



**Cyber Security (CYBER);
Quantum-Safe Cryptography (QSC);
Secure Implementation Guidance for
Key Encapsulation Mechanisms and
Digital Signature Schemes;
Part 2: ML-KEM**

Reference

DTR/CYBER-QSC-0027-2

Keywords

cyber security, key exchange,
quantum safe cryptography

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced in any form or by any means except for the purpose of implementation of standards.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.
All rights reserved.

Contents

Intellectual Property Rights	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	8
3.3 Abbreviations	8
4 Introduction	8
5 ML-KEM interfaces	9
5.1 Parameters	9
5.2 Key generation	9
5.2.1 Full key generation	9
5.2.2 Key formats	10
5.2.3 Seed format key generation	10
5.3 Encapsulation	11
5.4 Decapsulation.....	11
6 General implementation considerations	12
6.1 Perform input validation.....	12
6.1.1 Encapsulation inputs	12
6.1.2 Decapsulation inputs.....	12
6.1.3 Internal algorithms	13
6.2 Perform output validation.....	14
6.2.1 Ciphertext re-encryption check.....	14
6.2.2 Pairwise consistency test	14
6.2.3 Self testing	15
6.2.4 Public key linting	16
6.3 Prevent leakage of intermediate values	16
6.3.1 Zeroise intermediate values after use.....	16
6.3.2 Limit external access to internal functions	17
6.4 Handle errors gracefully	17
6.4.1 Specified errors.....	17
6.4.2 Unspecified errors.....	17
6.4.3 Implicit rejection.....	18
6.5 Randomness	18
7 Side-channel and fault attack considerations	18
7.1 Introduction	18
7.2 Key generation	18
7.2.1 Overview	18
7.2.2 Timing analysis considerations.....	19
7.2.3 Power analysis considerations	19
7.2.4 Fault attack considerations.....	20
7.3 Encapsulation	21
7.3.1 Overview	21
7.3.2 Timing analysis considerations.....	21
7.3.3 Power analysis considerations	21
7.3.4 Fault attack considerations.....	22
7.4 Decapsulation	22
7.4.1 Overview	22

7.4.2	Timing analysis considerations.....	23
7.4.3	Power analysis considerations	23
7.4.4	Fault attack considerations.....	23
8	Testing and formal verification considerations	24
8.1	Testing considerations	24
8.2	Formal verification considerations	24
Annex A:	NIST FIPS 203 algorithms	25
A.1	Key encapsulation (external).....	25
A.2	De-randomized key encapsulation (internal only)	25
A.3	Public-key encryption (internal only).....	25
A.4	Sampling.....	25
A.5	Arithmetic.....	25
A.6	Encoding.....	26
Annex B:	ML-KEM security properties	27
B.1	Indistinguishability	27
B.1.1	IND-CPA security	27
B.1.2	IND-CCA security.....	27
B.2	Binding.....	28
B.2.1	Re-encapsulation attacks	28
B.2.2	Binding properties	29
Annex C:	Hybrid ML-KEM.....	31
C.1	Deployment considerations	31
C.2	Implementation considerations.....	31
Annex D:	Change history	33
History		34

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the [ETSI IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [i.3].

The present document provides implementation guidance for the Module-Lattice-based Key Encapsulation Mechanism (ML-KEM).

Modal verbs terminology

In the present document **"should"**, **"should not"**, **"may"**, **"need not"**, **"will"**, **"will not"**, **"can"** and **"cannot"** are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"must" and **"must not"** are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document provides developers with guidance to aid the secure implementation of the quantum-safe key encapsulation mechanism ML-KEM as specified by NIST FIPS 203 [i.5]. This highlights some potential ML-KEM implementation hazards; identifies some side-channel and fault attack issues specific to ML-KEM; considers some testing and formal verification aspects relevant to ML-KEM; and briefly discusses the secure usage of ML-KEM.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

- [i.1] ETSI TS 103 744 (V1.2.2): "CYBER; Quantum-Safe Cryptography (QSC); Quantum-safe Hybrid Key Establishment".
- [i.2] ETSI TR 103 966: "CYBER Security (CYBER); Quantum-Safe Cryptography (QSC); Deployment Considerations for Hybrid Schemes".
- [i.3] ETSI TR 104 239-1: "Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes; Part 1: General".
- [i.4] IETF RFC 9935: "Internet X.509 Public Key Infrastructure - Algorithm Identifiers for the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM)".
- [i.5] NIST FIPS 203: "Module-Lattice-Based Key-Encapsulation Mechanism Standard".
- [i.6] NIST SP 800-133 Rev. 2: "Recommendation for Cryptographic Key Generation".
- [i.7] NIST SP 800-227: "Recommendations for Key-Encapsulation Mechanisms".
- [i.8] NIST: "[Automated Cryptographic Validation Test System](#)".
- [i.9] NIST: "[Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program](#)".
- [i.10] C. Aguilar Melchor et al.: "[Hamming Quasi-Cyclic \(HQC\): Fourth round version](#)". NIST Post-Quantum Cryptography Standardization Process.
- [i.11] J.B. Almeida et al.: "Formally verifying Kyber Episode V: Machine-checked IND-CCA security and correctness of ML-KEM in EasyCrypt". CRYPTO 2024.
- [i.12] R. Avanzi et al.: "CRYSTALS-Kyber: Algorithm specification and supporting documentation (version 3.02)". NIST Post-Quantum Cryptography Standardization Process.
- [i.13] D.J. Bernstein et al.: "KyberSlash: Exploiting secret-dependent division timings in Kyber implementations". CHES 2025.

- [i.14] J. Bos et al.: "CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM". Euro S&P 2018.
- [i.15] J. Bos et al.: "Masking Kyber: First- and higher-order implementations". CHES 2021.
- [i.16] BSI TR-02102-1: "Cryptographic mechanisms: Recommendations and key lengths", January 2026.
- [i.17] Community Cryptography Specification Project: "[Project Wycheproof](#)".
- [i.18] C. Cremers, A. Dax and N. Medinger: "Keeping up with the KEMs: Stronger security notions for KEMs and automated analysis of KEM-based protocols". CCS 2024.
- [i.19] Cybersecurity & Infrastructure Security Agency, US Government: "[Secure-by-Design - Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software](#)".
- [i.20] Department of Science, Innovation and Technology, UK Government: "[Software Security Code of Practice](#)".
- [i.21] B. Gierlichs et al.: "Mutual information analysis". CHES 2008.
- [i.22] C. Glénaz et al.: "[Finding bugs in implementations of HQC, the fifth post-quantum standard](#)".
- [i.23] Q. Guo, T. Johansson and A. Nilsson: "A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM". CRYPTO 2020.
- [i.24] J. Hermelink, P. Pessl and T. Pöppelmann: "Fault-enabled chosen-ciphertext attacks on Kyber". INDOCRYPT 2021.
- [i.25] K. Hövelmanns and M. Kudinov: "Treating dishonest ciphertexts in post-quantum KEMs - Explicit vs. implicit rejection in the FO transform". PQCrypto 2025.
- [i.26] M.J. Kannwischer, P. Pessl and R. Primas: "Single-trace attacks on Keccak". CHES 2020.
- [i.27] E. Karatsiolis et al.: "Public Key Linting for ML-KEM and ML-DSA". ACNS 2025.
- [i.28] S. Nkotto: "Template and CPA side channel attacks on the Kyber/ML-KEM pair-pointwise multiplication". IACR ePrint Archive 2025/1577.
- [i.29] Post-Quantum Cryptography Alliance: "[mlkem-native](#)".
- [i.30] P. Ravi et al.: "Number 'not used' once - Practical fault attack on pqm4 implementations of NIST candidates". COSADE 2019.
- [i.31] P. Ravi et al.: "On configurable SCA countermeasures against single trace attacks for the NTT". SPACE 2020.
- [i.32] S. Schmieg: "Unbindable Kemmy Schmidt: ML-KEM is neither MAL-BIND-K-CT nor MAL-BIND-K-PK". IACR ePrint Archive 2024/523.
- [i.33] Symbolic Software: "[Crucible](#)".
- [i.34] T. Tosun, E. Oswald and E. Savaş: "Non-profiled higher-order side-channel attacks against lattice-based post-quantum cryptography". IACR Communications in Cryptology, 2025.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

$a[i:j]$	Sub-string $a_i \dots a_{j-1}$ of the byte string $a := a_0 \dots a_{n-1}$
(a, b)	Ordered pair of values a and b
$a b$	Concatenation of the byte strings a and b
$a = b$	Return true if the values a and b are equal and false otherwise
$a \leftarrow b$	Assign the value b to the variable a

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
CBD	Centred Binomial Distribution
CVE	Common Vulnerabilities and Exposures
DPA	Differential Power Analysis
ECDH	Elliptic Curve Diffie-Hellman
FIPS	Federal Information Processing Standard
FO	Fujisaki-Okamoto
HMAC	Hash-based Message Authentication Code
HQC	Hamming Quasi-Cyclic
IND-CCA	Indistinguishability against Chosen Ciphertext Attacks
IND-CPA	Indistinguishability against Chosen Plaintext Attacks
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
LWE	Learning With Errors
ML-DSA	Module-Lattice-based Digital Signature Algorithm
ML-KEM	Module-Lattice-based Key Encapsulation Mechanism
NIST	National Institute of Standards and Technology
NTT	Number Theoretic Transform
PKE	Public Key Encryption
PKE	Public-Key Encryption
PQC	Post-Quantum Cryptography
RBG	Random Bit Generator
SHA	Secure Hash Algorithm
SHAKE	Secure Hash Algorithm Keccak
SLH-DSA	Stateless Hash-based Digital Signature Algorithm
SP	Special Publication
TLS	Transport Layer Security

4 Introduction

The Module-Lattice-based Key Encapsulation Mechanism (ML-KEM) is a post-quantum Key Encapsulation Mechanism (KEM) selected for standardization following the multi-year NIST Post-Quantum Cryptography (PQC) Standardization Process. It is specified in NIST FIPS 203 [i.5] and support for ML-KEM is being integrated into internet protocols such as TLS.

NOTE: ML-KEM is based on the CRYSTALS-Kyber submission to the NIST PQC Process [i.12], but changes made during the development of NIST FIPS 203 [i.5] mean that it is not interoperable with Kyber.

ML-KEM received a significant amount of analysis during the NIST PQC Process, but its security also depends on the way in which it is implemented and used. The present document builds on the general guidance in ETSI TR 104 239-1 [i.3] to provide developers with some specific guidance to aid the secure implementation of ML-KEM:

- It describes the ML-KEM interfaces and different options for private key formats (clause 5).

- It extends the general implementation considerations from ETSI TR 104 239-1 [i.3] with ML-KEM specific aspects such as input validation, consistency checks, and error handling (clause 6).
- It discusses different side-channel considerations for ML-KEM key generation, encapsulation and decapsulation (clause 7).
- It touches on testing and formal validation for ML-KEM implementations (clause 8).

The present document also gives some background on ML-KEM security properties (annex B) and some considerations on the use of ML-KEM in hybrid schemes (annex C).

As with ETSI TR 104 239-1 [i.3], the guidance is primarily aimed at secure implementations in software, although some of the recommendations will also be relevant to hardware implementations. Developers implementing ML-KEM should also ensure that they follow best practice for developing secure systems in general [i.19] and [i.20].

5 ML-KEM interfaces

5.1 Parameters

NIST FIPS 203 [i.5] specifies three approved parameter sets for ML-KEM:

- **ML-KEM-512** targets security category 1, which is equivalent to key recovery for AES-128;
- **ML-KEM-768** targets security category 3, which is equivalent to key recovery for AES-192; and
- **ML-KEM-1024** targets security category 5, which is equivalent to key recovery for AES-256.

ML-KEM-768 is recommended as the default parameter set. ML-KEM-512 can be used in applications that require smaller public keys or ciphertexts. ML-KEM-1024 can be used in applications that require a higher level of security.

Table 1 lists the sizes of the ML-KEM private decapsulation keys, public encapsulation keys and ciphertexts.

Table 1: ML-KEM private key, public key, ciphertext and shared secret lengths (in bytes)

Parameter set	Private decapsulation key	Public encapsulation key	Ciphertext	Shared secret
ML-KEM-512	1 632	800	768	32
ML-KEM-768	2 400	1 184	1 088	32
ML-KEM-1024	3 168	1 568	1 568	32

5.2 Key generation

5.2.1 Full key generation

The specification of ML-KEM key generation in NIST FIPS 203 [i.5], algorithm 19 samples a pair of 32-byte values and deterministically generates the key pair from those values via an internal key generation function (see table 2).