Hybrid Cryptography: Combining Post-Quantum and Classical Solutions

As billions of dollars are being spent globally to build the world's first large-scale quantum computer, which could induce major advances in science, technology, finance, and more, the world is also preparing for the negatives, a complete break in the foundational security of the internet and other digital applications. The National Institute of Standards and Technology (NIST) and others are developing quantum-safe (also called post-quantum) standards that could replace cryptographic algorithms currently in use. These standards will take a few years to fully draft even though the winning algorithm(s) could be announced by the end of 2021.

Unfortunately, many companies may not be ready to implement post-quantum cryptography by this time. However, **crypto-agility** and preparing for this inevitable transition will save them time and money and make their customers feel safer about their data and information.

One concern about the adoption of post-quantum cryptography is the larger public key sizes that are computed and shared. Two current (i.e. classical) algorithms that will be replaced are **RSA** (based on large integer factorization) and **ECC** (based on special graphs called elliptic curves). We have seen the RSA key size slowly increase over the years to 384 bytes (3,072 bits) for NIST security level 1. Because of this constant increase, the current standard is to instead implement ECC, which has a key size that has remained at 32 bytes (256 bits). In comparison, there is only one post-quantum candidate, which is comparable to either of these key sizes. SIKE, which stands for supersingular isogeny key encapsulation, has a public key size of 330 bytes, still 10 times bigger than ECC. The next closest algorithms in the current standardization have public key sizes of about 670 bytes to 1 KB (30 times bigger), and some still have a public key size of up to 512 KB (16,000 times bigger than ECC!).

For many Internet of Things (IoTs) devices even the current RSA key is too large, thus adopting any of these new algorithms will be a challenge. An additional concern with these new post-quantum algorithms is they are not as tried and tested as current algorithms. Therefore, while it may increase these larger key sizes even more, a safe solution is **hybrid cryptography** which combines classically secure algorithms (one or more) with quantumly secure ones (one or more) such that any attacker must break all algorithms to gain access, rather than simply one. This may give the needed confidence for companies to adopt these new algorithms and upgrade their security systems before time runs out.

One obvious hybrid choice is combining ECC with SIKE, since isogenies utilize elliptic curve arithmetic. Even though each of these has a small key size in comparison, it is extremely important to mitigate this and any additional overhead, especially in resource constrained devices such as IoTs. This is one of PQSecure's current efforts.

To construct this hybrid scheme, PQSecure first found new elliptic curves that work quite efficiently in such a hybrid mode. These curves, were found in a similar fashion to the way NIST standardized curves X25519 and Curve448, but also have additional, useful properties.

For NIST security level 1, our system added 55 bytes for the public key of our elliptic curve to the SIKE public key of 330 bytes, making a combined public key length of 385 bytes. This key is still 50% smaller than any other public key size in the NIST standardization (other than SIKE obviously).

This hybrid scheme computes each algorithm simultaneously and concatenates the results into one (doubly secure) public key. The results showed an approximate 10% increase of latency and 16% in communication overhead for the additional hybrid computations and completed the operation on ASIC in less than 250 ms. As research into developing quantum computers continues, a company's crypto-agility will be tested. Developing and improving these hybrid key exchange schemes will be necessary as we transition to a fully quantum-safe infrastructure. For more information, read here[1].

[1] R. Azarderakhsh, R. ElKhatib, B. Koziel and B. Langenberg, "Hardware Deployment of Hybrid PQC," online, 23 April 2021, https://eprint.iacr.org/2021/541.pdf