



THE POST-QUANTUM CRYPTOGRAPHY ALGORITHM CHEAT SHEETS

Mario Schiener

10 November 2024
v0.6 *Draft*

THE PQC ALGORITHM CHEAT SHEETS



SYMBOLS

General color coding

Best to Worst: ■ ■ ■ ■ Links and TBDs: ■

Symbols

- | | |
|--|-----------------------------|
| ⓘ Recommendations differ depending on organization | 🔑 Key / Key Generation |
| ⚙️ Parameter set | 🔒 Decryption |
| 🔒 Encryption / Ciphertext | ❓ Verification |
| ✍️ Signing / Signature | 🖨️ CPU Cycles |
| 📅 Not yet standardized by NIST | 🌀 Implementation complexity |
| 🔗 Implementation Code | |
| 📏 Implementation size | |

Security categories of parameter sets

V IV III II I NIST Security Categories V, IV, III, II, I

Higher is more secure.

Implementation complexity and size

C^{*} M^{*} H^{*} Low/Medium/High implementation complexity
S^{*} M^{*} H^{*} Low/Medium/High implementation size

Lower is better. * can be 🔑, ✍️, ❓, 🔒, or 🖨️.

Rating scales for parameter sizes and performance

Best to Worst: ■ $n \leq 2$, ■ $n \in \{3, 4\}$, ■ $n \in \{5, 6\}$, ■ $n \in \{7, 8\}$, ■ $n \geq 9$

- | | |
|--------------------------|--|
| $\mathcal{O}(5^n)$ | CPU kilo cycles for key generation |
| $\mathcal{O}(5^n)$ | CPU kilo cycles for signing |
| $\mathcal{O}(5^n)$ | CPU kilo cycles for signature verification |
| $\mathcal{O}(5^n)$ | CPU kilo cycles for encryption / key encapsulation |
| $\mathcal{O}(5^n)$ | CPU kilo cycles for decryption / key decapsulation |
| $\mathcal{O}(2^n)$ | KB of signature size |
| $\mathcal{O}(2^n)$ | KB of ciphertext size |
| $\mathcal{O}(2^{(n-5)})$ | KB of signature algorithm public key size |
| $\mathcal{O}(2^n)$ | KB of encryption algorithm public key size |

HOW TO INTERPRET THE CHEAT SHEETS

The goal of this series of cheat sheets is to make it as easy as possible to figure out which algorithm to pick for a given use case. Algorithm ID cards break down algorithm parameter sets, their important values and performance characteristics. The cheat sheets are intended to help users primarily in technical roles, such as engineers, architects or software developers working with post-quantum cryptography.

The focus is to avoid giving specific numbers measured in bits, bytes or cycles as this makes comparing numbers across algorithms difficult. Instead, this complexity is simplified by only providing a **color-coded number indicating the order of magnitude of each metric**. Furthermore, an **“Algorithm Overall Usability Score”** is assigned to each algorithm. This score aims to make it visible at first glance how good of an overall package the algorithm offers (refer to the appendix for the definition of the score).

This approach prioritizes easy interpretation and comparability of metrics and in general quick informational gain over absolute precision of data – remember this is a cheat sheet, not a standard! This document is not intended to replace the study of algorithm specifications. It just aims to point you in the right direction quickly.

The approach of focusing on orders of magnitude walks a fine line between treating too many things as “equal” and not simplifying things enough to be easy to read and compare. “In the same order of magnitude” usually refers to “equal up to a factor of at most 10”, which is a very coarse way of comparing numbers. Treating metrics that differ by a factor of e.g. 9.9 as “equal” because $9.9 < 10$ paints a distorted picture. In cryptography, factors of 5 or even 2 can make a significant difference in security or performance, both in theory and in practice. In order to still tease out the differences in metrics without throwing too many things together that actually differ significantly, this cheat sheet applies different scaling and “orders of magnitude” (i.e., not regarding base 10) for different metrics.

It turns out that for **metrics measured in (kilo) CPU cycle counts, i.e. algorithm performance**, “up to a factor of 5” is a scale that is granular enough to work out the differences between algorithms while maintaining easy comparability. Those cycle counts heavily depend on the CPU used during measurement, hence the numbers need to be taken with a grain of salt, even if given exactly and not in terms of orders of magnitude.

For **signature and ciphertext sizes as well as key sizes, measuring numbers in kilobytes** “up to a factor of 2” is well suited to work out the differences between algorithms while allowing for quick comparison. Specifically for signature public key sizes only, we offset the corresponding color coding by 5 orders of magnitude. This is because SLH-DSA has extremely small public keys compared to all other signature algorithms, which would extend the scale into negative numbers (e.g. for SLH-DSA-SHA2-128s, the public key has $32=2^5$ bytes, which corresponds to an order of magnitude of -5 when measuring in orders of magnitude of base 2 and in kilobytes). This phenomenon of algorithm metrics spanning a very large range of orders of (base 2) magnitudes does not occur to this extent for encryption algorithms, making an offset unnecessary.

All values thus have a lower bound of 0. We do not limit the upper end of scales, but don’t distinguish values greater than 10 anymore in terms of color coding. Please refer to the definitions on the left for symbol explanations, color coding and interpretation of numeric values.

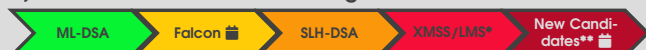


ALGORITHM CHOICE GUIDANCE: RULES OF THUMB

The following orders of preference should be considered as general rules of thumb applicable to most use cases. They should however not be considered to be universal truths. Unstandardized algorithms are listed for the sake of completeness. All information is valid at the time of writing (10 November 2024) only. Note that cryptography may become obsolete in the future.

SIGNATURE ALGORITHMS

Objective: Best All-Around Package



Objective: Performance of Key Generation



Objective: Performance of Signing



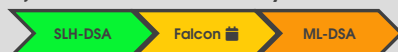
Objective: Performance of Verification



Objective: Small Signatures



Objective: Small Public Keys



* XMSS/LMS is not suitable for general purpose signatures
** Security still unclear, none recommended yet at the moment

ENCRYPTION/KEY ENCAPSULATION ALGORITHMS

Objective: Best All-Around Package



Objective: Performance of Key Generation



Objective: Performance of Encryption



Objective: Performance of Decryption



Objective: Small Ciphertext



Objective: Small Public Keys



* Classic McEliece is only suitable for general encryption with limitations

SECURITY CATEGORY CHOICES

- As a baseline, first consider using parameters.
- Use or for more security if possible (i.e., if a decrease in performance is not a concern and if no constraints apply).
- Use or if and only if or higher is not an option due to constraints (e.g. performance, memory, etc.).
- Comparing post-quantum security categories of algorithms to their traditional security level in bits is a complex subject and like comparing apples and oranges to some degree.

PURE VS. PRE-HASHING

- First, consider using pure** (i.e., without pre-hashing) as this is the general recommendation.
- Pre-Hashing may be considered if one or more of the following apply:**
 - The message M is too large to be sent to the cryptographic module (CM) for hashing without significantly impacting performance. This may be the case e.g. in CMS related use cases such as S/MIME or code signing, or in cases of very narrow communication channels to the CM (e.g. between APDUs exchanged between smartcard and smartcard reader).
 - The hash needs to be signed with different algorithms and would be computed repeatedly without pre-hashing.
 - The specific hash function is not supported in a CM.

PURE PQC vs PQ/T HYBRID

This topic depends on too many factors (e.g. cost of migration, security considerations, risk profile, GRC requirements) to give general advice. Those aspects will differ greatly between different organizations. The main reasons to adopt PQ/T hybrids are to still have traditional algorithms in place in case a new algorithm turns out to be insecure, and that PQ/T might help to avoid a big bang migration as systems could simply ignore the PQC component if they do not support it yet. Consider recommendations from different government agencies: BSI and ANSSI recommend PQ/T hybrid strategies, whereas NIST is more reserved towards PQ/T. **If using PQ/T hybrids, preferably use ECC (e.g. secp256r1, brainpoolP256r1, Curve25519) instead of RSA for the traditional component to keep key sizes as small as possible.**

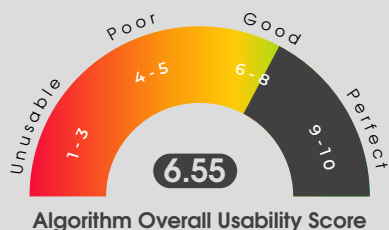


SIGNATURE ALGORITHMS

ID Cards



ML-DSA (MODULE-LATTICE-BASED DIGITAL SIGNATURE ALGORITHM)



PREVIOUS NAME CRYSTALS-DILITHIUM
SPECIFICATION [FIPS 204](#)
TYPE Signature
FAMILY Lattice
SUITABLE FOR GENERAL USE Yes
STANDARDIZATION STATUS Standardized
RECOMMENDED BY NIST, BSI, ANSSI
HASHING Pure, Pre-Hashing
NAMING by $k \times l$ matrix A
 (e.g. $6 \times 5 \rightarrow$ ML-DSA-65)

IMPLEMENTATION



COMPLEXITY



SIZE



PARAMETER SET	OID	SECURITY CATEGORY	PERFORMANCE	SIGNATURE SIZE	PUBLIC KEY SIZE	PRE-HASHING
ML-DSA-44	2.16.840.1.101.3.4.3.17 2.16.840.1.101.3.4.3.32					SHA512
ML-DSA-65	2.16.840.1.101.3.4.3.18 2.16.840.1.101.3.4.3.33					SHA512
ML-DSA-87	2.16.840.1.101.3.4.3.19 2.16.840.1.101.3.4.3.34					SHA512

👍 / Pros / Use If:

- You need a general-purpose signature algorithm with decent specs in all categories
- Usually the best option for a signature algorithm in most protocols (e.g. TLS, SSH, S/MIME, etc.).
- Good choice for X.509 certificates, including CA certificates.

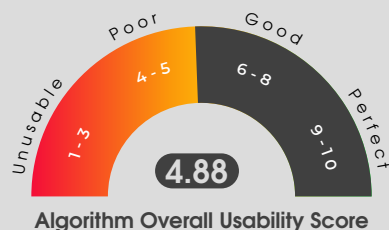
👎 / Cons / Don't Use If:

- You don't want a lattice-based algorithm

THE PQC ALGORITHM CHEAT SHEETS



SLH-DSA (STATELESS HASH-BASED DIGITAL SIGNATURE STANDARD)



PREVIOUS NAME SPHINCS+
SPECIFICATION [FIPS 205](#)
TYPE Signature
FAMILY Hash (stateless)
SUITABLE FOR GENERAL USE Yes
STANDARDIZATION STATUS Standardized
RECOMMENDED BY NIST, BSI, ANSSI
HASHING Pure, Pre-Hashing
NAMING based on various characteristics (*s=small signatures, *f=fast)

IMPLEMENTATION

🔑 ✎ ?

COMPLEXITY

Ⓢ? Ⓢ? Ⓢ?

SIZE

Ⓢ? Ⓢ? Ⓢ?

PARAMETER SET	OID (PURE, <i>PRE-HASH</i>)	SECURITY CATEGORY	PERFORMANCE 🔑 ✎ ?	SIGNATURE SIZE	PUBLIC KEY SIZE	PRE-HASHING
SLH-DSA-SHA2-128s	2.16.840.1.101.3.4.3.20 2.16.840.1.101.3.4.3.35	I	8 9 5	2	0	SHA-256
SLH-DSA-SHA2-128F	2.16.840.1.101.3.4.3.21 2.16.840.1.101.3.4.3.36	I	5 7 5	4	0	SHA-256
SLH-DSA-SHA2-192s	2.16.840.1.101.3.4.3.22 2.16.840.1.101.3.4.3.37	III	8 9 5	4	0	SHA-512
SLH-DSA-SHA2-192F	2.16.840.1.101.3.4.3.23 2.16.840.1.101.3.4.3.38	III	5 7 6	5	1	SHA-512
SLH-DSA-SHA2-256s	2.16.840.1.101.3.4.3.24 2.16.840.1.101.3.4.3.39	V	7 9 5	4	0	SHA-512
SLH-DSA-SHA2-256F	2.16.840.1.101.3.4.3.25 2.16.840.1.101.3.4.3.40	V	6 8 6	5	1	SHA-512
SLH-DSA-SHAKE-128s	2.16.840.1.101.3.4.3.26 2.16.840.1.101.3.4.3.41	I	8 9 5	2	0	SHAKE128
SLH-DSA-SHAKE-128F	2.16.840.1.101.3.4.3.27 2.16.840.1.101.3.4.3.42	I	5 7 5	4	0	SHAKE128
SLH-DSA-SHAKE-192s	2.16.840.1.101.3.4.3.28 2.16.840.1.101.3.4.3.43	III	8 9 5	4	0	SHAKE256
SLH-DSA-SHAKE-192F	2.16.840.1.101.3.4.3.29 2.16.840.1.101.3.4.3.44	III	5 7 6	5	1	SHAKE256
SLH-DSA-SHAKE-256s	2.16.840.1.101.3.4.3.30 2.16.840.1.101.3.4.3.45	V	7 9 5	4	0	SHAKE256
SLH-DSA-SHAKE-256F	2.16.840.1.101.3.4.3.31 2.16.840.1.101.3.4.3.46	V	6 8 6	5	1	SHAKE256

👍 / Pros / Use If:

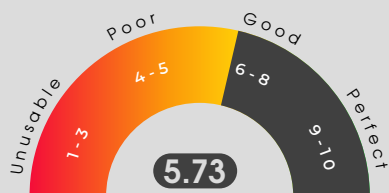
- Alternative to ML-DSA and Falcon that is not based on lattices
- Very small public keys
- Generally good for use in most protocols, even if ML-DSA is the preferred option.
- Use as a more conservative choice in use cases with less frequent algorithm execution, i.e. where latency or message size are not a big concern. For example, S/MIME, document or code signing, creation of CAs.

👎 / Cons / Don't Use If:

- Poor key generation and signing performance compared to other algorithms
- High complexity of the algorithm and the implementation
- Possible interoperability issues due to the many variants that may not all be supported everywhere



FALCON (FAST-FOURIER LATTICE-BASED COMPACT SIGNATURES OVER NTRU)



PREVIOUS NAME Falcon
SPECIFICATION [Project Page](#)
TYPE Signature
FAMILY Lattice
SUITABLE FOR GENERAL USE Yes
STANDARDIZATION STATUS Pending
RECOMMENDED BY TBD
HASHING TBD
NAMING TBD

IMPLEMENTATION

COMPLEXITY

SIZE

PARAMETER SET	OID	SECURITY CATEGORY	PERFORMANCE			SIGNATURE SIZE	PUBLIC KEY SIZE	PRE-HASHING
FALCON-512	TBD							TBD
FALCON-1024	TBD							TBD

👍 / Pros / Use If:

- Generally good for use in most protocols (e.g. TLS, SSH, S/MIME, etc.). Exceptions may apply in cases of repeated generation of ephemeral keys (poor performance).
- Falcon has smaller signature sizes than ML-DSA:
 vs. resp.
- Falcon has smaller public key sizes than ML-DSA:
 vs. on Level I, vs. on Level V.

👎 / Cons / Don't Use If:

- You need a medium security category between and .
- The algorithm is not yet standardized
- The algorithm requires expensive floating point arithmetic
- Key generation and signing are slower than for ML-DSA
- Less suitable in applications involving the creation of lots of ephemeral keys/certificates (key generation is slow).



XMSS / XMSS-MT (eXTENDED MERKLE SIGNATURE SCHEME / eXTENDED MERKLE SIGNATURE SCHEME MULTI TREE)



Algorithm Overall Usability Score

PREVIOUS NAME XMSS/XMSSMT
SPECIFICATION [SP 800-208](#), [RFC 8391](#)
TYPE Signature
FAMILY Merkle Trees (stateful hash trees)
SUITABLE FOR GENERAL USE No
STANDARDIZATION STATUS Standardized
RECOMMENDED BY NIST, BSI, ANSSI
HASHING TBD
NAMING XMSS-[Hashfamily]_[h]_[n]
 XMSSMT-[Hashfamily]_[h]/[d]_[n]
 where h is the tree height,
 d is the number of layers, and
 n is the message length in bits

IMPLEMENTATION



COMPLEXITY



SIZE



PARAMETER SET	NUMERIC IDENTIFIER	SECURITY CATEGORY	PERFORMANCE			SIGNATURE SIZE	MAXIMUM SIGNATURES	NUMBER OF LAYERS
XMSS-SHA2_10_256	0x00000001						2 ¹⁰	1
XMSS-SHA2_16_256	0x00000002						2 ¹⁶	1
XMSS-SHA2_20_256	0x00000003						2 ²⁰	1
XMSSMT-SHA2_20/2_256	0x00000001						2 ²⁰	2
XMSSMT-SHA2_20/4_256	0x00000002						2 ²⁰	4
XMSSMT-SHA2_40/2_256	0x00000003						2 ⁴⁰	2
XMSSMT-SHA2_40/4_256	0x00000004						2 ⁴⁰	4
XMSSMT-SHA2_40/8_256	0x00000005						2 ⁴⁰	8
XMSSMT-SHA2_60/3_256	0x00000006						2 ⁶⁰	3
XMSSMT-SHA2_60/6_256	0x00000007						2 ⁶⁰	6
XMSSMT-SHA2_60/12_256	0x00000008						2 ⁶⁰	12

NOTE:

[SP 800-208](#) defines further parameter sets not listed in [RFC 8391](#) using other hash functions (SHA256/192, SHAKE256/256, SHAKE256/192). Furthermore, [RFC 8391](#) lists optional parameter sets that are not approved in [SP 800-208](#). All of those variants are omitted here as they are not likely to be widely used, in particular not after ML-DSA and SLH-DSA have been standardized in the meantime.

👍 / Pros / Use If:

- You can predict the maximum number of signatures that are going to be required
- Firmware signing use cases
- You want a signature scheme where the security only relies on the security of the hash function used without assuming the hardness of another mathematical problem.
- Cf. [SP 800-208, Section 1.1](#) for additional explanations

👎 / Cons / Don't Use If:

- You require an algorithm for general use
- You cannot predict the maximum number of signatures that are going to be required, or the number of required signatures exceeds the maximum number of signatures enabled through the approved parameter sets
- Your application does not allow for the careful state management and tracking of signatures performed that is required with this algorithm



LMS/HSS (LEIGHTON-MICALI SIGNATURE / HIERARCHICAL SIGNATURE SYSTEM)



Algorithm Overall Usability Score

PREVIOUS NAME LMS, LMS/HSS
SPECIFICATION [SP 800-208](#), [RFC 8554](#)
TYPE Signature
FAMILY Merkle Trees (stateful hash trees)
SUITABLE FOR GENERAL USE No
STANDARDIZATION STATUS Standardized
RECOMMENDED BY NIST, BSI, ANSSI
HASHING TBD
NAMING LMS_SHA256_M32_[h]
 where h is the tree height

IMPLEMENTATION



COMPLEXITY



SIZE



PARAMETER SET	NUMERIC IDENTIFIER	SECURITY CATEGORY	PERFORMANCE	SIGNATURE SIZE	MAXIMUM SIGNATURES
LMS_SHA256_M32_H5	0x00000005				2 ⁵
LMS_SHA256_M32_H10	0x00000006				2 ¹⁰
LMS_SHA256_M32_H15	0x00000007				2 ¹⁵
LMS_SHA256_M32_H20	0x00000008				2 ²⁰
LMS_SHA256_M32_H25	0x00000009				2 ²⁵

NOTE:

[SP 800-208](#) defines further parameter sets not listed in [RFC 8554](#) using other hash functions (SHA256/192, SHAKE256/256, SHAKE256/192). Those variants are omitted here as they are not likely to be widely used, in particular not after ML-DSA and SLH-DSA have been standardized in the meantime. Similar to XMSS multi-tree variants, a comparable structure exists with Hierarchical Signature System (HSS) variants of LMS that involves a number of LMS instances.

👍 / Pros / Use If:

- You can predict the maximum number of signatures that are going to be required
- Firmware signing use cases
- You want a signature scheme where the security only relies on the security of the hash function used without assuming the hardness of another mathematical problem.
- Cf. [SP 800-208, Section 1.1](#) for additional explanations

👎 / Cons / Don't Use If:

- You require an algorithm for general use
- You cannot predict the maximum number of signatures that are going to be required, or the number of required signatures exceeds the maximum number of signatures enabled through the approved parameter sets
- Your application does not allow for the careful state management and tracking of signatures performed that is required with this algorithm

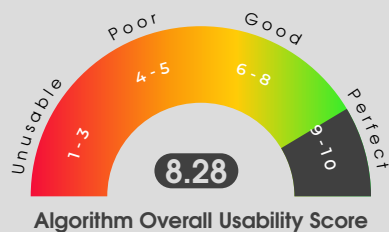


ENCRYPTION / KEM ALGORITHMS

ID Cards



ML-KEM (MODULE-LATTICE-BASED KEY-ENCAPSULATION MECHANISM STANDARD)



PREVIOUS NAME CRYSTALS-KYBER
SPECIFICATION [FIPS 203](#)
TYPE Encryption/KEM
FAMILY Lattice
SUITABLE FOR GENERAL USE Yes
STANDARDIZATION STATUS Standardized
RECOMMENDED BY NIST, BSI, ANSSI
NAMING TBD

IMPLEMENTATION



COMPLEXITY



SIZE



PARAMETER SET	OID	SECURITY CATEGORY	PERFORMANCE			CIPHERTEXT SIZE	PUBLIC KEY SIZE
			Key Gen	Enc	Dec		
ML-KEM-512	2.16.840.1.101.3.4.4.7	I	2	2	2	0	0
ML-KEM-768	2.16.840.1.101.3.4.4.2	III	2	2	3	0	0
ML-KEM-1024	2.16.840.1.101.3.4.4.3	V	3	3	3	0	0

👍 / Pros / Use If:

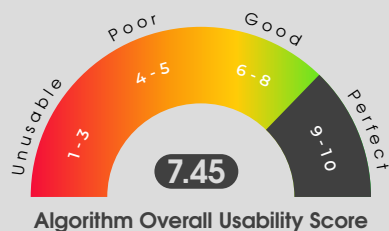
- Currently the only post-quantum encryption/key encapsulation algorithm standardized by NIST
- Need a general-purpose encryption / key-encapsulation algorithm with decent specs in all categories
- Usually the best choice in most protocols involving an encryption/KEM component (e.g. TLS, S/MIME, etc.)

👎 / Cons / Don't Use If:

- You don't want a lattice-based algorithm



BIKE (BIT FLIPPING KEY ENCAPSULATION)



PREVIOUS NAME BIKE
SPECIFICATION [Project Page](#)
TYPE Encryption/KEM
FAMILY Codes
SUITABLE FOR GENERAL USE Yes
STANDARDIZATION STATUS 4th round candidate
RECOMMENDED BY NAMING TBD
 after security categories I, III and V

IMPLEMENTATION



COMPLEXITY



SIZE



PARAMETER SET	OID	SECURITY CATEGORY	PERFORMANCE			CIPHERTEXT SIZE	PUBLIC KEY SIZE
BIKE-L1	TBD	I	3	2	4	0	0
BIKE-L3	TBD	III	4	3	5	1	1
BIKE-L5	TBD	V	n/a	n/a	n/a	2	2

NOTE:

No data available for BIKE-L5 for cycle counts. The algorithm overall usability score is computed over BIKE-L1 and BIKE-L3 only.

👍 / Pros / Use If:

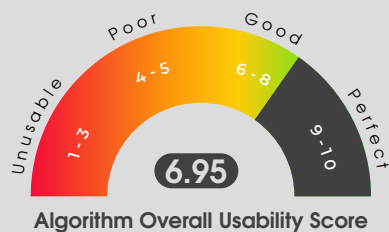
- Possible alternative to ML-KEM not based on lattices.

👎 / Cons / Don't Use If:

- Not yet standardized. Note that NIST intends to standardize at most one of the algorithms HQC and BIKE.
- Metrics not as good as the ones of ML-KEM.



HQC (HAMMING-QUASI-CYCLIC)



PREVIOUS NAME HQC
SPECIFICATION [Project Page](#)
TYPE Encryption/KEM
FAMILY Codes
SUITABLE FOR GENERAL USE Yes
STANDARDIZATION STATUS 4th round candidate
RECOMMENDED BY TBD
NAMING 128, 192 and 256 bits of security in reference to security categories I, III and V

IMPLEMENTATION



COMPLEXITY



SIZE



PARAMETER SET	OID	SECURITY CATEGORY	PERFORMANCE			CIPHERTEXT SIZE	PUBLIC KEY SIZE
HQC-128	TBD	I	2	3	3	2	1
HQC-192	TBD	III	3	3	4	3	2
HQC-256	TBD	V	3	4	4	3	2

👍 / Pros / Use If:

- Possible alternative to ML-KEM not based on lattices.

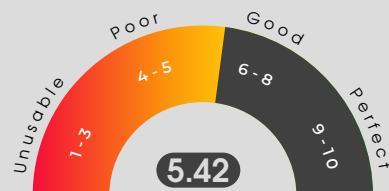
👎 / Cons / Don't Use If:

- Not yet standardized. Note that NIST intends to standardize at most one of the algorithms HQC and BIKE.
- Metrics not as good as the ones of ML-KEM.

THE PQC ALGORITHM CHEAT SHEETS



FRODOKEM



PREVIOUS NAME

FrodoKEM

SPECIFICATION

[Project Page](#)

TYPE

Encryption/KEM

FAMILY

Lattice

SUITABLE FOR GENERAL USE

Yes

STANDARDIZATION STATUS

Disregarded by NIST

RECOMMENDED BY

BSI, ANSSI

NAMING

FrodoKEM-[n]-[AES | SHAKE]
where n is a matrix dimension

IMPLEMENTATION



COMPLEXITY



SIZE



PARAMETER SET

OID

SECURITY CATEGORY

PERFORMANCE

CIPHERTEXT SIZE

PUBLIC KEY SIZE

FrodoKEM-640-AES	TBD	I	4	4	4	3	3
FrodoKEM-640-SHAKE	TBD	I	5	5	5	3	3
FrodoKEM-976-AES	TBD	III	4	4	4	3	3
FrodoKEM-976-SHAKE	TBD	III	6	6	6	3	3
FrodoKEM-1344-AES	TBD	V	5	5	5	4	4
FrodoKEM-1344-SHAKE	TBD	V	6	6	6	4	4

NOTE:

There are also ephemeral versions of FrodoKEM (eFrodoKEM-640, etc.), but BSI only recommends FrodoKEM-976 and FrodoKEM-1344 versions for long-term protection. The algorithm score also only includes the non-ephemeral versions listed above.

👍 / Pros / Use If:

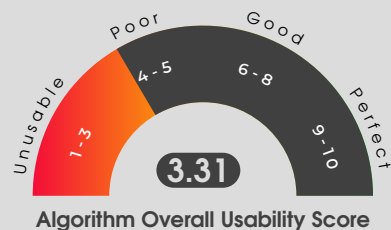
- More conservative than ML-KEM since it is based on unstructured grids

👎 / Cons / Don't Use If:

- Not standardized by NIST because ML-KEM is more efficient.



CLASSIC McELIECE



PREVIOUS NAME Classic McEliece
SPECIFICATION [Project Page](#)
TYPE Encryption/KEM
FAMILY Codes
SUITABLE FOR GENERAL USE No / With Limitations
STANDARDIZATION STATUS 4th round candidate (NIST)
RECOMMENDED BY BSI
NAMING mceliece[n][deg(F(y))][[f]]
 where n, F(y) are parameters
 non-f versions: $(\mu, \nu) = (0, 0)$
 f versions: $(\mu, \nu) = (32, 64)$

IMPLEMENTATION

COMPLEXITY

SIZE

PARAMETER SET	OID	SECURITY CATEGORY	PERFORMANCE			CIPHERTEXT SIZE	PUBLIC KEY SIZE
MCElIECE348864	TBD	I	6	2	3	0	8
MCElIECE348864F	TBD	I	6	n/a	n/a	0	8
MCElIECE460896	TBD	III	7	2	3	0	9
MCElIECE460896F	TBD	III	7	n/a	n/a	0	9
MCElIECE6688128	TBD	V	8	3	3	0	10
MCElIECE6688128F	TBD	V	7	n/a	n/a	0	10
MCElIECE6960119	TBD	V	7	3	3	0	10
MCElIECE6960119F	TBD	V	7	n/a	n/a	0	10
MCElIECE8192128	TBD	V	8	3	3	0	10
MCElIECE8192128F	TBD	V	8	n/a	n/a	0	10

NOTE:

No data available for the f versions for encryption/decryption cycle counts. The algorithm overall usability score is computed over non-f versions only. Non-f and f versions are interoperable, with f versions offering faster key generation and non-f versions having simpler key generation.

👍 / Pros / Use If:

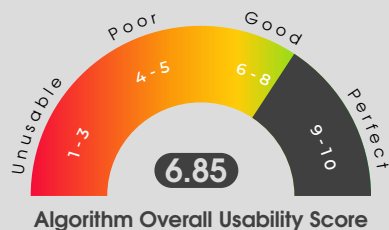
- Possible alternative to ML-KEM not based on lattices.
- Considered safe and recommended by BSI even though not standardized by NIST.
- Use cases that allow for pre-sharing of keys where the large public key size is not a concern.

👎 / Cons / Don't Use If:

- Not yet standardized by NIST.
- Not suitable for general use due to the very large public keys and poor performance of key generation.
- Due to aforementioned point, likely not suitable for embedded devices.



NTRU (NUMBER THEORY RESEARCH UNIT / NUMBER THEORISTS 'R' US)



PREVIOUS NAME NTRU
SPECIFICATION [Project Page](#)
TYPE Encryption/KEM
FAMILY Lattice
SUITABLE FOR GENERAL USE Yes
STANDARDIZATION STATUS Not Standardized
RECOMMENDED BY n/a
NAMING author initials and a prime number

IMPLEMENTATION



COMPLEXITY



SIZE



PARAMETER SET	OID	SECURITY CATEGORY	PERFORMANCE			CIPHERTEXT SIZE	PUBLIC KEY SIZE
NTRUHPS2048509	N/A	I	5	4	4	0	0
NTRUHRSS701	N/A	III	6	4	5	0	0
NTRUHPS2048677	N/A	III	6	4	5	0	0
NTRUHPS4096821	N/A	V	6	4	5	0	0

👍 / Pros / Use If:

- The intellectual property rights of ML-KEM have been unclear for a while, with NTRU being a possible backup alternative without such issues. This topic is now considered sufficiently clear and resolved by NIST. In case legal concerns about ML-KEM still apply in some exceptional cases, NTRU might be an option. However, ML-KEM is usually the better option in terms of technical aspects.

👎 / Cons / Don't Use If:

- Not standardized
- Performance not as good as ML-KEM, especially for key generation. Similarly, BIKE and HQC offer better metrics.



THE PQC ALGORITHM CHEAT SHEETS



OVERVIEW: HASH ALGORITHMS AND EXTENDABLE OUTPUT FUNCTIONS (XOF) TBV

FAMILY	VARIANT	OUTPUT SIZE [Bits]	ROUNDS	CONSTRUCTION	TRADITIONAL PRE-QUANTUM SECURITY [Bits]			POST-QUANTUM SECURITY [Bits]			PERFORMANCE
					COLLISION	PRE-IMAGE	2ND PRE-IMAGE	COLLISION	PRE-IMAGE	2ND PRE-IMAGE	
SHA-2	SHA-224	224	64	Merkle-Damgård Construction	112	224	224	74	112	112	7.62
	SHA-256	256	64	Merkle-Damgård Construction	128	256	256	85	128	128	7.63
	SHA-384	384	80	Merkle-Damgård Construction	192	384	384	128	192	192	5.12
	SHA-512	512	80	Merkle-Damgård Construction	256	512	512	170	256	256	5.06
	SHA-512/224	224	80	Merkle-Damgård Construction	112	224	224	TBD	TBD	TBD	≈ SHA-384
	SHA-512/256	256	80	Merkle-Damgård Construction	128	256	256	TBD	TBD	TBD	≈ SHA-384
SHA-3	SHA3-224	224	24	Keccak Sponge Construction	112	224	224	74	112	112	8.12
	SHA3-256	256	24	Keccak Sponge Construction	128	256	256	85	128	128	8.59
	SHA3-384	384	24	Keccak Sponge Construction	192	384	384	128	192	192	11.06
	SHA3-512	512	24	Keccak Sponge Construction	256	512	512	170	256	256	15.88
	SHAKE128	d (ARBITRARY)	24	Keccak Sponge Construction	$\min\left(\frac{d}{2}; 128\right)$	$\min\left(\frac{d}{2}; 128\right)$	$\min\left(\frac{d}{2}; 128\right)$	$\min\left(\frac{d}{3}; 128\right)$	$\min\left(\frac{d}{2}; 128\right)$	$\min\left(\frac{d}{2}; 128\right)$	7.08
	SHAKE256	d (ARBITRARY)	24	Keccak Sponge Construction	$\min\left(\frac{d}{2}; 256\right)$	$\min\left(\frac{d}{2}; 256\right)$	$\min\left(\frac{d}{2}; 256\right)$	$\min\left(\frac{d}{3}; 256\right)$	$\min\left(\frac{d}{2}; 256\right)$	$\min\left(\frac{d}{2}; 256\right)$	8.59

NOTES & TAKEAWAYS

- SHAKE128 and SHAKE256 are extendable output functions and allow for an arbitrary output size d .
- SHA-512/224 and SHA-512/256 denotes the truncation of the SHA-512 hash to 224 resp. 256 bits.
- Security against collision attacks is specified using values according to Brassard et al. ([Source](#))
- Performance is measured in median cycles/byte on a Skylake CPU ([Source](#)).
- Hash functions other than SHA-2 and SHA-3 variants (e.g. SHA-1, RipeMD-160, MD5, etc.) should generally be avoided as they are less secure. They are therefore not part of the above overview.

A large, stylized hexagonal graphic centered on the page. It is composed of six thick, slightly overlapping segments in a rainbow color scheme: blue at the top, followed by green, yellow, orange, red, and pink. The word "APPENDIX" is written in a bold, black, sans-serif font in the center of the hexagon.

APPENDIX

THE PQC ALGORITHM CHEAT SHEETS



TRADITIONAL VS. POST-QUANTUM SECURITY LEVEL COMPARISON TBV

TRADITIONAL PRE-QUANTUM SECURITY		ATTACK IN TERMS OF BIT SIZE n	ALGORITHM EXAMPLES	NIST SECURITY CATEGORIES DEFINED THROUGH ATTACK	POST-QUANTUM SECURITY			
Security [Bits]	Classical Attack Complexity				Classical Attack Improvement	Quantum Attack Complexity	Security [Bits]	Signature Parameter Sets
n	$\mathcal{O}(2^n)$	n -BIT KEY SPACE EXHAUSTIVE KEY SEARCH	AES		GROVER	$\mathcal{O}\left(2^{\frac{n}{2}}\right)$	$\frac{n}{2}$	
n	$\mathcal{O}(2^n)$	n -BIT HASH PRE-IMAGE ATTACK	SHA-2, SHA-3		GROVER	$\mathcal{O}\left(2^{\frac{n}{2}}\right)$	$\frac{n}{2}$	
n	$\mathcal{O}(2^n)$	n -BIT HASH 2ND-PRE-IMAGE ATTACK	SHA-2, SHA-3		GROVER	$\mathcal{O}\left(2^{\frac{n}{2}}\right)$	$\frac{n}{2}$	
$\frac{n}{2}$	$\mathcal{O}\left(2^{\frac{n}{2}}\right)$	n -BIT HASH COLLISION ATTACK	SHA-2, SHA-3		BRASSARD ET AL.	$\mathcal{O}\left(2^{\frac{n}{3}}\right)$	$\frac{n}{3}$	
128	$\mathcal{O}(2^{128})$	128-BIT KEY SPACE EXHAUSTIVE KEY SEARCH	AES-128	CATEGORY 1	GROVER	$\mathcal{O}(2^{64})$	64	FALCON-512, SLH-DSA 128 VARIANTS
		128-BIT HASH PRE-IMAGE ATTACK	N/A		GROVER	$\mathcal{O}(2^{64})$	64	
		128-BIT HASH 2ND-PRE-IMAGE ATTACK	N/A		GROVER	$\mathcal{O}(2^{64})$	64	
		256-BIT HASH COLLISION ATTACK	SHA-256, SHA3-256	CATEGORY 2	BRASSARD ET AL.	$\mathcal{O}(2^{85})$	85	
192	$\mathcal{O}(2^{192})$	192-BIT KEY SPACE EXHAUSTIVE KEY SEARCH	AES-192	CATEGORY 3	GROVER	$\mathcal{O}(2^{96})$	96	ML-DSA-67, SLH-DSA 192 VARIANTS
		192-BIT HASH PRE-IMAGE ATTACK	N/A		GROVER	$\mathcal{O}(2^{96})$	96	
		192-BIT HASH 2ND-PRE-IMAGE ATTACK	N/A		GROVER	$\mathcal{O}(2^{96})$	96	
		384-BIT HASH COLLISION ATTACK	SHA-384, SHA3-384	CATEGORY 4	BRASSARD ET AL.	$\mathcal{O}(2^{128})$	128	
256	$\mathcal{O}(2^{256})$	256-BIT KEY SPACE EXHAUSTIVE KEY SEARCH	AES-256	CATEGORY 5	GROVER	$\mathcal{O}(2^{128})$	128	ML-DSA-85, SLH-DSA 256 VARIANTS TBVXMS
		256-BIT HASH PRE-IMAGE ATTACK	N/A		GROVER	$\mathcal{O}(2^{128})$	128	
		256-BIT HASH 2ND-PRE-IMAGE ATTACK	N/A		GROVER	$\mathcal{O}(2^{128})$	128	
		512-BIT HASH COLLISION ATTACK	SHA-512, SHA3-512		BRASSARD ET AL.	$\mathcal{O}(2^{170})$	170	
384	$\mathcal{O}(2^{384})$	384-BIT KEY SPACE EXHAUSTIVE KEY SEARCH	N/A		GROVER	$\mathcal{O}(2^{192})$	192	
		384-BIT HASH PRE-IMAGE ATTACK	SHA-384, SHA3-384		GROVER	$\mathcal{O}(2^{192})$	192	
		384-BIT HASH 2ND-PRE-IMAGE ATTACK	SHA-384, SHA3-384		GROVER	$\mathcal{O}(2^{192})$	192	
		768-BIT HASH COLLISION ATTACK	N/A		BRASSARD ET AL.	$\mathcal{O}(2^{256})$	256	
512	$\mathcal{O}(2^{512})$	512-BIT KEY SPACE EXHAUSTIVE KEY SEARCH	N/A		GROVER	$\mathcal{O}(2^{256})$	256	
		512-BIT HASH PRE-IMAGE ATTACK	SHA-512, SHA3-512		GROVER	$\mathcal{O}(2^{256})$	256	
		512-BIT HASH 2ND-PRE-IMAGE ATTACK	SHA-512, SHA3-512		GROVER	$\mathcal{O}(2^{256})$	256	
		1024-BIT HASH COLLISION ATTACK	N/A		BRASSARD ET AL.	$\mathcal{O}(2^{341})$	341	

NOTES & TAKEAWAYS

- The above is still a simplified view. It does not dive into the specific assumptions made in the new algorithms' security proofs and the possible attacks on those algorithms (e.g., is a collision attack on a hash function enough, or would a pre-image be required to break the signature scheme using that hash function). It is also not including considering practical considerations and predictions about quantum computers, such as runtime or quantum circuit depth. Cf. [NIST PQC Evaluation Criteria, 4.A.5](#) for further details.
- A pre-quantum security level can have different post-quantum security levels equivalents. It all depends on the specific attack in question, resp. the security assumption a new post-quantum algorithm is based on or must be secure against. For hashing, the often cited "SHA-256 offers 128 bits of security" is not wrong, but only part of the picture: it offers 256 bits of security against pre-image and 2nd-preimage-attacks. The n bits of security against 2nd-preimage attacks is still a slightly simplified and harmonized view to avoid different formulas for different hash functions. Cf. [NIST: Hash Functions](#) for details.
- The fact that the exact level of post-quantum security still depends on so many assumptions about CRQCs, comparing pre-quantum and post-quantum security levels remains an apples and oranges comparison to some degree. Such comparisons should be taken with a grain of salt, especially when done only on a rather superficial level.
- The lines marked with colors ■, ■, ■ and ■ are the ones used by NIST to define categories I, II, III, IV and V. The lines marked in lighter colors ■, ■, and ■ have the same post-quantum security as the defining lines of categories I, III and V, respectively. They therefore fulfill the "comparable to or greater than" clause in NIST's category definitions. Note that categories IV and V are differentiated despite having 128 bits of post-quantum security – again highlighting the fact that a precise categorization is difficult and requires a detailed analysis of many aspects.



ALGORITHM OVERALL USABILITY SCORE

We try to measure an algorithm's overall usability for a general use case (i.e., a use case without any special characteristics and constraints) by calculating a single number between 0 (worst) and 10 (best) for the algorithm. This calculation is taking into account all parameter sets, performance metrics, public key size, signature/ciphertext size, the number of security categories provided, whether or not it is suitable for general use, and the complexity and size of its implementation. There are many possible ways to define a formula for this purpose and weigh in different individual metrics into overall usability. Here, we define an algorithm's overall score as

$$\text{score}_{\text{algorithm}} = \max \left\{ 0, \text{avg} \left\{ \text{score}_{\text{parameterSet}} \mid \text{parameterSet is a parameter set of algorithm} \right\} - \frac{1}{8} \cdot (5 - \text{categories}_{\text{algorithm}}) - \frac{1}{4} \cdot \text{impl}_{\text{algorithm}} - \text{generality}_{\text{algorithm}} \right\}$$

where $\text{score}_{\text{parameterSet}}$ is a score for an individual algorithm parameter set. It aims to express the various performance and size metrics of the specific variant. Depending on the type of algorithm, $\text{score}_{\text{parameterSet}}$ is defined as

$$\text{score}_{\text{signature-parameterSet}} = 10 - \text{avg} \left\{ n_{\text{O}}^{\text{O}}, n_{\text{O}}^{\text{O}}, n_{\text{O}}^{\text{O}}, n_{\text{O}}^{\text{O}}, n_{\text{O}}^{\text{O}} \right\}$$

respectively

$$\text{score}_{\text{encryption-parameterSet}} = 10 - \text{avg} \left\{ n_{\text{O}}^{\text{O}}, n_{\text{O}}^{\text{O}}, n_{\text{O}}^{\text{O}}, n_{\text{O}}^{\text{O}}, n_{\text{O}}^{\text{O}} \right\}.$$

Furthermore, $1 \leq \text{categories}_{\text{algorithm}} \leq 5$ denotes the number of different NIST security categories offered by *algorithm*. By assigning numeric values of $0 = \text{L}_{\text{O}}^*$, $1 = \text{M}_{\text{O}}^*$ and $2 = \text{H}_{\text{O}}^*$, we set

$$\text{impl}_{\text{signature-algorithm}} = \text{avg} \left\{ c_{\text{O}}^{\text{O}}, c_{\text{O}}^{\text{O}}, c_{\text{O}}^{\text{O}}, s_{\text{O}}^{\text{O}}, s_{\text{O}}^{\text{O}}, s_{\text{O}}^{\text{O}} \right\}$$

respectively

$$\text{impl}_{\text{encryption-algorithm}} = \text{avg} \left\{ c_{\text{O}}^{\text{O}}, c_{\text{O}}^{\text{O}}, c_{\text{O}}^{\text{O}}, s_{\text{O}}^{\text{O}}, s_{\text{O}}^{\text{O}}, s_{\text{O}}^{\text{O}} \right\}$$

to take into account the implementation size and complexity (here, complexity doesn't mean running time, but difficulty of implementing the algorithm correctly). Finally, we define

$$\text{generality}_{\text{algorithm}} = \begin{cases} 0 & \text{if } \text{algorithm} \text{ is a general purpose algorithm} \\ 2 & \text{else} \end{cases}$$

to take into account if the algorithm is suitable for general use (i.e., algorithms not suitable for general use are penalized by subtracting two usability points).

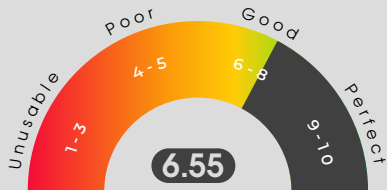
TBD: In the algorithm scores given in ID cards, we currently use $\text{impl}_{\text{algorithm}} = 0$ in the respective computations because the necessary values for implementation complexity and size are still TBD. This will be corrected later.

EXAMPLE: ML-DSA OVERALL USABILITY SCORE

We calculate

$$\text{score}_{\text{ML-DSA-44}} = 10 - \text{avg} \left\{ 3_{\text{O}}^{\text{O}}, 3_{\text{O}}^{\text{O}}, 2_{\text{O}}^{\text{O}}, 1_{\text{O}}^{\text{O}}, 5_{\text{O}}^{\text{O}} \right\} = 10 - 2.8 = 7.2$$

Similarly, we obtain $\text{score}_{\text{ML-DSA-65}} = 7.0$ and $\text{score}_{\text{ML-DSA-87}} = 6.2$. Furthermore, $\text{categories}_{\text{ML-DSA}} = 3$ since ML-DSA offers the three security categories II_{O}^* , III_{O}^* , and V_{O}^* , and $\text{generality}_{\text{ML-DSA}} = 0$ since ML-DSA is a general purpose signature algorithm. This results in an overall usability score of 6.55:



ML-DSA Overall Usability Score

$$\begin{aligned} \text{score}_{\text{ML-DSA}} &= \max \left\{ 0, \text{avg} \left\{ \text{score}_{\text{ML-DSA-44}}, \text{score}_{\text{ML-DSA-65}}, \text{score}_{\text{ML-DSA-87}} \right\} - \frac{1}{8} \cdot (5 - \text{categories}_{\text{ML-DSA}}) - \frac{1}{4} \cdot \text{impl}_{\text{ML-DSA}} - \text{generality}_{\text{ML-DSA}} \right\} \\ &= \max \left\{ 0, \text{avg} \{ 7.2, 7.0, 6.2 \} - \frac{1}{8} \cdot (5-3) - 0 - 0 \right\} \\ &= \max \{ 0, 6.8 - 0.25 \} \\ &= \max \{ 0, 6.55 \} \\ &= 6.55 \end{aligned}$$

TBD: We use $\text{impl}_{\text{ML-DSA}} = 0$ because the necessary values to compute it are still TBD, cf. ML-DSA ID card. This will be corrected later.



ALGORITHM IMPLEMENTATION COMPLEXITY AND SIZE TBD

Size

In some contexts, algorithm implementation size can be important. For example, on smartcards or embedded devices with little storage or memory capacity and limited computational resources, an algorithms “footprint” may be a relevant factor. Developers may have to determine it is even possible to fit an algorithms implementation on a particular device and execute it. For that reason, this cheat sheet aims to include indicators for algorithms’ implementation size for key generation, signature generation and verification resp. encryption and decryption.

However, it is difficult to define a useful way to measure an implementation’s size: possible metrics could be lines of source code or the size of a compiled binary measured in bytes. However, those measurements would depend on factors such as programming language, compiler, and platform architecture. They are thus not ideal.

Complexity

Similarly, some developers may be concerned with an algorithm’s implementation complexity. Here, “complexity” refers not to running time or space complexity, but rather to the level of difficulty of implementing an algorithm correctly without introducing vulnerabilities by mistake. The question of how difficult it is to implement a particular algorithm compared to another has repeatedly come up in exchanges on cryptography mailing lists or forums. It is also not specific to PQC (e.g. it is often claimed that ECDSA is harder to implement without vulnerabilities than RSA). Therefore, this cheat sheet also aims to include indicators about that complexity/difficulty.

However, as with an algorithm’s size, there is no obvious and objective way to measure this complexity.

For the aforementioned reasons, all algorithm ID cards contain tables for implementation complexity and size, which are however not filled with actual values for the time being. The intention is to complete these tables with simple values of Low, Medium, or High: .

To complete this part of the cheat sheets in a useful manner, suggestions and contributions from the cryptography community for how to do so are welcome and necessary!

General considerations for developers implementing cryptographic algorithms

For implementations of cryptography, unlike other algorithms, getting the correct outputs is not sufficient. For a secure implementation, it is crucial that no sensitive and confidential information leaks in any way, not even through side channel attacks. Such a leak could occur in many different ways and places in an implementation (e.g. leaked nonces, biased bits in (pseudo-)random numbers, prime numbers, execution times of certain parts of the code, etc.). Compilers, code generation tools or even an IDE applying code formatting rules may try to optimize code to make it more performant - but introduce a vulnerability while doing so.



Developers should be aware of the possible pitfalls of implementing cryptography on their own. Caution is advised, and if possible, it is recommended to use well-known cryptographic libraries and products developed by experts instead of using self-developed implementations.