Hybrid post-quantum encryption by Virgil Security, Inc.

What is Post-Quantum Cryptography?

Post-quantum cryptography is a set of cryptographic algorithms that can be implemented within classical (i.e. today's) computers but withstand powerful quantum computers.

Data encrypted without post-quantum cryptography is at risk for being unlocked when quantum computers arrive. Re-encrypting currently encrypted data with post-quantum algorithms may take years, depending on the amount of data stored.

Therefore, it is important for organizations and companies to start using post-quantum cryptography now to encrypt new data as well as re-encrypting any stored data.

To achieve this, Virgil Security has built a hybrid solution that utilizes both classical encryption as well as newer methods that are designed to withstand quantum computers.

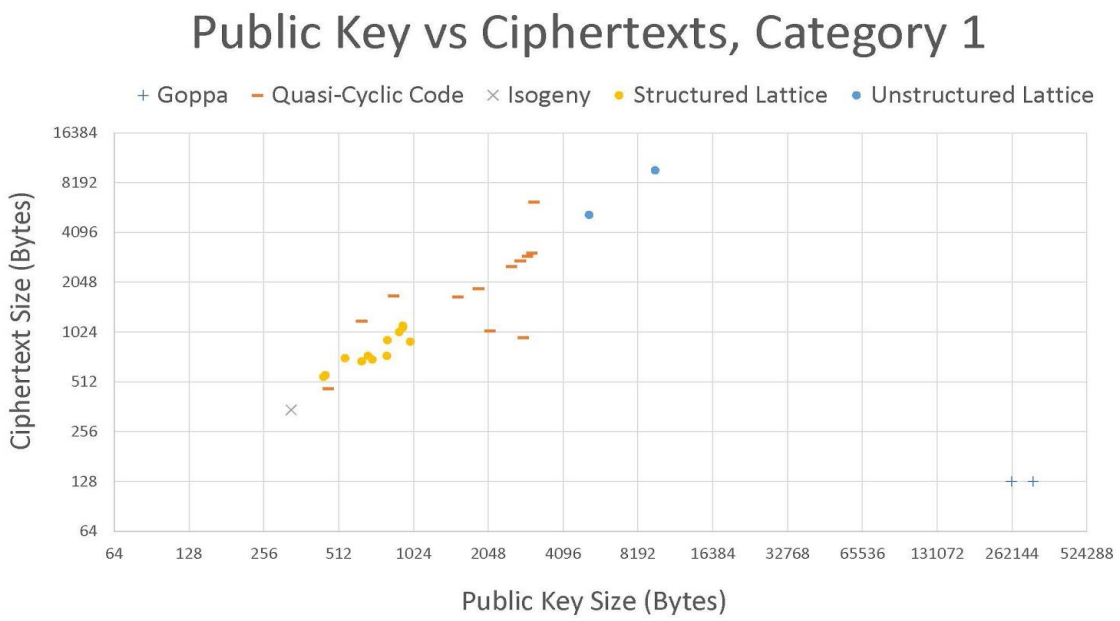
PQC: Round5 and Falcon

The Virgil Security team evaluated the NIST PQC Round 2 submissions, looking for options that were ready for real-world usage with acceptable speed and key sizes. For example:

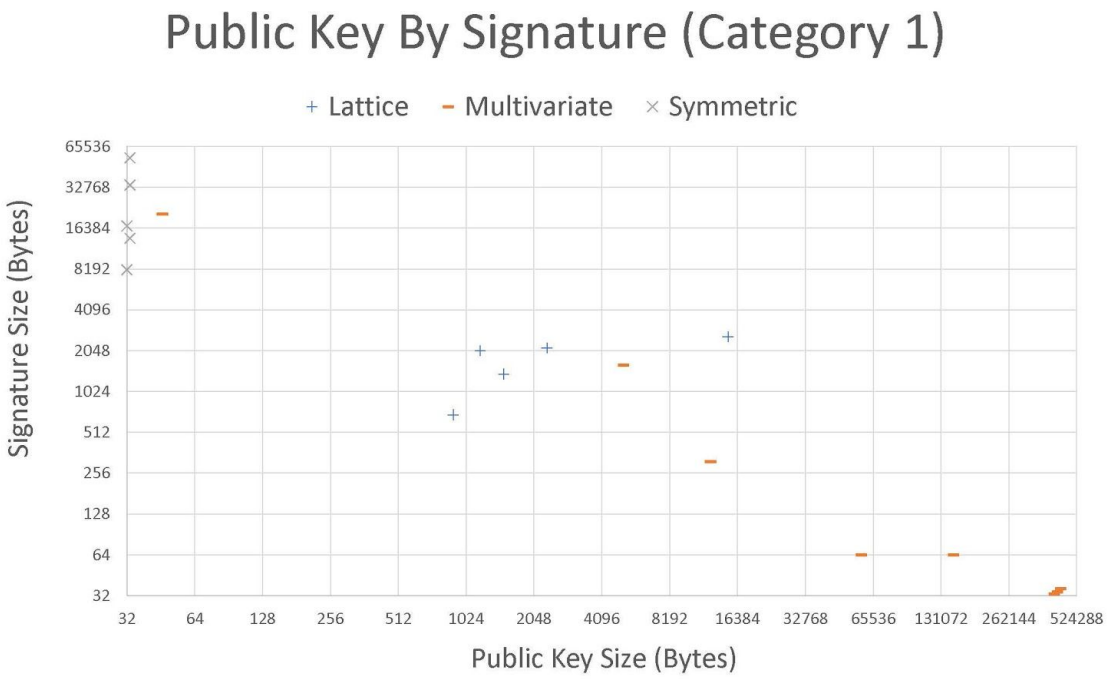
1. The McEliece cryptosystem keys are several megabytes and therefore too large for general commercial use.
2. Isogeny-based algorithms have smaller and therefore acceptable public keys, but their performance is too slow and they are still considered to be too immature.

Ultimately, we chose to use Round5 key encapsulation for encryption and Falcon for digital signature.

They are both based on the lattice problem which is hard to solve even by quantum computers and allow for relatively small keys, ciphertexts and signatures (around 1 kb) and fast implementations (thousands of operations per second). Round5 has the smallest key/ciphertext size among other candidates and Falcon signatures are substantially shorter than in any lattice-based signature scheme with the same security guarantees.



We chose one of the orange ones (Round5). Slides are from here.



We chose one of the + ones (Falcon)

Round5 is a leading candidate for NIST PQC key-encapsulation and public-key encryption. It enables a single description and implementation of multiple algorithms relying on different underlying problems. This gives the user the flexibility to choose the parameter set and algorithm that fits his application best.

The usage of the strong constant-time XEf error correction code allows Round5 to support the smallest configuration parameters among the NIST lattice-based proposals, and thus, offer the best performance in terms of bandwidth, CPU, and memory usage. Since XEf is constant-time, timing attacks on the error correction are not feasible.

We chose the parameter set R5ND_5CCA_5d which provides security corresponding to Nist Level 5

Level	Security Description
I	At least as hard to break as AES128 (exhaustive key search)
II	At least as hard to break as SHA256 (collision search)
III	At least as hard to break as AES192 (exhaustive key search)
IV	At least as hard to break as SHA384 (collision search)
V	At least as hard to break as AES256 (exhaustive key search)

It has a 978 byte public key and 1285 byte ciphertext which is large compared to current elliptic curve algorithms which have 32 bytes public key size. However, it is still more than practical for modern applications.

CPU, and memory usage. Since XEf is constant-time, timing attacks on the error correction are not feasible.

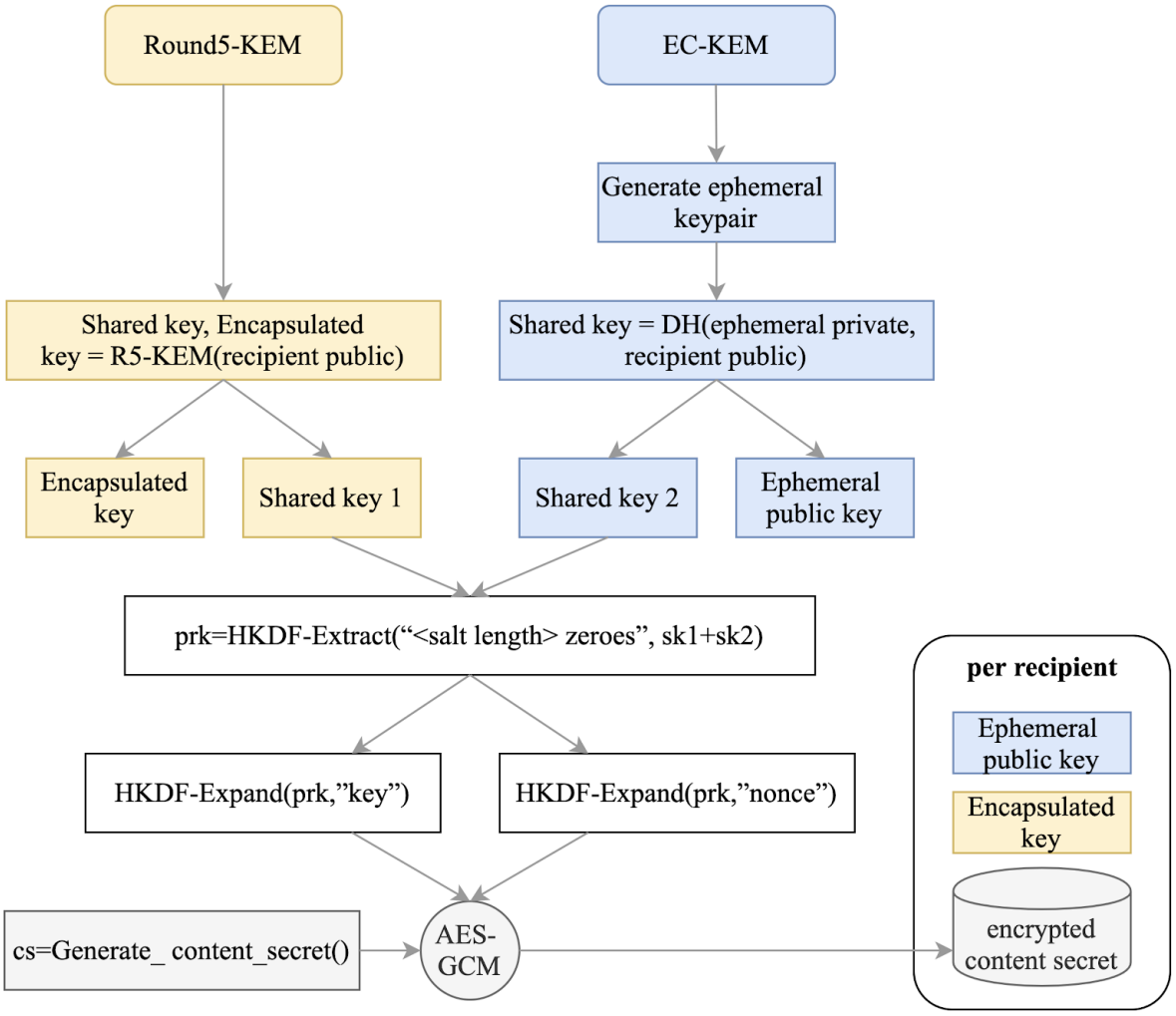
Falcon is a cryptographic signature algorithm submitted to NIST Post-Quantum Cryptography Project. We decided to use Falcon-512 with a public key size of 897 bytes and signature size of 658 bytes. Due to the use of NTRU lattices, signatures are substantially shorter than in any lattice-based signature scheme with the same security guarantees, while the public keys are around the same size. The use of fast Fourier sampling allows for very fast implementations, in the thousands of signatures per second on a common computer; verification is five to ten times faster. Falcon's enhanced key generation algorithm uses less than 30 kilobytes of RAM, a hundredfold improvement over previous designs such as NTRUSign. Falcon is compatible with small, memory-constrained embedded devices.

There are two main disadvantages of using Round5 and Falcon:

1. Key size and signature/ciphertext size: both Round5 and Falcon have entity sizes about 1 kb, so it might be a problem for very constrained environments, though we haven't experienced that yet.
2. Though Round5 and Falcon are both second-round Nist PQC standardization candidates, which started on January 30, 2019, they are still considered relatively new and are in the process of being analyzed by cryptologists and security experts. The risk of finding a vulnerability in these algorithms is higher than with more mature algorithms.

Virgil Security's Hybrid Algorithm Approach

As post-quantum algorithms are not yet mature as classic ones, we have combined post-quantum together with classical into one packaged solution in order to achieve the strongest possible security and lessen the risk of vulnerability relating to using a newer, less tested algorithm.



We use Round5 KEM and ECIES-KEM to generate two secret values which are then used to produce a single AES encryption key for the data. To decrypt that data you need both Round5 and Curve25519 private keys.

So if the post-quantum algorithms are broken or compromised, the data will still be protected by the classic algorithms.

As for the signatures, we simply sign the data with both private keys and then validate with two public keys, so digital signature algorithms work in tandem.

Other solutions like layered encryption are less efficient.

Virgil Security, Inc., provides software developers with password-free authentication, strong encryption, and verification of data, devices, and identities that is quickly and easily integrated into their products — often in just hours — with no prior cryptographic knowledge or training required.

Virgil provides this via a cloud-based service in combination with open-source libraries that are available for desktop, embedded, mobile, and cloud/web applications with support for a wide variety of modern programming languages.

Learn more at VirgilSecurity.com.