[NIST Post-Quantum Cryptosystem (PQC) Competition Round 2](https://csrc.nist.gov/news/2019/pqc-standardization-process-2nd-round-candidates) (Semi-final)  
([*see Round 1 for more details*](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions))

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Public-Key Encryption** | | | | |
| **Lattice-based/Ring-LWE** | | **Code-based** | | **Other** |
| **1** | [NTRU Prime](https://ntruprime.cr.yp.to/) | (R-lattice) | [Classic McEliece](https://classic.mceliece.org/) | (Binary Goppa) |  |
| **2** | [NTRU](https://www.onboardsecurity.com/nist-post-quantum-crypto-submission)  *European Encryption Standard* | (R-lattice) | [HQC](http://pqc-hqc.org/) | (BCH & cyclic) |  |
| **3** | [LAC](https://cs.rit.edu/~ats9095/csci762/pdfs/LAC.pdf) | (R-LWE) | [RQC](http://pqc-rqc.org/) | (cyclic) |  |
| **4** | [SABER](https://www.esat.kuleuven.be/cosic/publications/article-2877.pdf) | (Mod-LWR) | [LEDA](https://www.ledacrypt.org/LEDApkc/) | (LDPC) |  |
| **5** | [Round5](https://round5.org/) | (R-LWR) | [ROLLO  (LAKE & LOCKER)](https://csrc.nist.gov/CSRC/media/Presentations/LAKE-and-LOCKER/images-media/Lake-and-Locker-April2018.pdf) | (LRPC) |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Key Establishment/Encapsulation** | | | | |
| **Lattice-based/Ring-LWE** | | **Code-based** | | **Other** |
| **1** | [NewHope](https://newhopecrypto.org/) | (R-LWE) | [BIKE](https://bikesuite.org/) | (MDPC) | [SIKE](https://sike.org/) (Isogeny) |
| **2** | [NTRU](https://www.onboardsecurity.com/nist-post-quantum-crypto-submission)  *European Encryption Standard* | (R-lattice) | [NTS-KEM](https://nts-kem.io/) | (Binary Goppa) |  |
| **3** | [FrodoKEM](https://frodokem.org/) | (R-LWE) | [LEDA](https://www.ledacrypt.org/LEDAkem/) | (LDPC) |  |
| **4** | [CRYSTALS-KYBER](https://pq-crystals.org/) | (R-LWE) | [ROLLO  (LAKE & LOCKER)](https://csrc.nist.gov/CSRC/media/Presentations/LAKE-and-LOCKER/images-media/Lake-and-Locker-April2018.pdf) | (LRPC) |  |
| **5** | [SABER](https://www.esat.kuleuven.be/cosic/publications/article-2877.pdf) | (Mod-LWR) |  |  |  |
| **6** | [Three Bears](https://sourceforge.net/p/threebears/code/ci/master/tree/threebears-spec.pdf) | (Mod-LWE) |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Digital Signature** | | | |
| **Lattice-based/Ring-LWE** | | **Multivariate-based** | **Hash-based** |
| **1** | [FALCON](https://falcon-sign.info/) | (NTRU R-lattice) | [GeMSS](https://www-polsys.lip6.fr/Links/NIST/GeMSS.html) | [Picnic](https://microsoft.github.io/Picnic/) |
| **2** | [qTESLA](https://qtesla.org/) | (R-LWE) | [MQDSS](http://mqdss.org/) | [SPHINCS+](https://sphincs.org/) |
| **3** | [CRYSTALS-DILITHIUM](https://pq-crystals.org/) | (R-LWE) | [LUOV](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions) |  |
| **4** |  |  | [Rainbow](https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions) |  |