CRYSTALS-Kyber

Stephen Tambussi

Research Objective

Objective

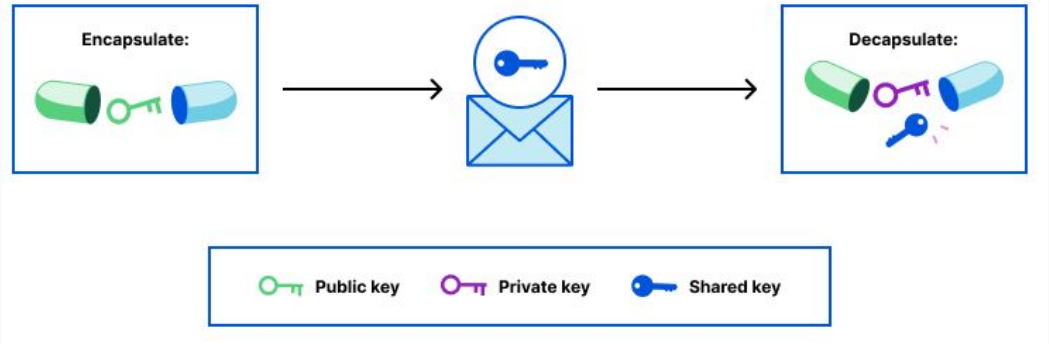
To determine and review the latest cryptographic algorithm and its impact on the security world.

Why Kyber?

Kyber is the winner of NIST’s PQC project and it provides the best defense against attacks from future quantum computers, which will render current encryption insecure.

What is Kyber?

- One of two quantum-secure cryptographic primitives in **CRYSTALS** (Cryptographic Suite for Algebraic Lattices)



[1]

- It is a **KEM** (Key Encapsulation Mechanism) – a method to establish a shared secret key between two parties

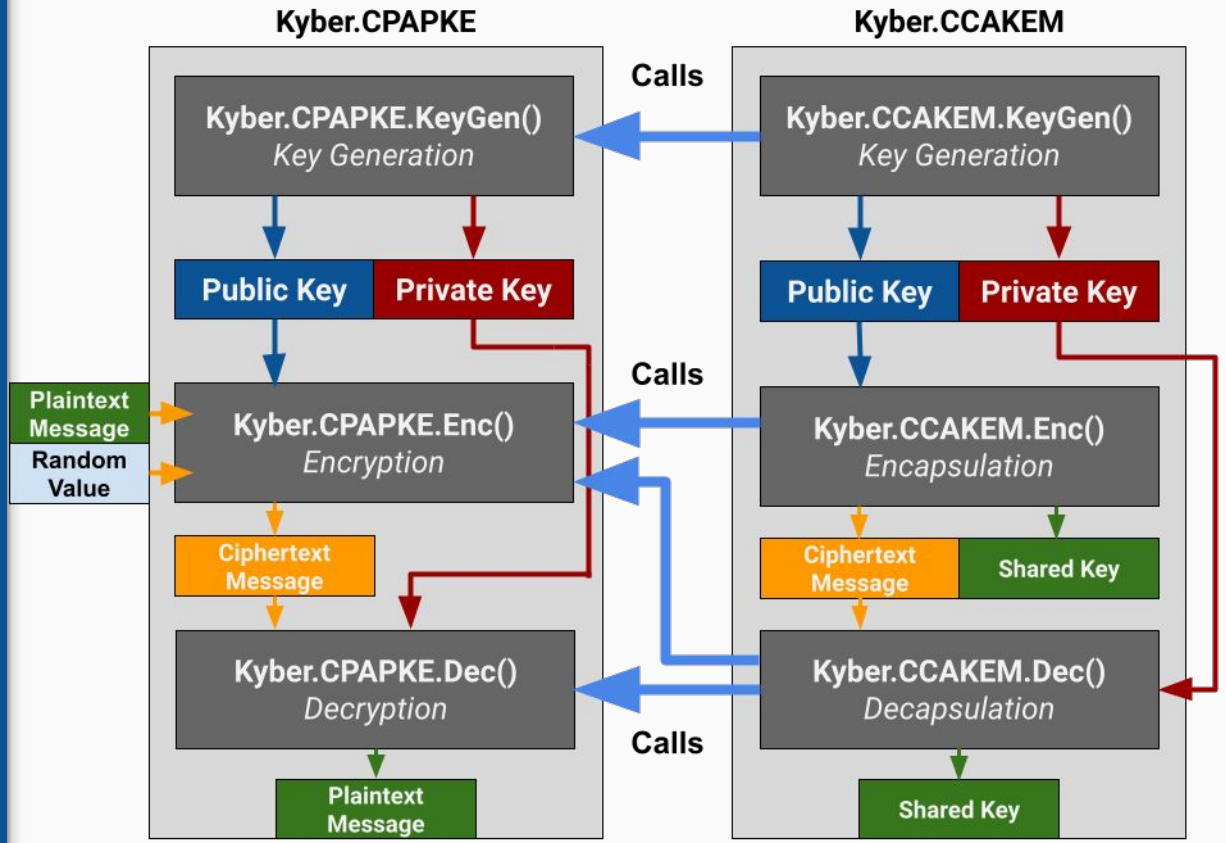
Kyber Specifics

Two Stages

1. Kyber.CPAPKE
2. Kyber.CCAKEM

- Symmetric primitives (SHA-3)
- Lattice-based Cryptography (MLWE)

[2] [3] Algorithm Overview



Kyber Security

Kyber-512	Kyber-768	Kyber-1024
Security ≅ AES-128	Security ≅ AES-192	Security ≅ AES-256
[4] Time to Crack	Time to Crack	Time to Crack
2.61×10^{12} years	1.97×10^{22} years	2.29×10^{32} years

Potential Vulnerabilities

- Side-channel attacks on platform-specific implementations
- Attacks against underlying symmetric primitives

Advantages and Limitations of Kyber

Advantages

- Fastest of post-quantum algorithms
- Secure against attacks from quantum computers
- Easy to implement and many optimizations possible

Limitations

- Can be slower than pre-quantum encryption
- Symmetric primitives are a potential point for attack
- Certain implementations shown to be vulnerable to side-channel attacks

Conclusion

- Kyber is very secure against quantum computers
  - Same goes for classical computers
- Many use cases due to similar structure to public-key encryption
- Very fast compared to other post-quantum algorithms
- Adoption should be easy

Questions?

References

[1] https://blog.cloudflare.com/post-quantum-key-encapsulation/

[2] V. Lyubashevsky, "*Standardizing Lattice Cryptography … and Beyond*", PQCRYPTO 2017.

[3] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. Schanck, P. Schwabe, G. Seiler, and D. Stehlé, "CRYSTALS-Kyber," Algorithm Specifications And Supporting Documentation (version 3.02), 4 Aug. 2021.

[4] https://nap.nationalacademies.org/read/25196/chapter/6#98