Quantum Safe NIST Candidates

Kyber is one of the 4 NIST finalist cryptography algorithms which (should) offer post-quantum security. Of the 4 Key Encapsulation finalists, this algorithm is most likely to see widespread adoption, so will be the subject of most focus here.

Kyber’s security, as do 2 other KEM finalists (NTRU, Saber) depends on solving problems involving *lattices.*

# lattice based cryptography

Lattice based algorithms typically have very small key sizes < 1.5KB, often on the order of hundreds of bytes, and faster than RSA to encrypt and decrypt. There is a decent, simple explanation of what a lattice is at <https://medium.com/cryptoblog/what-is-lattice-based-cryptography-why-should-you-care-dbf9957ab717> . NTRU is based on the SVP (discussed in the article), but Saber and Kyber are based on a different class of problems – Learning With Errors/Rounding.

## Kyber Algorithm In Detail

An explanation of (Module) Learning With Errors is given below in the case of Kyber. Note that the implementation below assumes a fixed message size (around 32 bits with the base specification for Kyber). Multiple iterations of the algorithm are performed when longer messages are involved (which will be essentially aways).

### Key Generation

**A** - a k by k matrix, generated from the hash of a seed sampled from a uniform distribution. A random A is generated by the server, which the client can recreate from the public key

**s** – a length k vector, with elements sampled from a centred binomial distribution

**e** – a length k vector, with elements sampled from a centred binomial distribution

This is somewhat a simplification, as kyber does not work with matrices and vectors of integers, but polynomials in a specific quotient vector space. We will ignore this temporarily, without losing the core ideas of the algorithm.

Let:

**t**, combined with the seed used to generate **A** form the public key.

**s** acts as the private key

### Encryption

1. The server generates **A** from the public key, as discussed above.
2. A new vector **r** of length k is sampled from a centred binomial distribution
3. **e1** , **e2** are similarly sampled (*from a potentially different centred binomial distribution*)

Where u,v form the ciphertext. Note that the full algorithm also performs compression and decompression on the ciphertext, which reduces ciphertext sizes, and also provides error tolerance if implemented correctly.

### Decryption

Decryption is (without the encoding, decompression steps) simply

### Breaking LWE Decryption

It can be proven that solving these equations for unknowns reduces to MLWE, as follows (unrigorously, any errors in justification here are my own)

Consider

An attacker will be able to derive **A** and **t** from the public key, but **e** is an unknown. Were it not there, the attacker would be able to relatively trivially solve for **s** with a method such as Gaussian elimination. It is conjectured that versions of this LWE problem are NP-hard for both quantum and classical systems, but no proof has yet to be demonstrated. There is therefore a risk that over the next number of years and decades, a proof will be produced that will lead to practical attacks on many LWE-based algorithms.

### Matrix and Vector Elements

As I mentioned earlier, it was heavily implied above that vector and matrix elements were integers, or at the very least Real. For Kyber however (and many other lattice based cryptography algorithms), it is more secure and effective to work with elements in the ring , where n is a power of two.

More transparently, this corresponds to the set of all polynomials of degree less than n, with integer coefficients modulo q.

This means that for every vector addition and matrix multiplication we perform above, the operations are between polynomials. If computed naively, these would take O(k) operations for each addition and O(k^2) operations for *each individual multiplication.* However, by applying a version of the Discrete Fourier Transform known as the Number Theoretic Transform, we can reduce this to the order of O(k log k) operations. Note that this is dependent on the choice of n – (it is chosen as a power of two > 2, due to some characteristics of roots of unity in power-of-two rings, but this is not important to understand). Further, the NTT of two polynomials can be computed without requiring extra memory, and can be implemented in a heavily optimized manner that brings the number of clock cycles used to compute an NTT in almost k cycles.

The underlying principles of the NTT are similar (albeit taken to a slightly higher level of complexity) to those of using a FFT to perform ordinary polynomial multiplication. There is an explanation (although quite dense and not very well structured) here for using a FFT to multiply polynomials efficiently

https://medium.com/@aiswaryamathur/understanding-fast-fourier-transform-from-scratch-to-solve-polynomial-multiplication-8018d511162f

## Points of Note About Kyber

### Utilising hardware optimisation

When benchmarking implementations of Kyber, it is worth bearing in mind that it has been noted in the official specification for Kyber that the majority of the execution time for Kyber encryption, decryption and key generation (given properly implemented NTT and inverse NTT functions) is spent computing hashes, using algorithms such as SHA3, SHA2, SHAKE . If any hardware accelerated implementations versio of these algorithms are available on a system, it is highly beneficial to use an implementation of Kyber that capitalizes on this.

### No Guarantee That a Message is Decryptable

The specification of Kyber suggests a number of sets of parameters that deliver estimated increasing levels of classical and quantum security. Each of these has been shown to have no guarantee that a message encrypted with an arbitrary key can be decrypted, but the probability of this happening is between 2-139 and 2-174, a quantity so insignificant that no errors can be expected to occur even with universal adoption, for the remainder of the lifespan of the universe. Thus, its chances are dwarfed by those other potential system failures, and can be discounted.

### No Quantum or Classical Security Proof

The MLWE problem has not yet been proven to be NP-hard. It is worth noting that rings/vector spaces such as the ring of polynomials used in Kyber have an extremely high amount of structure – the possibility of this being exploited to arrive at a polynomial algorithm is very real. As a counterpoint, the exact sort of ring used by Kyber, with q as a prime number and the quotient , as a cyclotomic polynomial have been heavily researched in terms of their properties for hundreds of years. Nonetheless, it would be extremely imprudent to deploy Kyber as a sole algorithm used to encrypt sensitive data. On the other hand, it is very desirable to being securing communications against quantum attacks in the very near future – while large scale error corrected quantum computing is still likely a few decades a way at least, this horizon is less than the confidentiality of much data being transmitted today. This leaves an ever growing incentive for attackers to intercept, and store sensitive data that will retain value over many years.

The best compromise that addresses this issue is to implement a hybrid approach of standard, provably classically secure, Elliptic Curve or RSA encryption in conjunction with Kyber. In this configuration, the security of the encrypted data can only be compromised with both access to a large scale error corrected quantum computer, as well as a polynomial time solution to the MLWE problem – a much less likely prospect than both happening individually.

## Saber

Saber is similar to Kyber in many respects, but the most pertinent difference is that its security is based on Learning With Rounding, rather than learning with errors – instead of adding an error term that makes the secret key difficult to solve for, it rounds the elements of the resulting vector. Note that rounding has more algebraic structure than addition of well-distributed errors, which could be a (although there is no evidence as yet of such) vulnerability. There is in fact some rounding of the error terms in Kyber, which is not relied heavily on in its theorized security, but is beneficial. This does give the impression of Kyber being more rich in substance than Saber, although this is purely an opinion on my part – and there is no empirical evidence to back this opinion up.

Classic McEliece

Classic McEliece is being considered by NIST as an alternative candidate, mainly should the underlying problems on lattices above are shown to be solvable in polynomial time. It was introduced in 1978 and has been thoroughly researched since then – we can thus be somewhat more confident in its security than the lesser-researched and unproven lattice methods. The underlying principle that creates its security involved decoding certain Error correcting Codes. It has the major drawback of having extremely large keys, from roughly 200KB – 1.5MB, although ciphertexts can be quite short (less than 250 bytes) and encryption and decryption are faster than RSA. This all means that this is not really feasibly in most scenarios, but there may be some very limited instances where the larger key sizes are acceptable, and the higher confidence in its proof of security over lattice based methods may be much more useful.