



TECHNICAL REPORT

**Cyber Security (CYBER);
Quantum-Safe Cryptography (QSC);
Secure Implementation Guidance for
Key Encapsulation Mechanisms and
Digital Signature Schemes;
Part 1: General**

Reference

RTR/CYBER-QSC-0032

Keywordscyber security, digital signature, 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.....	8
3.1 Terms.....	8
3.2 Symbols.....	9
3.3 Abbreviations	9
4 Introduction	9
5 Interfaces	10
5.1 Key encapsulation mechanisms.....	10
5.1.1 Key encapsulation interface.....	10
5.1.2 Errors	11
5.1.3 Decapsulation failures.....	11
5.2 Digital signature schemes.....	12
5.2.1 Digital signature interface.....	12
5.2.2 Errors	12
5.2.3 Pre-hashing	13
5.2.4 Context strings	13
6 Best practice guidance.....	14
6.1 Reuse existing implementations	14
6.2 Perform input validation.....	14
6.2.1 Check input formats.....	14
6.2.2 Check cryptographic inputs	14
6.3 Perform output validation.....	15
6.3.1 Include consistency checks	15
6.3.2 Use expected output formats.....	15
6.4 Prevent leakage of intermediate values	16
6.4.1 Zeroise intermediate values after use.....	16
6.4.2 Limit access to intermediate functions.....	16
6.5 Handle errors gracefully	16
6.5.1 Include specified error handling	16
6.5.2 Avoid leaking information through errors	17
6.5.3 Indicate the severity of errors	17
6.6 Use good randomness.....	17
6.6.1 Use a secure random bit generator.....	17
6.6.2 Use good entropy	18
6.6.3 Perform de-randomization correctly	18
7 Side-Channels and Fault Attacks	18
7.1 Introduction	18
7.1.1 Concept.....	18
7.1.2 Physical Access	19
7.1.3 Duration	19
7.1.4 Control	19
7.2 Timing Analysis	20
7.2.1 Concept.....	20
7.2.2 Secret-Dependent Branching	20
7.2.3 Variable Time Operations.....	20
7.2.4 Secret-Dependent Memory Addressing.....	21

7.2.5	Mitigations	21
7.3	Power and EM Analysis	21
7.3.1	Concept	21
7.3.2	Mitigations	22
7.3.3	Randomization	22
7.3.4	Masking	23
7.4	Fault Attacks	23
7.4.1	Concept	23
7.4.2	Mitigations	24
8	Testing and Formal Verification	24
8.1	Introduction	24
8.2	Testing	24
8.2.1	Concept	24
8.2.2	Benefits and Limitations	25
8.3	Functional Correctness	25
8.3.1	Concept	25
8.3.2	Benefits and limitations	26
8.4	Memory-safety and Type-safety	27
8.4.1	Concept	27
8.4.2	Benefits and Limitations	28
History	29

Sample Document

get full document from standards.iteh.ai

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.

BLUETOOTH® is a trademark registered and owned by Bluetooth SIG, Inc.

Foreword

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

The present document is part 1 of a multi-part deliverable covering implementation guidance for quantum-safe key encapsulation mechanisms and digital signature schemes, as identified below:

- Part 1:** "General";
- Part 2: "ML-KEM" [i.2];
- Part 3: "ML-DSA" [i.3];
- Part 4: "SLH-DSA" [i.4].

Later parts of this multi-part deliverable will provide implementation guidance for specific algorithms, building on the general guidance provided in the present document.

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 general guidance to aid the secure implementation of quantum-safe algorithms. This includes an overview of the interfaces and expected security properties of quantum-safe algorithms; some general good practice guidance for cryptographic implementations; some background on side-channel and fault attacks; and a brief discussion of testing and formal verification.

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 EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".
- [i.2] ETSI TR 104 239-2: "Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes; Part 2: ML-KEM".
- [i.3] ETSI TR 104 239-3: " Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes; Part 3: ML-DSA".
- [i.4] ETSI TR 104 239-4: " Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Secure Implementation Guidance for Key Encapsulation Mechanisms and Digital Signature Schemes; Part 4: SLH-DSA".
- [i.5] IRTF RFC 7748: "Elliptic Curves for Security".
- [i.6] IETF RFC 8017: "PKCS #1: RSA Cryptography Specifications version 2.2".
- [i.7] IRTF RFC 8032: "Edwards-Curve Digital Signature Algorithm (EdDSA)".
- [i.8] IRTF RFC 9180: "Hybrid Public Key Encryption".
- [i.9] IRTF RFC 9474: " RSA Blind Signatures".
- [i.10] ISO/IEC 14888-3:2018: "IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms".
- [i.11] ISO/IEC 18033-2:2006: "Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers".
- [i.12] NCSC: "[Timelines for migration to post-quantum cryptography](#)".
- [i.13] NIST FIPS 186-5: "Digital Signature Standard (DSS)".

- [i.14] NIST FIPS 203: "Module-Lattice-Based Key-Encapsulation Mechanism Standard".
- [i.15] NIST FIPS 204: "Module-Lattice-Based Digital Signature Standard".
- [i.16] NIST FIPS 205: "Stateless Hash-Based Digital Signature Standard".
- [i.17] NIST SP 800-56A Rev. 3: "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography".
- [i.18] NIST SP 800-56B Rev. 2: "Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography".
- [i.19] NIST SP 800-89: "Recommendation for Obtaining Assurances for Digital Signature Applications".
- [i.20] NIST SP 800-90 Series.
- [i.21] NIST: "[Automated Cryptographic Validation Test System](#)".
- [i.22] NIST: "[Cryptographic Algorithm Validation Program \(CAVP\)](#)".
- [i.23] NIST: "[Announcing Approval of Three Federal Information Processing Standards \(FIPS\) for Post-Quantum Cryptography](#)".
- [i.24] J. B. Almeida et al.: "Formally verifying Kyber Episode IV: Implementation correctness". IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(3), pp. 164-193, 2023.
- [i.25] M. Barbosa et al.: "SoK: Computer-aided cryptography", IEEE™ Symposium on Security and Privacy (SP), pp. 777-795, 2021.
- [i.26] G. Becker et al.: "Test Vector Leakage Assessment (TVLA) methodology in practice". International Cryptographic Module Conference 2013.
- [i.27] R. Benadjila et al.: "Deep learning for side-channel analysis and introduction to ASCAD database". Journal of Cryptographic Engineering Volume 10 (2020), pp. 163-188, 2020.
- [i.28] D. J. Bernstein et al.: "KyberSlash: Exploiting secret-dependent division timings in Kyber implementations". IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(2), pp. 209-234, 2025.
- [i.29] E. Biham and A. Shamir: "Differential fault analysis of secret key cryptosystems". Advances in Cryptology - CRYPTO' 97. Lecture Notes in Computer Science, vol. 1294, 1997.
- [i.30] G. Camurati et al.: "Screaming channels: When electromagnetic side channels meet radio transceivers". CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 163-177, 2018.
- [i.31] Cybersecurity & Infrastructure Security Agency, US Government: "[Secure-by-Design - Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software](#)".
- [i.32] Department of Science, Innovation and Technology, UK Government: "[Software Security Code of Practice](#)".
- [i.33] fail0verflow: "Console hacking 2010". 27th Chaos Communication Congress, 2010.
- [i.34] A. Genêt: "On Protecting SPHINCS+ Against Fault Attacks". IACR Transactions on Cryptographic Hardware and Embedded Systems, pp. 80-114, 2023.
- [i.35] M. Hastings et al.: "Weak keys remain widespread in network devices". Proceedings of the 2016 Internet Measurement Conference (IMC 16), pp. 49-63, 2016.
- [i.36] N. Heninger et al.: "Mining your Ps and Qs: Detection of widespread weak keys in network devices". 21st USENIX Security Symposium (USENIX Security 12), pp. 205-220.
- [i.37] X. Hou et al.: "Fully automated differential fault analysis on software implementations of block ciphers". IACR Transactions on Cryptographic Hardware and Embedded Systems, 2019(3), pp. 1-29, 2019.