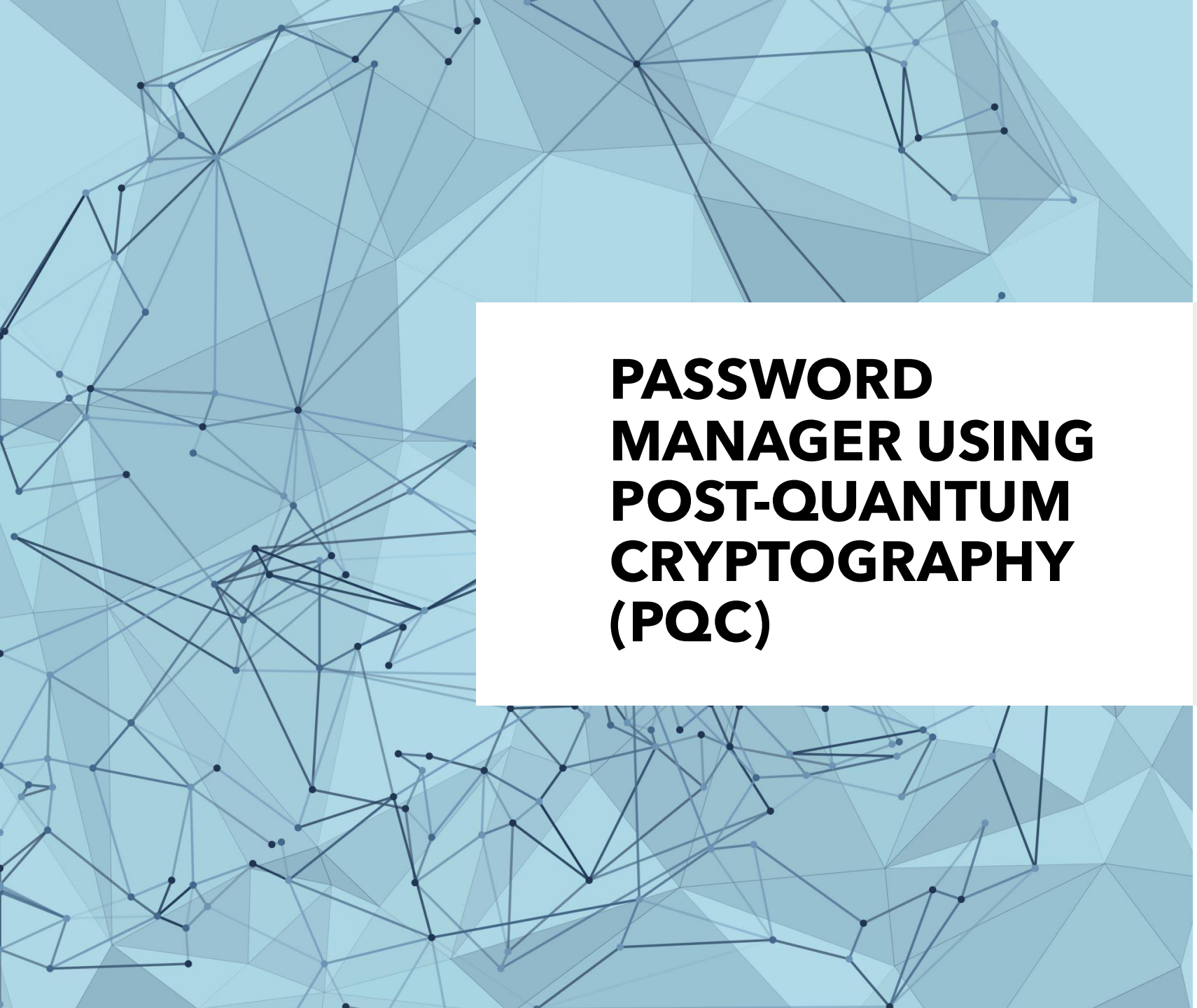


PASSWORD MANAGER USING POST-QUANTUM CRYPTOGRAPHY (PQC)

TEAM MEMBERS

- KARTHIKEYA DEVARAJ
- P NAITHIK
- BINIT BALAK SEN
- SOHAM ROY

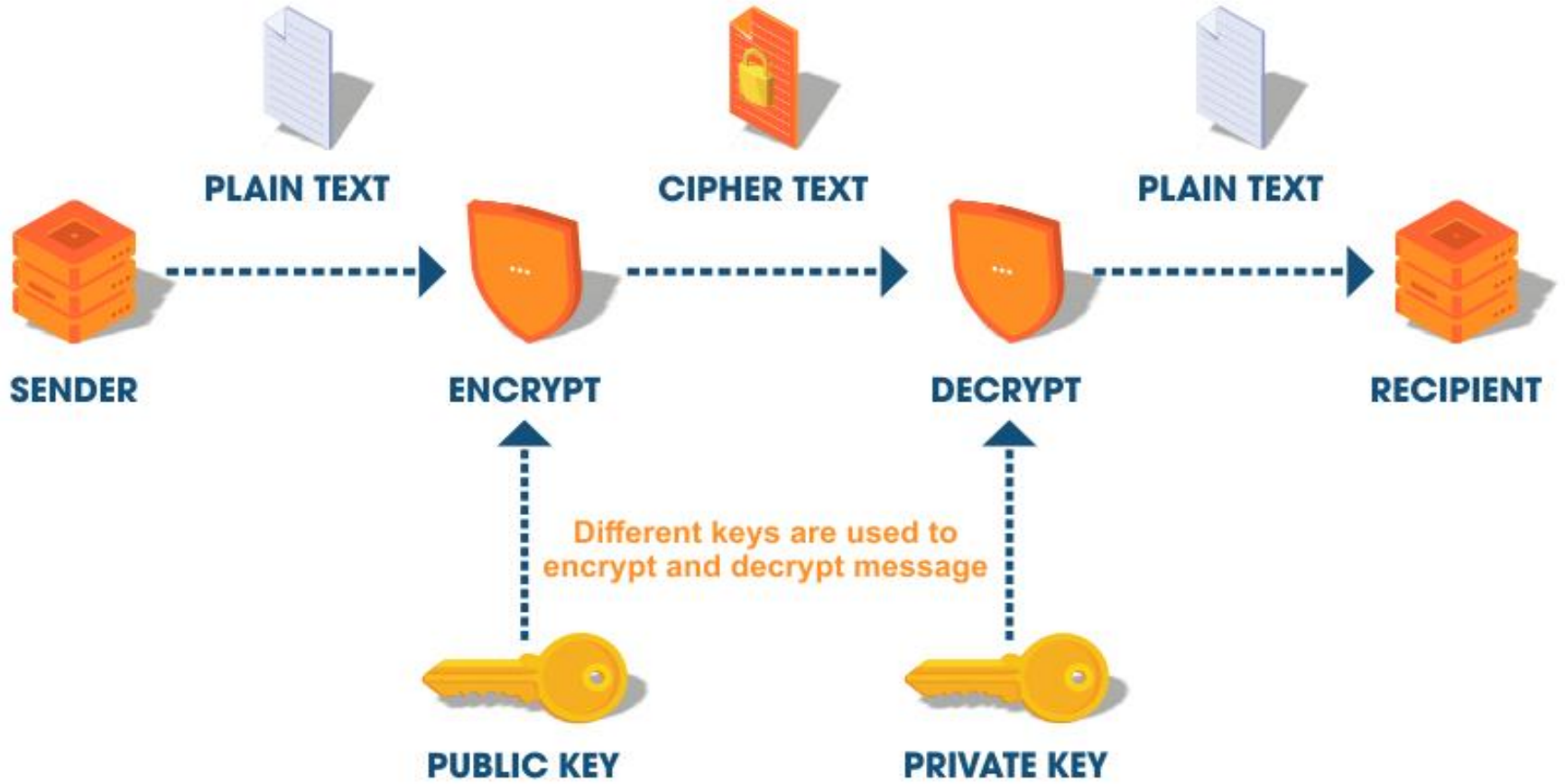
Basic idea behind our project

- Our Project is based on **Post-Quantum Cryptography (PQC)**.As it is quite an impossible task to penetrate the security of Lattice-Based Cryptography, we want to integrate this Quantum Cryptographic System in our platform that will serve as a **tamper-proof password/biometric /document vault** ensuring security from any advisaries. We aim to facilitate this idea in platforms such as an application.

Why use Post Quantum Cryptography?

- Traditional cryptographic algorithms like RSA and ECC are vulnerable to **Shor's algorithm**, which a sufficiently powerful quantum computer could use to break them in polynomial time. The goal of integrating PQC into a password manager is to ensure:
- Password encryption remains secure **even against quantum attacks**.
- Secure **key exchange** between devices without exposure to quantum threats.
- Strong authentication methods that are **resistant to forgery** by quantum adversarie

How does Encryption and Decryption works Internally?

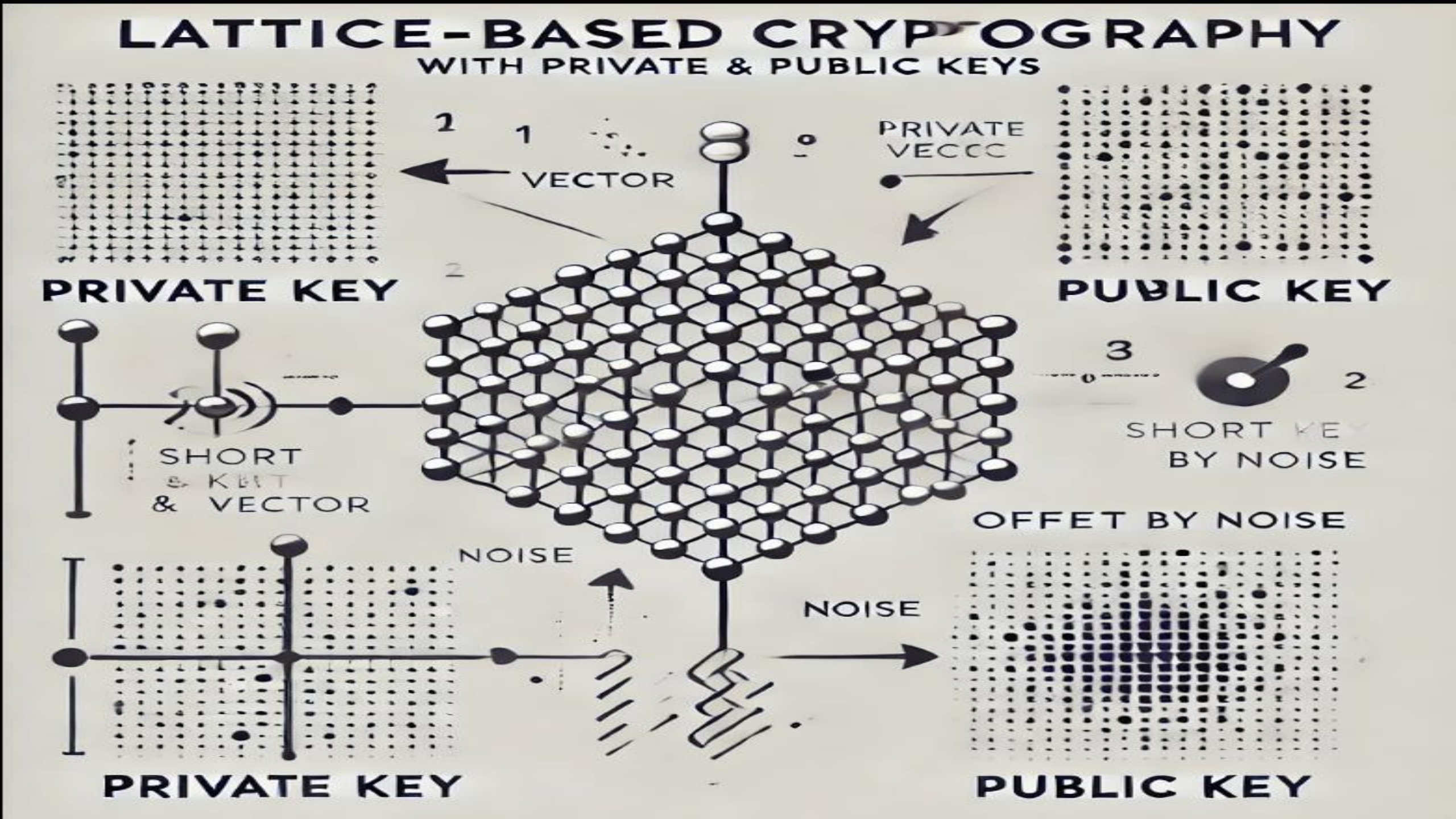


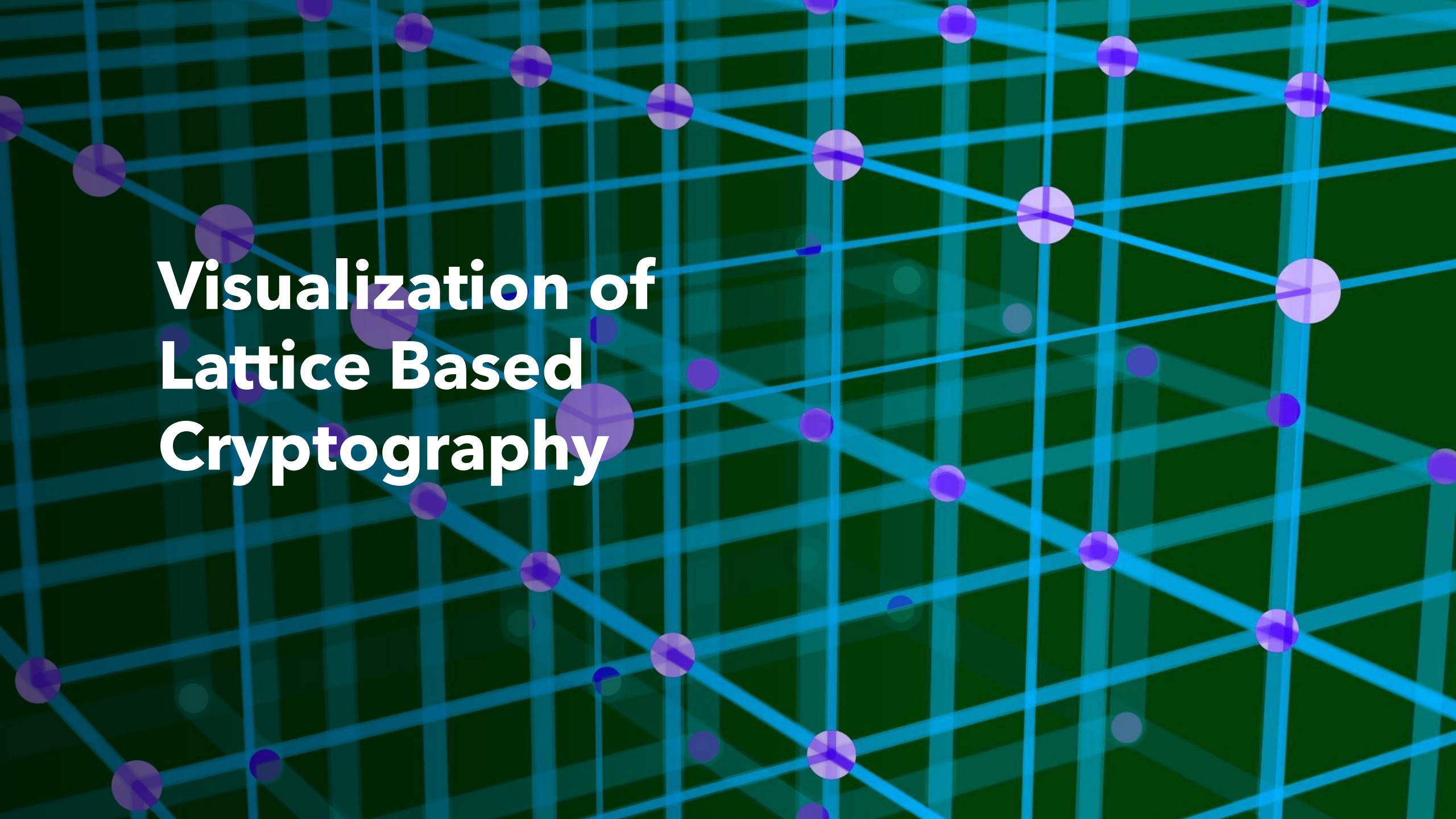
Encryption with Kyber

Decryption with Dilithium

LATTICE-BASED CRYPTOGRAPHY

WITH PRIVATE & PUBLIC KEYS




Visualization of
Lattice Based
Cryptography

Comparison between PQC and traditional security

Feature	Traditional Security (RSA/ECC + AES)	Post-Quantum Security (Kyber + Dilithium + AES)
Key Exchange Algorithm	RSA-3072 or ECDH-256 (Elliptic Curve Diffie-Hellman)	Kyber-768 or Kyber-1024 (Lattice-based KEM)
Key Generation Time	RSA-3072: ~5ms	Kyber-768: ~2.5ms (faster)
Public Key Size	RSA-3072: 384 bytes / ECDH-256: 64 bytes	Kyber-768: 1 KB (larger but quantum-safe)
Private Key Size	RSA-3072: 2.5 KB / ECDH-256: 32 bytes	Kyber-768: 2.4 KB
Signature Size	RSA-3072: 384 bytes	Dilithium-III: 2.8 KB (larger, but quantum-resistant)
Resistance to Quantum Attacks	Not secure (RSA, ECC broken by quantum computers)	Quantum-safe (hard lattice problems)
Long-Term Security	Compromised when large quantum computers exist	Secure for the foreseeable future