**Share inquiry or 3rd party draft with local MR and DSS Marcom HQ**

# Post-quantum cryptography: Status of the NIST standardization process

by Thomas Poeppelmann, March 2020

Quantum computers may have the potential to break cryptographic schemes like RSA or elliptic curve cryptography (ECC), which are widely used for encrypting digital communication. Although this threat may only become a reality in 15 to 20 years, researchers in academia, industry and government organizations are already working intensely on quantum-safe security schemes and their standardization.

Quantum-safe cryptography is often called post-quantum cryptography (PQC). PQC comprises public-key encryption or digital signature algorithms that rely on the hardness of sophisticated mathematically problems. It is assumed that these problems are intractable for both quantum and classical computers. To facilitate the development of new quantum-safe and practical schemes the National Institute of Standards and Technology (NIST) has started a standardization process in 2016. In their call for submissions, NIST asked researchers to submit schemes that could become a new standard and thus replace current schemes that are vulnerable to attacks by quantum computers. This process is open to submitters from all over the world and it follows the spirit of previous competitions that have led to the standardization of the widely adopted block cipher Advanced Encryption Standard (AES) or recently standardized hash algorithm SHA-3 (SHA, Secure Hash Algorithm). However, the scope of the PQC standardization process is much wider than in previous competitions. This is because NIST is asking in parallel for public-key encryption and digital signature schemes. Moreover, the solution space for PQC algorithms is much broader than for block ciphers or hash functions. Thus, NIST may alter the rules and selection criteria based on new research and will most likely not pick one winner. Moreover, NIST stated that the process should not be seen as a competition, but rather as an effort of the community to find several algorithms suitable for future use. Currently, the assessment of the security of post-quantum cryptographic schemes is a hard task as no practical experience with quantum computers is available and as the very diverse underlying mathematical problems need to be studied very carefully over a long period of time. NIST is also explicitly asking the cryptographic community and industry to provide feedback on the suitability of these submissions. This feedback can be provided either over a public mailinglist (pqc-forum)[1], by submitting presentations or by approaching NIST during conferences.

## The PQC standardization process

In December 2017, NIST published 69 submissions as first-round candidate schemes that met minimal formal standards. Overall, 278 individual submitters from 25 countries and 6 continents with academic, industry and government affiliations were involved in the design of the submissions.


Interestingly, after the first three weeks of round 1 already twelve schemes had been broken or significantly attacked. Such attacks or vulnerabilities in implementations were mainly communicated over the pqc-forum. In addition, the community used the forum to discuss advantages and disadvantages of proposed schemes or their underlying basic mathematical problems as well as practical matters. This

[1]See https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Email-List

makes the forum one of the primary sources on news in academic post–quantum cryptography and allows easy access to statements and contributions of key experts. At the end of round 1 there were over 1000 posts including over 300 official comments on the pqc-forum.

For round 2 of the standardization process, NIST selected the 26 most promising schemes out of the 69 remaining submissions[2], in January 2019. The main selection criteria were cryptographic strength but also aspects like cost and performance as well as algorithm and implementation characteristics, e.g. simplicity.

Notably, the overall timeline of the standardization process still stands with the goal of having draft standards available in 2022/2024. The goal in the 3rd Round is to focus further on schemes that are ready for standardization and it is anticipated that NIST will further reduce the pool of candidate schemes.

| Name of scheme | Mathematical Problem | Sub-Category |
|---|---|---|
| CRYSTALS- DILITHIUM | Lattice | Fiat-Shamir |
| qTESLA | Lattice | Fiat-Shamir |
| FALCON | Lattice | Hash-then-sign |
| MQDSS | Multivariate | Fiat-Shamir |
| LUOV | Multivariate | Unbalanced Oil and Vinegar (UOV) |
| Rainbow | Multivariate | Unbalanced Oil and Vinegar (UOV) |
| GeMSS | Multivariate | Hidden-Field-Equations (HFE) |
| Picnic | Symmetric | Zero Knowledge Proof (ZKP) |
| SPHINCS+ | Symmetric | Hash |
| CRYSTALS-KYBER | Lattice | Modular Learning with Errors (MLWE) |
| SABER | Lattice | Modular Learning with Rounding (MLWR) |
| FrodoKEM | Lattice | Learning with Errors (LWE) |
| Round5 | Lattice | General Learning with Rounding (GLWR)/Ring Learning with Rounding (RLWR) |
| LAC | Lattice | Ring Learning with Errors (RLWE) |
| NewHope | Lattice | Ring Learning with Errors (RLWE) |
| Three Bears | Lattice | Integer Modular Learning with Errors (IMLWE) |
| NTRU | Lattice | NTRU |
| NTRU Prime | Lattice | NTRU |
| Classic McEliece | Codes | Goppa codes |
| NTS-KEM | Codes | Goppa codes |
| BIKE | Codes | Short Hamming codes |
| HQC | Codes | Short Hamming codes |
| LEDAcrypt | Codes | Short Hamming codes |
| ROLLO | Codes | Low rank codes |
| RQC | Codes | Low rank codes |
| SIKE | Isogeny | Supersingular Isogeny |

*Table: Schemes in Round 2 of the NIST standardization process: Infineon is contributing to New Hope and SPHINCS+*

Other standardization bodies involved in PQC standardization are ETSI and ISO who run study groups dedicated to PQC. However, currently it seems that ETSI and ISO will rely on NIST for the initial selection of algorithms. Moreover, stateful hash-based signatures, a special class of signature schemes with certain limitations, are currently in standardization at the Internet Engineering Task Force (IETF) and NIST and so standards are expected earlier than the NIST PQC process. Additionally, several European research projects, e.g. PROMETHEUS and FutureTPM are currently investigating the efficiency, security, and practicability of PQC schemes. Moreover, several PQC-related publicly funded projects (Aquorypt, QuaSiModO, QuantumRISC, PQC4MED, FLOQI, SIKRIN-KRYPTOV, and KBLS) have recently been started after a call for proposal by the German Federal Ministry of Education and Research had been issued.

[2] [pqc-forum] Announcement of 2nd Round Candidates, 'Moody, Dustin (Fed)' via pqc-forum pqc-forum@list.nist.gov, 30.01.2019