Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY
Bangalore Chapter

IAS IEEE INDUSTRY APPLICATIONS SOCIETY
Linking Research to Practice
Bangalore Chapter

6th **INTERNATIONAL CONFERENCE ON**

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS

(PKIA 2025)

SEPTEMBER 3-4th, 2025

Design and Implementation of a Post-Quantum Double Ratchet using ML-KEM

Paper ID: 9

PRESENTING AUTHOR: AKASH ANGOM

AUTHOR AND CO-AUTHORS: AKASH ANGOM, NIRMALYA KAR, TRIBID DEBBARMA, PRIYANKA BISWAS

AFFILIATIONS: NIT AGARTALA

https://pkiindia.in

Social Media /pkiindia

IEEE BANGALORE SECTION

Table of Contents

Introduction

- **Signal Protocol:** Peer-reviewed, open-source end-to-end encryption protocol for secure messaging
- **Double Ratchet:** Guarantees that every message is encrypted under an individual key, which is termed ”ongoing rekeying” [1]
- Traditionally dependent on *Diffie-Hellman(DH)* key exchange, eg, X25519 [2]
- Designing and substituting with a *Post-Quantum (PQ)* secure primitive is crucial in the PQ era
- NIST’s drafted standard for the key encapsulation mechanism, the *ML-KEM* [3], is a potential substitute

Motivation

- Apple's iMessage PQ3 protocol [4] claims to use a hybrid PQ rekeying scheme, but details remain unpublished
- Signal is developing its own PQ upgrade, not yet released
- To address this gap, we propose ML-KEM as a replacement for legacy Diffie-Hellman in Double Ratchet
- Direct substitution is non-trivial, since KEMs and DH differ fundamentally in operation

Background

- **Security Objectives:** *Confidentiality, Forward secrecy, Message authentication, Integrity protection, Post Compromise recovery, Asynchronous messaging, Replay attack resistance*
- **ML-KEM:** NIST's drafted standard *Module-lattice-based key encapsulation mechanism*, enabling two parties to agree on a shared secret key over an open communication channel
- **AES-GCM:** *Advanced Encryption Standard in Galois/Counter Mode* [5], an authenticated encryption algorithm ensuring confidentiality, authenticity, and integrity of messages.
- **KDF:** *Key Derivation Function*, a cryptographic algorithm that creates one or more secret keys derived from an initial source of keying material

Classical Double Ratchet of Signal

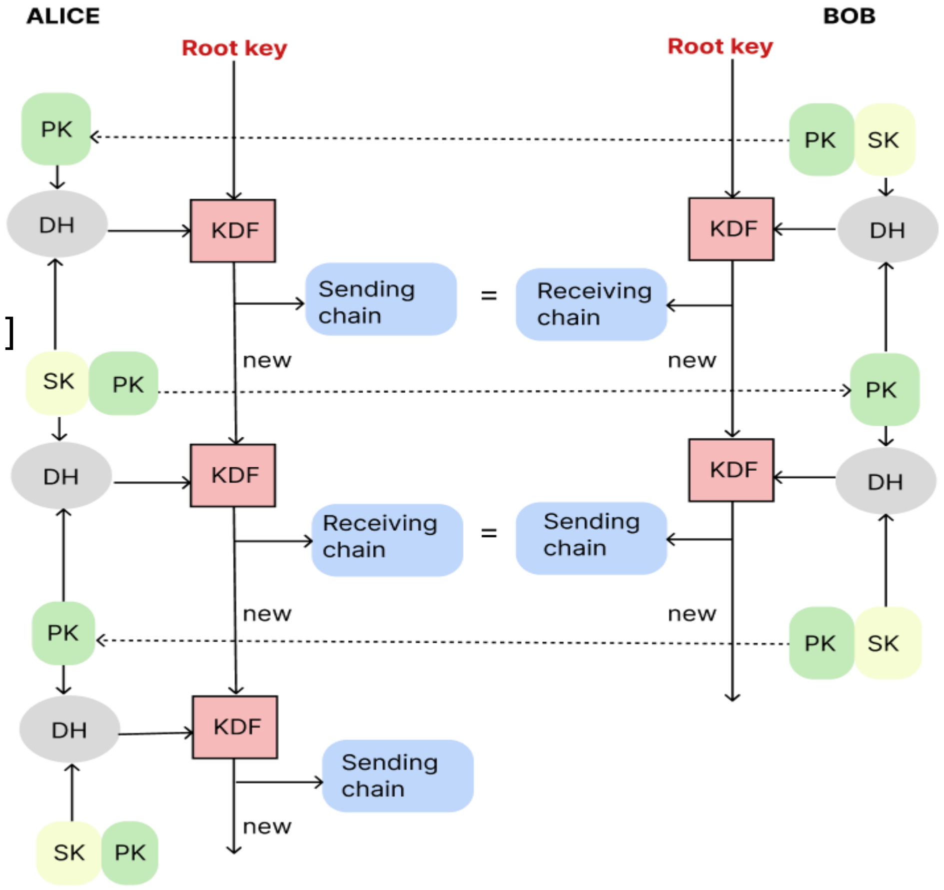


Fig. 1. DH-ratchet [1]

PK = public key
SK = secret key

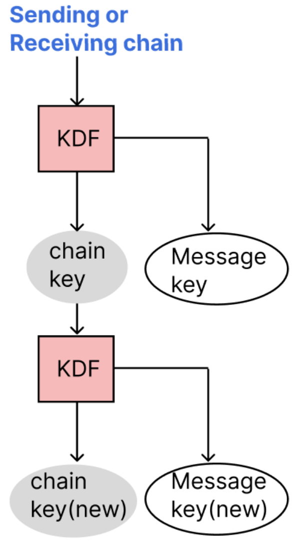


Fig. 2. Symmetric-key ratchet

Note: Root key is generated by a preceding key establishment process such as PQXDH [6]

Design Approach

PQ Double Ratchet

Using ML-KEM:

Here,

EK = Encapsulation key

DK = Decapsulation key

Encaps = Encapsulation

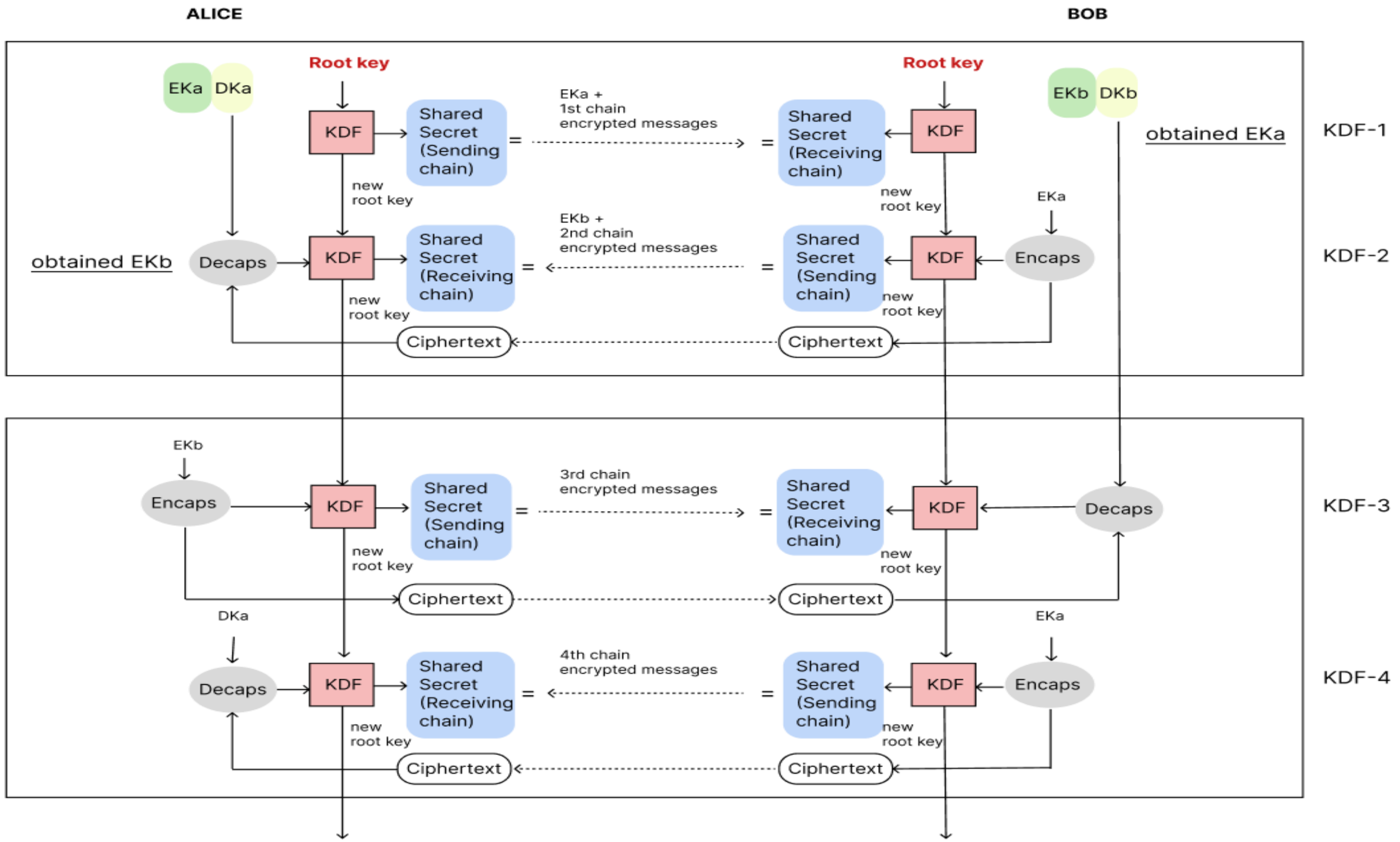
Decaps = Decapsulation

Ciphertext = Encapsulated shared key

**Key updation is necessary to minimise post compromise*

PHASE 1
(Handling Initial chain, obtaining public keys & initial Ciphertext)

PHASE 2
(Ciphertext only exchange)



Implementation

Implementation flow of ML-KEM-based double ratchet

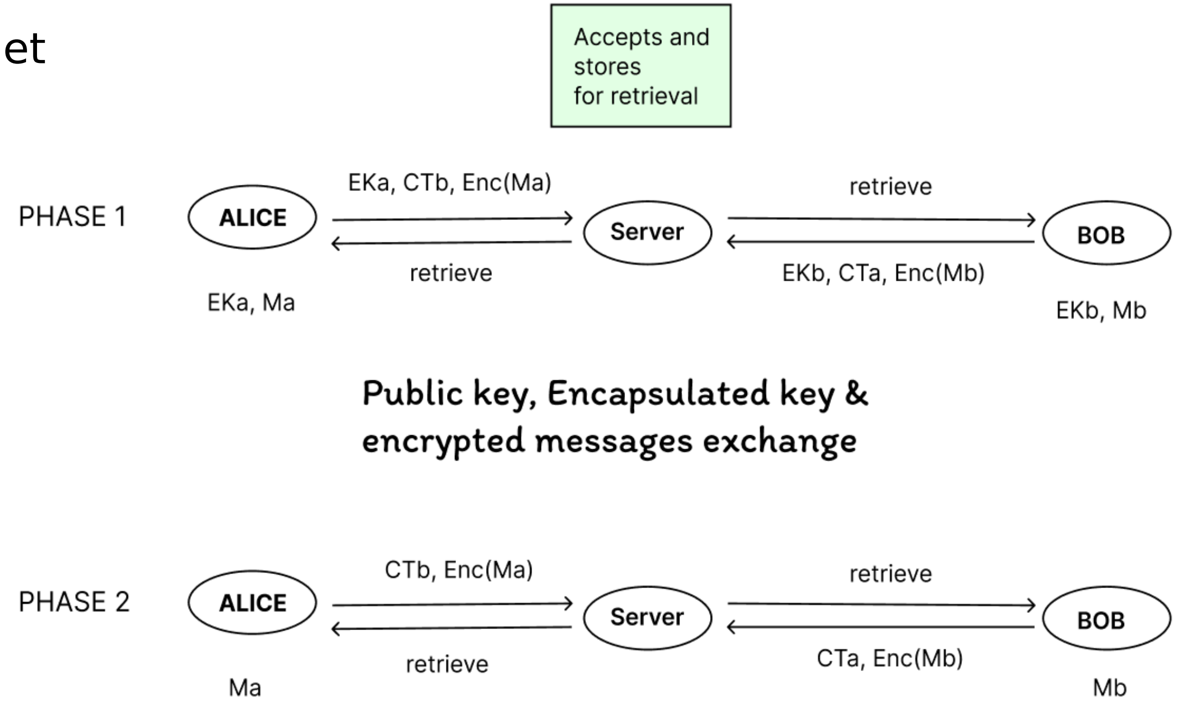
Here,

CTb = encapsulated key using EKb
Cta = encapsulated key using EKa

Ma = message from Alice

Mb = message from Bob

Enc(x) = Encrypted message



ur proof-of-concept implementation, written in Python, is as faithful to the official specifications of the cryptographic primitives as possib
he full source code is posted at: https://github.com/Akash2002-bit/ML-KEM-double-ratchet

Results and Analysis

Correctness: *The input to Alice's receiving chain is the same as Bob's sending chain input, and the other way around.*

Security properties preservation:

Security Property	Mechanism
Confidentiality	Key encapsulation and encryption
Forward Secrecy	Ongoing rekeying
Message Authentication	Authenticated Encryption with Associated Data (AES-GCM)
Message Integrity	Authenticated Encryption with Associated Data (AES-GCM)
Post-Compromise Security	Key updates
Asynchronous Messaging	Use of the server
Replay Attack Resistance	Unique identifiers

Network Load Discussion: *Increased due to encapsulated key and key sizes. Not necessary to generate new key pairs for every PQ ratchet (feasible because of the probabilistic nature of ML-KEM)*

Conclusion and Future Work

A PQ secure variant of the Signal's Double Ratchet by replacing standard Diffie-Hellman-based exchanges with ML-KEM. A proof-of-concept implementation shows the feasibility of achieving a fully PQ Double Ratchet with real-world usability-friendly efficiency, and network overhead remains reasonable, particularly when optimization of the key reuse strategy is implemented.

Current and further investigations can examine more refinements, strict mathematical proof of security, and usage fields towards strengthening the vigor and adoption of post-quantum secure ratcheting mechanisms.

REFERENCES

1. Moxie Marlinspike. The double ratchet algorithm. https://signal.org/docs/specifications/doubleratchet/, November 2016.

2. Diffie, W. and Hellman, M.E., 2022. New directions in cryptography. In Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman (pp. 365-390).

3. National Institute of Standards and Technology (2024) Module-Lattice-Based Key-Encapsulation Mechanism Standard. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publication (FIPS) NIST FIPS 203. https://doi.org/10.6028/NIST.FIPS.203

4. Apple Security Engineering and Architecture. iMessage with PQ3: The new state of the artin quantum-secure messaging at scale, February 2024. URL: https://security.apple.com/blog/imessage-pq3/

5. Dworkin, M.J., 2007. Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC.

6. Kret, E. and Schmidt, R., 2023. The PQXDH key agreement protocol.url: https://signal.org/docs/specifications/pqxdh/pqxdh. pdf.

THANK YOU