ETSI TR 103 966 V1.1.1 (2024-10)

CYBER Security (CYBER);
Quantum-Safe Cryptography (QSC);
Deployment Considerations for Hybrid Schemes

Reference

DTR/CYBER-QSC-0021

Keywords

cybersecurity, hybrid, 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

Contents

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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).

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 explores issues around combining traditional and post-quantum algorithms to construct hybrid cryptographic schemes.

Specifically, the present document examines some of the reasons for proposing and adopting hybrid schemes, both for key establishment and digital signatures; clarifies some of the terminology used to describe hybrid schemes; discusses some of the security, efficiency, and agility trade-offs; highlights some important things to consider when selecting algorithm and parameter combinations; explores some potential deployment and migration issues; and identifies situations where hybrid schemes will need to be deprecated in favour of purely post-quantum algorithms.

The present document does not provide guidance on whether or not to use hybrid schemes.

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 are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 616: "CYBER; Quantum-safe signatures".

[i.2] ETSI TR 103 692: "CYBER; State management for stateful authentication mechanisms".

[i.3] ETSI TS 103 744: "CYBER; Quantum-Safe Cryptography (QSC); Quantum-safe hybrid key exchanges".

[i.4] ETSI TR 103 823: "CYBER; Quantum-safe public-key encryption and key encapsulation".

[i.5] IETF RFC 5652: "Cryptographic Message Syntax (CMS)".

[i.6] IETF RFC 6090: "Fundamental elliptic curve cryptography algorithms".

[i.7] IETF RFC 8551: "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 message specification".

[i.8] IETF RFC 9370: "Multiple key exchanges in the Internet Key Exchange protocol Version 2 (IKEv2)".

[i.9] IRTF IETF RFC 7748: "Elliptic curves for security".

[i.10] IRTF IETF RFC 8391: "XMSS: eXtended Merkle Signature Scheme".

[i.11] IRTF IETF RFC 8554: "Leighton-Micali hash-based signatures".

[i.12] IRTF IETF RFC 9180: "Hybrid public key encryption".

[i.13] NIST FIPS 140-3: "Security requirements for cryptographic modules".

[i.14] NIST FIPS 186-4: "Digital Signature Standard (DSS)".

[i.15] NIST FIPS 203 (initial public draft): "Module-lattice-based key-encapsulation mechanism standard".

[i.16] NIST FIPS 204 (initial public draft): "Module-lattice-based digital signature standard".

[i.17] NIST FIPS 205 (initial public draft): "Stateless hash-based digital signature standard".

[i.18] NIST SP 800-56A Rev. 3: "Recommendation for pair-wise key establishment schemes using discrete logarithm cryptography".

[i.19] NIST SP 800-56B Rev. 2: "Recommendation for pair-wise key establishment schemes using integer factorization cryptography".

[i.20] NIST: "Post-quantum cryptography FAQs".

[i.21] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public key and attribute certificate frameworks".

[i.22] M.R. Albrecht, et al: "Classic McEliece: conservative code-based cryptography". NIST round 3 post-quantum submission.

[i.23] R. Avanzi et al: "CRYSTALS-Kyber: Algorithm specifications and supporting documentation". NIST round 3 post-quantum submission.

[i.24] J.-P. Aumasson et al: "SPHINCS+: Submission to the NIST post-quantum project". NIST round 3 post-quantum submission.

[i.25] N. Aviram et al: "DROWN: Breaking TLS using SSLv2". USENIX Security 2016.

[i.26] J. Baena et al: "Improving support-minors rank attacks: Applications to GeMSS and Rainbow". CRYPTO 2022.

[i.27] S. Bai et al: "CRYSTALS-Dilithium: Algorithm specifications and supporting documentation". NIST round 3 post-quantum submission.

[i.28] M. Barbosa et al: "X-Wing: The hybrid KEM you've been looking for". IACR ePrint 2024/039.

[i.29] N. Bindel and B. Hale: "A note on hybrid signature schemes". IACR ePrint 2023/423.

[i.30] N. Bindel et al: "Hybrid key encapsulation mechanisms and authenticated key exchange". PQCrypto 2019.

[i.31] N. Bindel et al: "Transitioning to a quantum-resistant public key infrastructure". PQCrypto 2017.

[i.32] W. Beullens: "Breaking Rainbow takes a weekend on a laptop". CRYPTO 2022.

[i.33] D. Bleichenbacher: "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1". CRYPTO 1998.

[i.34] C. Bonnell et al: "A mechanism for encoding differences in paired certificates". IETF Internet-Draft (work in progress), draft-bonnell-lamps-chameleon-certs-03.

[i.35] F. Byszio, K.-D. Wirth and K. Nguyen: "Intelligent composed algorithms". IACR ePrint 2021/813.

[i.36] M. Campagna and A. Petcher: "Security of hybrid key encapsulation". IACR ePrint 2020/1364.

[i.37] W. Castryck and T. Decru: "An efficient key recovery attack on SIDH". EUROCRYPT 2023.

[i.38] D. Connolly, P. Schwabe and B. Westerbaan: "X-Wing: General-purpose hybrid post-quantum KEM". IETF Internet-Draft (work in progress), draft-connolly-cfrg-xwing-kem-01.

[i.39] Y. Dodis and J. Katz: "Chosen-ciphertext security of multiple encryption", TCC 2005.

[i.40] B. Dowling et al: "A cryptographic analysis of the TLS 1.3 handshake protocol candidates". ACM CCS 2015.

[i.41] P.-A. Fouque et al: "Falcon: Fast-Fourier lattice-based compact signatures over NTRU". NIST round 3 post-quantum submission.

[i.42] M. Friedl, J. Mojzis and S. Josefsson: "Secure Shell (SSH) key exchange method using hybrid Streamlined NTRU Prime sntrup761 and X25519 with SHA-512: sntrup761x25519-sha512". IETF Internet-Draft (expired), draft-josefsson-ntruprime-ssh-02.

[i.43] F. Giacon, F. Heuer and B. Poettering: "KEM combiners". PKC 2018.

[i.44] P. Kampanakis, D. Stebila and T. Hansen: "Post-quantum hybrid key exchange in SSH". IETF Internet-Draft (work in progress), draft-kampanakis-curdle-ssh-pq-ke-21.

[i.45] A. Kipnis, J. Patarin and L. Goubin: "Unbalanced oil and vinegar signature schemes". EUROCRYPT 1999.

[i.46] V. Klíma, O. Pokorný and T. Rosa: "Attacking RSA-based sessions in SSL/TLS". CHES 2003.

[i.47] S. Kousidis, J.Roth, F. Strenzke and A. Wussler: "Post-quantum cryptography in OpenPGP". IETF Internet-Draft (work in progress), draft-ietf-openpgp-pqc-02.

[i.48] K. Kwiatkowski and P. Kampanakis: "Post-quantum hybrid ECDHE-Kyber key agreement for TLSv1.3". IETF Internet-Draft (expired), draft-kwiatkowski-tls-ecdhe-kyber-01.

[i.49] A. Langley: "CECPQ1 results". Imperial Violet blog, 28 November 2016.

[i.50] A. Langley: "CECPQ2". Imperial Violet blog, 12 December 2018.

[i.51] Y. Nir: "A hybrid signature method with strong non-separability". IETF Internet-Draft (expired), draft-nir-lamps-altcompsigs-00.

[i.52] M. Ounsworth and J. Gray: "Composite ML-KEM for use in the internet X.509 Public Key Infrastructure and CMS". IETF Internet-Draft (work in progress), draft-ietf-lamps-pq-composite-kem-03.

[i.53] M. Ounsworth, J. Gray and S. Mister: "Composite encryption for use in internet PKI". IETF Internet-Draft (expired), draft-ounsworth-pq-composite-encryption-01.

[i.54] M. Ounsworth, J. Gray, M. Pala and J. Klaussner: "Composite signatures for use in internet PKI". IETF Internet-Draft (work in progress), draft-ietf-lamps-pq-composite-sigs-10.

[i.55] M. Ounsworth, M. Pala and J. Klaussner: "Composite public and private keys for use in internet PKI". IETF Internet-Draft (expired), draft-ounsworth-pq-composite-keys-05.

[i.56] M. Ounsworth, A. Wussler and S. Kousidis: "Combiner function for hybrid key encapsulation mechanisms (Hybrid KEMs)". IETF Internet-Draft (work in progress), draft-ounsworth-cfrg-kem-combiners-05.

[i.57] C. Paquin, D. Stebila and G. Tamvada: "Benchmarking post-quantum cryptography in TLS". PQCrypto 2020.

[i.58] A. Petcher and M. Campagna: "Security of hybrid key establishment using concatenation". IACR ePrint 2023/972.

[i.59] B. Poettering and S. Rastikian: "A study of KEM generalizations". SSR 2023.

[i.60] J. Proos and C. Zalka: "Shor's discrete logarithm quantum algorithm for elliptic curves". Quantum Information and Computation 3.4 (2003), 317-344.

[i.61] P.W. Shor: "Algorithms for quantum computation: discrete logarithms and factoring". FOCS, 1994.

[i.62] D. Sikeridis, P. Kampanakis and M. Devetsikiotis: "Post-quantum authentication in TLS 1.3: A performance study". NDSS 2020.

[i.63] D. Sikeridis, P. Kampanakis and M. Devetsikiotis: "Assessing the overhead of post-quantum cryptography in TLS 1.3 and SSH". CoNEXT 2020.

[i.64] V. Shoup: "A proposal for an ISO standard for public key encryption". IACR ePrint 2001/112.

[i.65] D. Stebila, S. Fluhrer and S. Gueron: "Hybrid key exchange in TLS 1.3". IETF Internet-Draft (work in progress), draft-ietf-tls-hybrid-design-10.

[i.66] G. Taspoulos et al: "Energy consumption evaluation of post-quantum TLS 1.3 for resource-constrained embedded devices". IACR ePrint 2023/506.

[i.67] B. Westerbaan and D. Stebila: "X25519Kyber768Draft00 hybrid post-quantum key agreement". IETF Internet-Draft (expired), draft-tls-westerbaan-xyber768d00-03.

[i.68] B. Westerbaan and C.A. Wood: "X25519Kyber768Draft00 hybrid post-quantum KEM for HPKE". IETF Internet-Draft (work in progress), draft-westerbaan-cfrg-hpke-xyber768d00-03.

[i.69] R. Zhang, et al: "On the security of multiple encryption or CCA-security + CCA-security = CCA-security?". PKC 2004.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

active adversary: adversary who can query a decapsulation oracle with chosen ciphertexts or a signing oracle with chosen messages

NOTE 1: An active adversary who is attempting to recover the session key for a target ciphertext is not permitted to query the decapsulation oracle with that ciphertext.

NOTE 2: An active adversary who is attempting to forge a signature value for a target message is not permitted to query the signing oracle with that message.

NOTE 3: The present document assumes that active adversaries only have classical access to the decapsulation or signing oracles. Adversaries who can query decapsulation or signing oracles with inputs in quantum superposition are out of scope.

classical adversary: adversary who can only implement attacks on classical computers

component algorithm: cryptographic algorithm that forms part of a hybrid scheme or hybrid protocol

hybrid interoperability: property that a hybrid scheme or hybrid protocol can be completed successfully provided that at least one component algorithm is supported by both parties

hybrid protocol: protocol that incorporates two or more component algorithms providing the same cryptographic functionality

NOTE 1: The present document only considers hybrid protocols where at least one component is a post-quantum algorithm and at least one is a traditional algorithm. Hybrid protocols that combine two or more post-quantum algorithms and no traditional algorithms are out of scope.

EXAMPLE 1: A protocol that uses a hybrid key establishment scheme for confidentiality and a traditional digital signature algorithm for authentication.

EXAMPLE 2: A protocol that uses a post-quantum key encapsulation mechanism for confidentiality and a hybrid digital signature scheme for authentication.

EXAMPLE 3: A protocol that establishes an initial session key using a traditional key exchange, updates the session key using a post-quantum key encapsulation mechanism, and then performs authentication using a traditional digital signature algorithm.

NOTE 2: A protocol that negotiates the use of either a traditional algorithm or a post-quantum algorithm, but not the use of both algorithms, is not considered to be a hybrid protocol.

hybrid scheme: cryptographic scheme that incorporates two or more component algorithms providing the same cryptographic functionality

NOTE: The present document only considers hybrid schemes where at least one component is a post-quantum algorithm and at least one is a traditional algorithm. Hybrid schemes that combine two or more post-quantum algorithms and no traditional algorithms are out of scope.

EXAMPLE 1: A hybrid key establishment scheme that combines a traditional key exchange and a post-quantum key encapsulation mechanism.

EXAMPLE 2: A hybrid digital signature scheme that combines a traditional digital signature algorithm and a post-quantum digital signature algorithm.

hybrid security: property that a hybrid scheme or hybrid protocol remains secure provided that at least one component algorithm is secure

oracle: functionality that provides an adversary with the output of a cryptographic operation without the adversary needing to know the keys used in the operation

passive adversary: adversary who can only query an encapsulation oracle or a verification oracle

post-quantum algorithm: public-key algorithm believed to be secure against both classical and quantum adversaries

EXAMPLE 1: Key encapsulation mechanisms based on lattices such as the Module-Lattice-based Key Encapsulation Mechanism (ML-KEM) [i.15], or error correcting codes such as Classic McEliece [i.22].

NOTE 1: ML-KEM is derived from the Kyber [i.23] submission to the NIST Post-Quantum Cryptography Standardisation Project

EXAMPLE 2: Digital signature algorithms based on lattices such as the Module-Lattice-based Digital Signature Algorithm (ML-DSA) [i.16], or hash functions such as the Stateless Hash-based Digital Signature Algorithm [i.17].

NOTE 2: ML-DSA is derived from the Dilithium [i.27] submission to the NIST Post-Quantum Cryptography Standardisation Project.

NOTE 3: SLH-DSA is derived from the SPHINCS^{+} [i.24] submission to the NIST Post-Quantum Cryptography Standardisation Project.

quantum adversary: adversary who can implement attacks on both classical and quantum computers

traditional algorithm: public-key algorithm based on integer factorisation, finite field discrete logarithms, or elliptic curve discrete logarithms

EXAMPLE 1: Key establishment algorithms such as RSA [i.19], Finite-Field Diffie-Hellman (FFDH), and Elliptic Curve Diffie-Hellman (ECDH) [i.18].

EXAMPLE 2: Digital signature algorithms such as RSA, the finite-field Digital Signature Algorithm (DSA), and the Elliptic Curve Digital Signature Algorithm (ECDSA) [i.14].

3.2 Symbols

Void.

3.3 Abbreviations

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

CCA	Chosen-Ciphertext Attack
CMS	Cryptographic Message Syntax
CRQC	Cryptographically Relevant Quantum Computer
DHKEM	Diffie-Hellman Key Encapsulation Mechanism

DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EUF-CMA	Existential Unforgeability under Chosen-Message Attack
FFDH	Finite-Field Diffie-Hellman
FIPS	Federal Information Processing Standard
HPKE	Hybrid Public-Key Encryption
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IND-CCA	Indistinguishability under Chosen-Ciphertext Attack
IND-CPA	Indistinguishability under Chosen-Plaintext Attack
IRTF	Internet Research Task Force
KDF	Key Derivation Function
KDFEM	Key Derivation Function Encapsulation Mechanism
KEM	Key Encapsulation Mechanism
LMS	Leighton-Micali Signature
ML-DSA	Module-Lattice-based Digital Signature Algorithm
ML-KEM	Module-Lattice-based Key Encapsulation Mechanism
OW-CCA	One-Way under Chosen-Ciphertext Attack
OW-CPA	One-Way under Chosen-Plaintext Attack
PKCS	Public-Key Cryptography Standards
PRF	Pseudo-Random Function
RSA	Rivest-Shamir-Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SIKE	Supersingular Isogeny Key Encapsulation
SLH-DSA	Stateless Hash-based Digital Signature Algorithm
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UOV	Unbalanced Oil and Vinegar
XMSS	eXtended Merkle Signature Scheme

4 Introduction

The security of traditional approaches to public-key cryptography, including key establishment and digital signatures, relies on the difficulty of factoring integers or computing discrete logarithms over finite fields or elliptic curves. When suitably parameterised, these algorithms are believed to be hard to break using classical computers. However, they are known to be vulnerable to attacks using quantum computers [i.60] and [i.61].

Although existing quantum computers are not large enough to threaten currently deployed algorithms, the risk associated with the future development of a Cryptographically Relevant Quantum Computer (CRQC) is best mitigated by migrating to post-quantum cryptography.

EXAMPLE 1: In a store-and-decrypt attack, long-lived sensitive information protected by a traditional key establishment algorithm could be intercepted and stored by an adversary, and subsequently decrypted once a CRQC is available.

EXAMPLE 2: In a future forgery attack, a long-lived root of trust protected by a traditional digital signature algorithm might still be trusted and could be exploited by an adversary once a CRQC is available.

Post-quantum algorithms are intended to be secure against both classical and quantum computers. ETSI TR 103 616 [i.1] gives an overview of post-quantum digital signature algorithms and ETSI TR 103 823 [i.4] gives an overview of post-quantum public-key encryption algorithms and key encapsulation mechanisms. (See annexes A and B for background on key encapsulation mechanisms and digital signature algorithms.)

During the migration to post-quantum cryptography there will be situations where it could be desirable to combine existing traditional algorithms with post-quantum algorithms in a hybrid scheme. The main reasons for considering hybrid schemes are:

- to maintain security in the event that vulnerabilities are found in the post-quantum algorithm or its implementation (see clause 5.1);