Kyber (KEM Algorithm)

1 TABLE OF CONTENTS

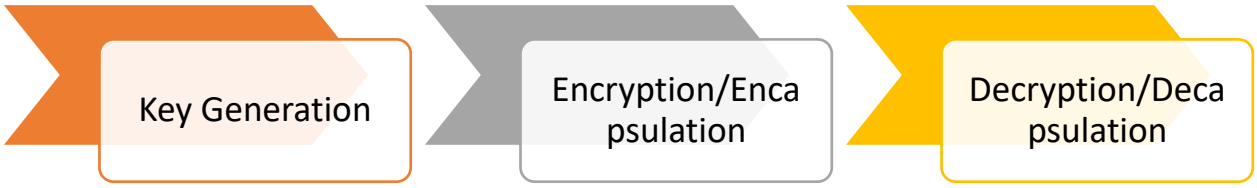
2 INTRODUCTION TO KYBER

Kyber, an algorithm, is basically a post-quantum cryptographic key encapsulation mechanism that has been primarily designed for securing communications when it comes to cyber vulnerabilities in quantum computing (Saoudi et al., 2024). This algorithm has also been defined under NIST framework, including Post-quantum cryptographic (PQC) project in the year 2022 for the purpose of standardizing the algorithm. Basically, the working of this algorithm is based on LWE and RLWE, which are referred to as Learning with Errors and Ring-LWE for resisting attacks from potential computers. The prime reason for using this algorithm for cryptographic key encapsulation mechanism is their efficiency, ease of implementation and even secure data transmission (He et al., 2024). This document delves deeper into Kyber algorithm based on its design, functionality and security related parameters.

3 DESIGNING AND FUNCTIONALITY

The working of Kyber algorithm is primarily based on lattice-based cryptography, which is basically a variant of **Learning with Errors** (LWE) problem. Basically, the hardness of this algorithm is based on mitigating the noisy nature of linear equations and making sure the challenge faced by quantum computers are fixed in an appropriate manner (Saoudi et al., 2024). This algorithm is built on the basis of

three different components such as key generation, encryption/encapsulation and lastly, decryption/de-capsulation. For each component, a detailed discussion have been made below for Kyber algorithm.



1. **Key Generation**: The first component is key generation which is almost same to other algorithms as the key generation is carried out using random polynomials. This generation is primarily done in the finite ring to generate the public and private keys. Once the keys are generated, the use of public key will be done for encryption whilst the private key will be used for decryption, as a normal cryptographic procedure.
2. **Encryption/Encapsulation:** The next component is encryption/encapsulation phase where a random session key is established, which is also said to be the shared key. The use of this key is done for encapsulation and is further transmitted to the recipient's public key. Based on this process, the further encapsulation is performed to the cipher text and finally, it can be shared over insecure channels easily.
3. **Decryption/Decapsulation:** The last one is decryption/decapsulation which is opposite of previous component and is used for decryption. Herein, when the receiver uses the private key, the decapsulation is done on the cipher text so that the original text or a message can be obtained (He et al., 2024).

Also, the working of Kyber algorithm is specified on two types of mathematical foundations such as modular arithmetic and error distribution. In the context of modular athematic, the working of this algorithm is on a ring of polynomials by utilizing coefficients under a modular arithmetic. When this has been done, it allows for efficient computation without causing any problem. Furthermore, in the context of error distribution, this algorithm primarily provides a random noise when encryption is being carried out so that when any attack is performed, the original data is not accessible. As a result of this error distribution, it ensures that security is maintained over different types of cyber-attacks. Moreover, the Kyber algorithm is also categorized as Kyber512, Kyber768 and even Kyber1024 levels where the

increasing level will assure higher security (Pathum, 2024). Also, the working of key encapsulation mechanism (KEM) is provided below that shows how the working of Kyber algorithm will be done between a client and a server.

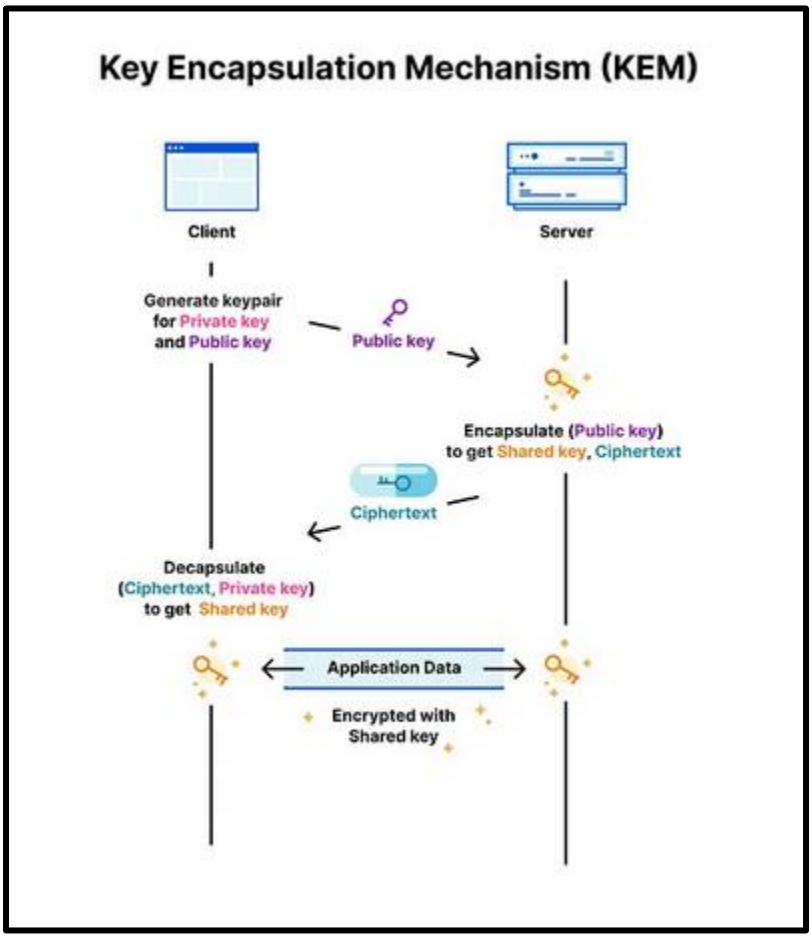


Figure 1: https://medium.com/@hwupathum/crystals-kyber-the-key-to-post-quantum-encryption-3154b305e7bd

4 KYBER'S SECURITY

As discussed earlier, the security of Kyber algorithm is based on ring learning with error problem which falls under the lattice cryptographic problem. In terms of security, the Kyber is expected to offer robust working model which will make sure encryption and decryption processes are carried out efficiently. There are various advantages of Kyber when it comes to security, these advantages are explained below.

- The first every advantage is based on post-quantum security where classical key algorithms named as ECC and RSA's reliance on integer factorization and other problems could be solved by

Shor algorithm easily. However, in the case of lattice-based problems, there are no chances for quantum based attacks (Rugo, 2021).

- Kyber is expected to offer provable security as it works under the lattice cryptography which clearly means it is very challenging to break it.
- In the context of chosen cipher text attack resistance (CCA), the selected algorithm offers built-in resistance to different cipher text based attacks. In case a manipulation is performed on the cipher text, there will be no interference to the private key because of message observation (Klas, 2023).
- Finally, for the performance, the designing of the Kyber algorithm is based on balancing a security and efficiency for its optimal working. Once it is done, it will make sure real-world applications such as cloud based services, mobile devices and other areas are protected. In comparison to other post-quantum algorithms, the selected algorithms offers small key sizes with faster key exchange times (Yang et al., 2023).

The tabular matrix provided below shows the three different variants of Kyber algorithm and list its parameters in the context of key sizes, cipher text, and security level.

Variant	Public Key Size	Cipher Text Size	Secret Key Size	Approx./ Security Level
Kyber512	800 bytes	768 bytes	1632 bytes	128-bit, level 1
Kyber768	1184 bytes	1088 bytes	2400 bytes	192-bit, level 3
Kyber1024	1568 bytes	1568 bytes	3168 bytes	256-bit, level 5

5 COMPARISON WITH OTHER POST-QUANTUM ALGORITHMS

In the race for post-quantum cryptography standardization, the Kyber algorithm is not only available algorithm as there are many other present such as NTRU, SABER and FrodoKEM. The table given below discusses why Kyber is better than other algorithms.

Parameters	Kyber	Other Algorithms (NTRU, SABER or FrodoKEM)
Key Sizes	The key sizes for Kyber is small than other algorithms, offering faster speed	The key sizes for these algorithms is larger than Kyber which could utilize more bandwidth

Computation	There is faster computation speed with Kyber as it offers quicker encapsulation and decapsulation times, assuring low latency	In other algorithms, the times are higher and even latency is high (Liang et al., 2024)
Security	The Kyber's security is underpinned by hardness of lattice based problems (Klas, 2023)	There are no guarantees for security in other algorithms just like Kyber

6 CHALLENGES AND FUTURE

There is no doubt that Kyber is leading in the post-quantum encryption scheme, but it still offers various challenges that have devastating impacts, these challenges are given below.

- The first challenge is based on standardization, even though it has been selected by NIST, but the final finalization is underway.
- Another challenge is related to the adoption as transitioning from the classical cryptographic procedures to the post-quantum cryptographic procedures will take a lot of time, including adoption to the Kyber algorithm (Liang et al., 2024).
- Even there are higher chances that the hybrid approach will be used in future where the classical and post quantum algorithms will be done for proceeding while compatibility issues may be faced.

In terms of future, it can be said that the use of this algorithm will be done in almost entire quantum computing cryptography so that a higher level of security is offered to data. Also, the continuous research is being done which portrays that Kyber is robust against evolving quantum related cyber threats (Liang et al., 2024).

7 REFERENCES

He, S. *et al.* (2024) 'A lightweight hardware implementation of CRYSTALS-Kyber,' *Journal of Information and Intelligence*, 2(2), pp. 167–176. https://doi.org/10.1016/j.jiixd.2024.02.004.

Klas, G. (2023) *CRYSTALS-Kyber for Post Quantum Cryptography demystified*. https://www.linkedin.com/pulse/crystals-kyber-post-quantum-cryptography-demystified-guenter-klas.

Liang, Z. *et al.* (2024) 'Compact and efficient KEMs over NTRU lattices,' *Computer Standards & Interfaces*, 89, p. 103828. https://doi.org/10.1016/j.csi.2023.103828.

Pathum, U. (2024) 'CRYSTALS Kyber : The Key to Post-Quantum Encryption | Medium,' *Medium*, 24 June. https://medium.com/@hwupathum/crystals-kyber-the-key-to-post-quantum-encryption-3154b305e7bd.

Rugo (2021) *Kyber - How does it work? | Approachable Cryptography*. https://cryptopedia.dev/posts/kyber/.

Saoudi, M. *et al.* (2024) 'Low latency FPGA implementation of NTT for Kyber,' *Microprocessors and Microsystems*, 107, p. 105059. https://doi.org/10.1016/j.micpro.2024.105059.

Yang, Y. *et al.* (2023) 'Chosen ciphertext correlation power analysis on Kyber,' *Integration*, 91, pp. 10–22. https://doi.org/10.1016/j.vlsi.2023.02.012.