Some implementation considerations

Ganyu (Bruce) Xu (g66xu)

June, 2024

Here are some considerations when implementing Kyber using "encrypt-then-mac"

1. Strong candidates for `MAC` are HMAC and KMAC. From an efficiency standpoint KMAC is preferable because $\texttt{HMAC}(k, m) = H(k \| H(k \| m))$ makes two calls to the hash function, but `KMAC` makes only one call to `Shake`. From a security and usability standpoint, HMAC is more widely used than KMAC. We can simply try both and report the results.

2. Since the `MAC` key is derived from the message, and in Kyber, the message $m \in \mathcal{M} = \{0,1\}^{256}$ is exactly 256-bit in length, we should choose the `MAC` key to also be exactly 256-bit in length. Any longer key is unnecessary, since it then because easier to simply search for the message.

3. There is argument about how HMAC is not affected by weakness in collision resistance in the underlying hash function[2] (the idea is that an adversary can only obtain a tag online, which is much slower than computing hash offline). In addition, collision resistance is less affected by quantum computing than preimage resistance is. The best classical attack on collision resistance is the birthday attack, with the expected number of steps being $2^{\frac{n}{2}}$ for an n-bit hash; the best quantum attack[1] is expected to take $2^{\frac{n}{3}}$ steps for an n-bit hash.

With the three points above, I came up with this table for the recommended parameters. For classical 128-bit security and 256-bit security, I chose a 256-bit and 384-bit hash for the tag because TLS 1.2 pairs SHA-256 with AES-128 and SHA-384 with AES-256. For quantum computing, we can choose more conservative parameters (such as using 384-bit hash for 128-bit security and 512-bit hash for 256-bit security).

	key size	tag size	pre-image resistance	collision resistance
classical, 128-bit security	256	256	256	128
classical, 256-bit security	256	384	384	192
quantum, optimistic	256	256	128	≈ 86
quantum, moderate	256	384	192	128
quantum, conservative	256	512	256	≈ 171

Table 1: Parameter sizes and estimated security levels, all in bits

References

[1] Gilles Brassard, Peter Hoyer, and Alain Tapp. Quantum algorithm for the collision problem. *arXiv preprint quant-ph/9705002*, 1997.

[2] Hugo Krawczyk, Mihir Bellare, and Ran Canetti. Hmac: Keyed-hashing for message authentication. Technical report, 1997.