Overview of NIST Round 3 Post-Quantum cryptography Candidates

	Key Encapsulation Mechanisms		Digital Signature Algorithms	
Type	**Finalists**	**Alternates**	**Finalists**	**Alternates**
Code-based	Classic McEliece	BIKE HQC		
Lattice-based	CRYSTALS-KYBER NTRU SABER	FrodoKEM NTRU Prime	CRYSTALS-DILITHIUM FALCON	
Isogeny-based		SIKE		
Multivariate			Rainbow	GeMSS
Zero-Knowledge				Picnic
Hash-based				SPHINCS+

On July 22, 2020, the National Institute of Standards and Technology (NIST) finally announced the long-awaited Round 3 finalists for their post-quantum standardization process. Of the 69 algorithms that survived initial scrutiny and made it into the start of Round 1 back in 2017, Round 2 saw this field cut to 26 candidates and now Round 3 has cut this down to 15. These 15 are further broken down into what NIST refers to as "finalists" and "alternates", where the alternates could be standardized during a Round 4. Round 3 is expected to last approximately 12-18 months. In addition to an email sent to members of the post-quantum community, NIST published an article on its website as well which can be found here.

Round 3 Finalists: Public-key Encryption

- **Classic McEliece** is a code-based KEM with very little changes since it was introduced in 1978 by Robert McEliece. The main change from the original McEliece is a simple "upscale" of the security parameters to keep up with the increased computing speeds and potential quantum threats. Classic McEliece has parameter sets to match all five NIST security levels and is by far the most researched candidate in this NIST process, and thus, has the highest level of assurance. Like other code-based cryptosystems, Classic McEliece has an extremely fast computation time, but also extremely large public key sizes which ranges from 250 KB for NIST security level 1 up to 1.3 MB for NIST security level 5.

- **CRYSTALS-KYBER** is a (structured) lattice-based public-key cryptosystem based on the hardness of solving the learning-with-errors problem over modules (M-LWE). CRYSTALS-KYBER is IND-CCA2 (indistinguishability under adaptive chosen ciphertext attack) and has three different parameter sets to match NIST security levels 1, 3, and 5. Lattice-based algorithms in general have a fast computation time (while not the fastest) and have a small public key (while not the smallest). CRYSTALS-KYBER does a good job at this trade off having its public key range from 800 bytes to 1.5 KB.

- **NTRU** is another structured lattice-based public-key cryptosystem which is IND-CCA2 secure. NTRU is based on the hardness of solving the Ring-learning-with-errors problem (Ring-LWE) and variants have been around since the mid-1990s, giving some confidence to its security. There were several candidates during Round 1 based off of the original NTRU cryptosystem, and in fact this candidate is the result of a merger of NTRUEncrypt and NTRU-HRSS-KEM before the beginning of Round 2.

- **SABER** is the third structured lattice-based KEM and relies on the hardness of the Module-learning-with-rounding problem (M-LWR) which is a variant of the LWE problem. There are three versions of SABER: LightSABER (NIST security level 1), SABER (NIST security level 3), and FireSABER (NIST security level 5).

Alternate Candidates:

- **BIKE** is a code-based IND-CCA (indistinguishability against chosen ciphertext attack) secure KEM based on quasi-cyclic moderate density parity-check codes (QC-MDPC). BIKE has parameters that target security levels 1 and 3.
- **FrodoKEM** is an IND-CCA secure KEM based on unstructured lattice and thus has a larger public key but less parameter restrictions. FrodoKEM targets security levels 1, 3, and 5.
- **HQC** is an IND-CPA (indistinguishability against chosen plaintext attack) code-based KEM targeting NIST levels 1, 3, and 5. The public key and ciphertexts are slightly larger than BIKE, but also has some advantages for efficiency.
- **NTRU Prime** is a tweak on the original NTRU proposed in the 1990s to use rings without the same required structures. NTRU Prime is also IND-CCA2
- **SIKE** is the only isogeny-based KEM. Isogenies can be thought of as maps between elliptic curves and thus shares some operations with typical elliptic curve cryptography. SIKE has the smallest public-key of all candidates but is also the slowest.

Round 3 Finalists: Digital Signature Algorithms

- **CRYSTALS-DILITHIUM** is a DSA that is strongly secure under chosen message attacks based on the hardness of lattice problems over module lattices.
- **FALCON** is a lattice DSA based on the hard problem of short integer solutions (SIS) over NTRU lattices. This gives Falcon short signatures and fast implementations; however, its side-channel resistance needs to be studied further. Falcon meets NIST security levels 1, 3, and 5.
- **Rainbow** is a multivariate DSA that is based on the unbalanced oil-vinegar (UOV) signature scheme, with layered UOV structures. Rainbow has been around since 2005 and has needed very few changes. It has small signatures and a fast signing/verification process but has large public and private keys.

Alternate Candidates:

- **GeMSS** is another multivariate DSA with small signatures and fast verification, but public keys are a bit larger. GeMSS is based on the hidden Field equation cryptosystem (HFEv-) using minus and vinegar modifiers.
- **Picnic** is a DSA based on the idea of zero-knowledge proofs which doesn't require number-theoretic, or structured hardness assumptions.
- **SPHINCS+** is a stateless hash-based DSA based on the original algorithm SPHINCS with some improvements to make the security more robust while still keeping the public key size the same.

What's Next?

"The finalists will continue to be reviewed for consideration for standardization at the conclusion of the third round," said NIST mathematician Dustin Moody. His email went on to state "As CRYSTALS-KYBER, NTRU, and SABER are all structured lattice schemes, NIST intends to select, at most, one for the standard. The same is true for the signature schemes CRYSTALS-DILITHIUM and FALCON." This leads to the assumption that NIST plans to standardize at most two KEMs (one code-based and one lattice-based) and at most two DSAs (one lattice-based and one multivariate) by the end of the 12-18 month Round 3 process.

NIST continued to state the alternate candidates will be considered for standardization during a Round 4, which will give them more time for further improvements. It is reasonable to assume this round will focus on the category types that had nothing standardized in Round 3 such as isogeny-based, zero-knowledge, or hash-based, if lattice-based, code-based, and multivariate schemes were standardized.

NIST requested any "tweaks" to specifications or implementations to be completed by October 1, 2020 for the remaining candidates and expects to hold a 3rd NIST PQC Standardization Conference in 2021, subject to the current global situation.