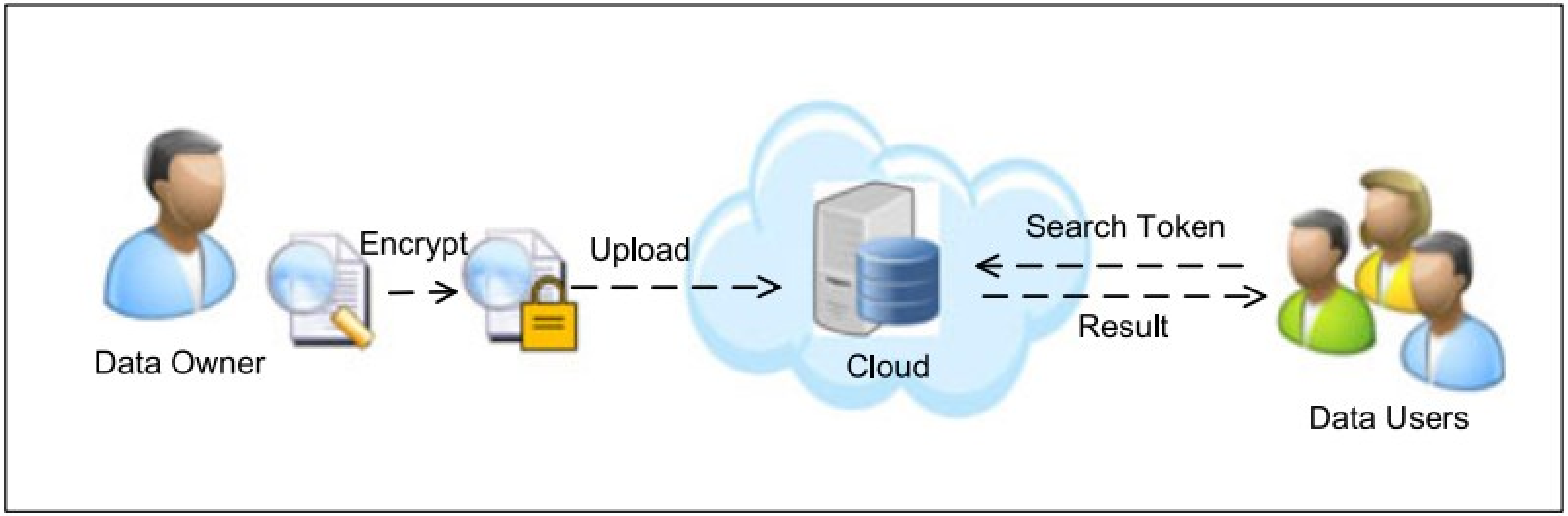
Introduction

- With rapid development of cloud, Banks tend to store their customers' electronic records into the cloud to reduce costs and maintenance.
- Since, the cloud server is not fully trusted, the privacy of bank customers (such as bank account details) may be compromised.
- Hence, protecting **Privacy of customer data** is become mandatory in the Cloud
- To protect data privacy, Banks prefer to encrypt their customers' bank account information before sending it to the cloud server. but **searching on encrypted data** is challenging task to get particular customer details



Public key Searchable Encryption (PKSE)

- Public key Searchable Encryption (PKSE) is proposed to perform **search over encrypted data** without decrypting data while protecting data privacy .



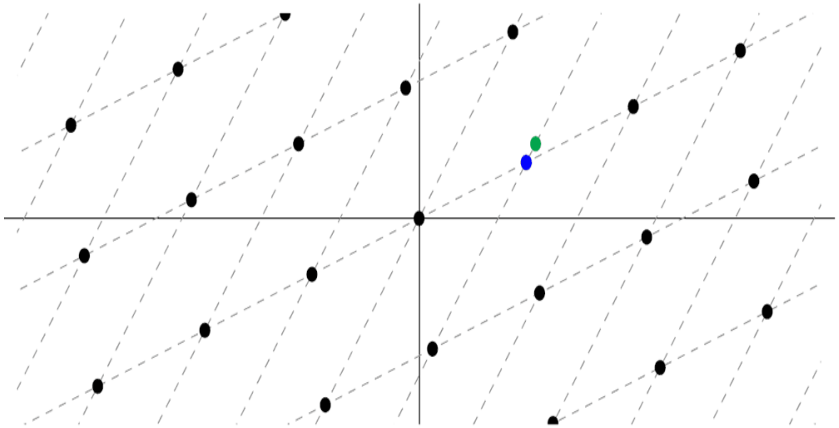
- But existing PKSE schemes designed using traditional public key Cryptography(PKC) based on hardness of solving **Factoring problem** or **Discrete logarithmic problem,** which prone to quantum attacks with advent of quantum computers.
- Hence, PKSE schemes no longer secure with advancement of quantum computers

QSafe-Quantum Safe Encrypted Cloud Storage

- To resist quantum attacks, we developed a Qsafe **Quantum Safe Encrypted Cloud Storage** using Lattice based Cryptography(LBC) which is a promising post-quantum cryptography
- Qsafe rides on a attribute based searchable encryption and provides both data privacy as well as Access control for bank customer data in the cloud and also secure on quantum computers
- The security of Qsafe is proved under **Learning With Errors (LWE)** problem.

Learning with errors (LWE)

- LWE: is the problem of solving linear equations with small error terms
- The oracle outputs (b=⟨a,s⟩+e mod q)
- Given a, b to find s
- The LWE problem comes in two variants, the **search** problem and the **decision** problem



LWE – More Precisely

- Easy to solve a linear system of equations

$$A \quad s \quad = \quad b \quad (mod\ q)$$

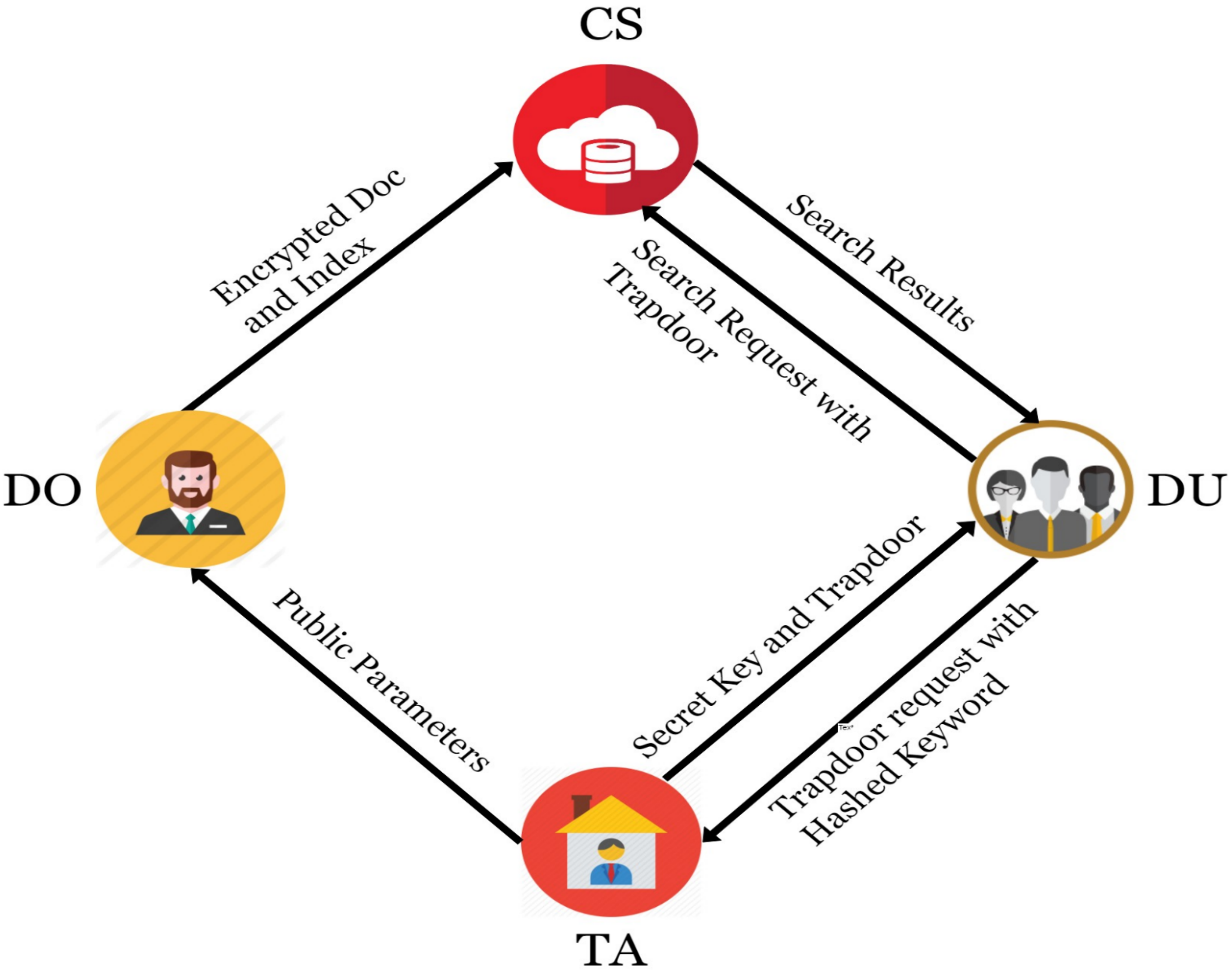
  - Given ***A***, ***b***, find ***s***
  - Solved using Gaussian elimination etc.

- Hard if we add a little noise

$$A \quad s \quad + \quad e \quad = \quad b \quad (mod\ q)$$

  - ***e*** is a noise vector, $|e| \ll q$
  - Given ***A***, ***b***, find ***s*** and/or ***e***

Qsafe Architecture



CS

DO

DU

TA

Encrypted Doc and Index

Search Results

Search Request with Trapdoor

Public Parameters

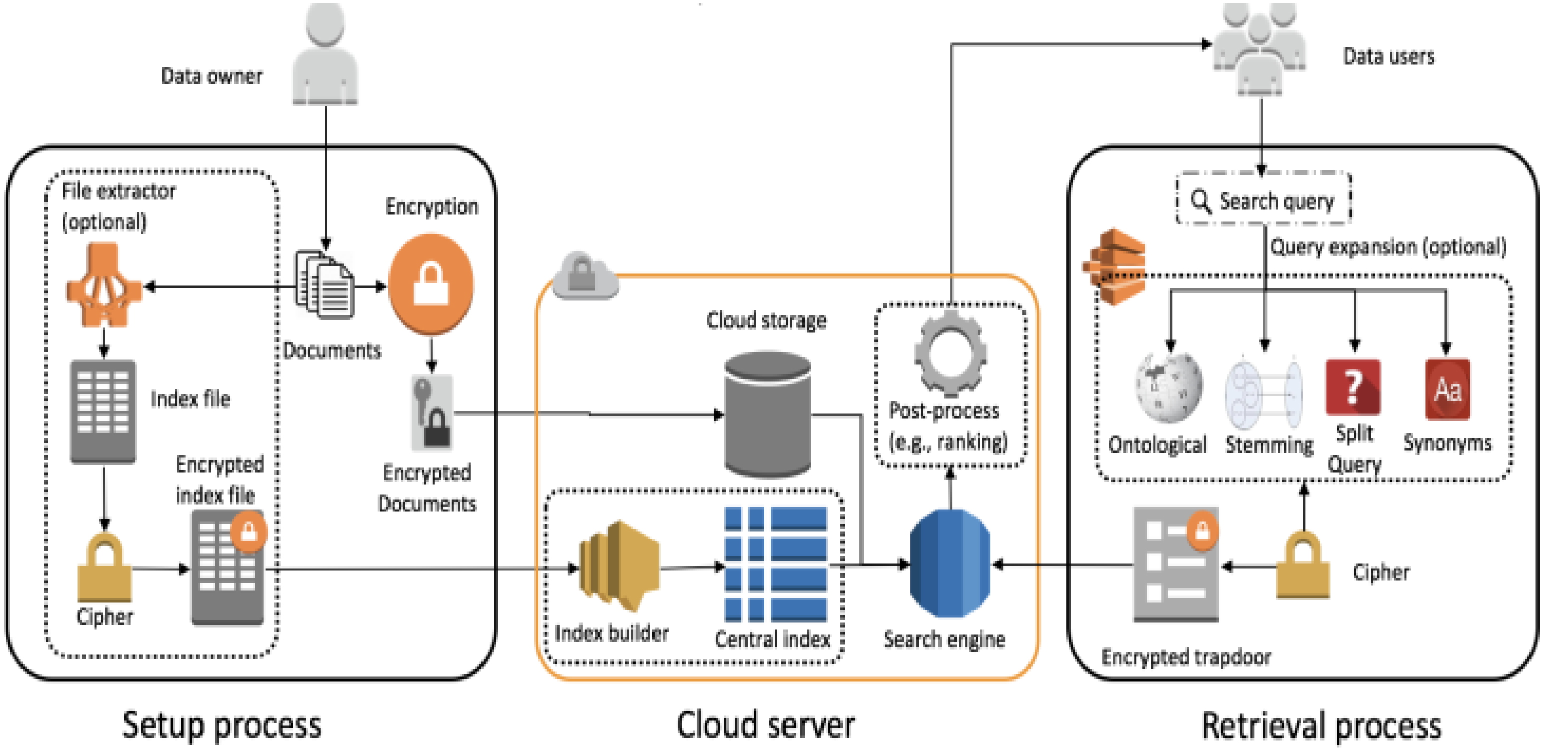
Secret Key and Trapdoor

Trapdoor request with Hashed Keyword

Q-Safe-Algorithms

1. **Setup(1^k) →(MPK, MSK) :** The Setup algorithm takes security parameter k and generates the master public key MPK and master secret key MSK.
2. **Encrypt(M, W, P, MPK)→CT :** The encrypt algorithm takes the data files M, public key MPK, Access policy P and keyword set W as inputs and generates the Chiphertext CT.
3. **Keygen(MSK, A) →SK** This algorithm takes a Master secret key MSK, user attributes *A* as input and produces the produce secret key SK for user
4. **Trapdoor(W’, SK)→$T_{w'}$:** This algorithm takes the keywords w’ and secret key SK, and then generates the trapdoor **$T_{w'}$**
5. **Search(CT, $T_{w'}$)→CT’:** This algorithm takes the trapdoor **T_{w}** and chiphertext CT and returns corresponding file
6. **Decrypt(CT, SK) → M. :** The Decrypt algorithm takes Chiphertext CT and user secret key SK as input and return M as input

Overview of Q-Safe



Q-Safe Objectives

- **Privacy*:*** Q-safe protects the privacy of sensitive data from unauthorized users in the cloud.
- **Fine-grained Access Control***:* Q-safe allows only authorized users to decrypt the encrypted data by providing fine-grained access controls
- **Secure**: The security of QSafe is proved under **Learning With Errors (LWE)** assumption, which resists quantum attacks and provides long-term security. Thus it is secure on both classical computers and Quantum computers
- **Efficient**: Q-safe is designed based on LBC, which only requires simple addition and multiplication operations instead of heavy pairing operations. Thus it is efficient.

Summary

- IDRBT developed a Qsafe product to protect data privacy in the cloud and also secure on quantum computers
- The Banks can use Qsafe product to store data in the cloud and retrieve data securely without disclosing any information

Thank you