|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Alg.  types | Algorithms names | Alg.  subtypes | Claimed NIST security level | Public key size (bytes) | Private key size (bytes) | Ciphertext size (bytes) | Shared secret size (bytes) |
| KEM | Classic McEliece | Code-based | 1, 3, 5 | 261120~1357824 | 6452~14080 | 128~240 | 32 |
| CRYSTALS-KYBER | Lattice-based | 1, 3, 5 | 800~1568 | 1632~3168 | 768~1568 | 32 |
| NTRU | Lattice-based | 1, 3, 5 | 699~1138 | 935~1450 | 699~1138 | 32 |
| SABER | Lattice-based | 1, 3, 5 | 672~1312 | 1568~3040 | 736~1472 | 32 |
| BIKE | Code-based | 1, 3 | 2542~6206 | 3110~13236 | 2542~6206 | 32 |
| FrodoKEM | Lattice-based | 1, 3, 5 | 9616~21520 | 19888~43088 | 9720~21632 | 16, 24, 32 |
| HQC | Code-based | 1, 3, 5 | 2249~7425 | 2289~7285 | 4481~14469 | 64 |
| NTRU Prime | Lattice-based | 2, 3, 4 | 897~1322 | 1125~1999 | 897~1184 | 32 |
| SIKE | SECI-based | 1, 2, 3, 5 | 197~564 | 350~644 | 236~596 | 16, 24, 32 |