ETSI TR 103 616 V1.1.1 (2021-09)

CYBER;
Quantum-Safe Signatures

Reference

DTR/CYBER-QSC-008

Keywords

algorithm, cybersecurity

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:
http://www.etsi.org/standards-search

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 at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

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 provides technical descriptions of the digital signature schemes submitted to the National Institute of Standards and Technology (NIST) for the third round of their post-quantum cryptography standardization process.

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] NIST FIPS 197: "Advanced Encryption Standard (AES)".

[i.2] NIST FIPS 180-4: "Secure Hash Standard".

[i.3] NIST FIPS 202: "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions".

[i.4] NIST IR 8105: "Report on Post-Quantum Cryptography".

[i.5] NIST FIPS 186-4: "Digital Signature Standard (DSS)".

[i.6] NIST SP-56A: "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography".

[i.7] NIST SP-56B: "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography".

[i.8] NIST: "Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process", December 2016.

NOTE: Available at https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf.

[i.9] NIST: "Post-Quantum Cryptography Standardization: Round 1 Submissions".

NOTE: Available at https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions.

[i.10] NIST IR 8240: "Status Report on the First Round of the NIST Post-Quantum Standardization Process".

[i.11] NIST: "Post-Quantum Cryptography Standardization: Round 2 Submissions".

NOTE: Available at https://csrc.nist.gov/Projects/post-quantum-cryptography/round-2-submissions.

[i.12] NIST IR 8309: "Status Report on the Second Round of the NIST Post-Quantum Standardization Process".

[i.13] NIST: "Post-Quantum Cryptography Standardization: Round 3 Submissions".

NOTE: Available at https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions.

[i.14] L. Lamport: "Constructing digital signatures from a one way function". Technical Report SRI-CSL-98. SRI International Computer Science Laboratory. 1979.

[i.15] R. Merkle: "A Certified Digital Signature". CRYPTO "89, LNCS, Vol. 263. Springer, pages 218-238, 1989.

[i.16] A. Fiat and A. Shamir: "How to Prove Yourself: Practical Solutions to Identification and Signature Problems". CRYPTO 86, LNCS, Vol. 435. Springer, pages 186-194, 1986.

[i.17] ETSI GR QSC 001: "Quantum-Safe Cryptography (QSC); Quantum-Safe Algorithmic Framework".

NOTE: Available at https://www.etsi.org/deliver/etsi_gr/QSC/001_099/001/01.01.01_60/gr_QSC001v010101p.pdf.

[i.18] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler and D. Stehlé: "CRYSTALS-DILITHIUM: Algorithm Specifications and Supporting Documentation". NIST round 3 post-quantum submission.

[i.19] V. Lyubashevsky: "Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures". Asiacrypt 2009, LNCS, Vol. 5912. Springer, pages 598-616.

[i.20] T. Prest, P.-A. Fouque, J. Hoffstein, P. Kirchner, V. Lyubashevsky, T. Pornin, T. Ricosset, G. Seiler, W. White and Z. Zhang: "FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU". NIST round 3 post-quantum submission.

[i.21] C. Gentry, C. Peikert, and V. Vaikuntanathan: "Trapdoors for Hard Lattices and New Cryptographic Constructions". STOC 2008, ACM, pages 197-206.

[i.22] J. Hoffstein, J. Pipher and J. H. Silverman: "NTRU: A Ring-Based Public Key Cryptosystem", ANTS-III, LNCS, Vol. 1423. Springer, pages 267-288, 1988.

[i.23] D. Stehlé and R. Steinfeld: "Making NTRU as Secure as Worst-Case Problems over Ideal Lattices". EUROCRYPT 2011, LNCS, Vol. 6632, pages 27-47.

NOTE: Available at https://eprint.iacr.org/2019/893.

[i.24] J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt and B.-Y. Yang: "Rainbow: Algorithm Specification and Documentation". NIST round 3 post-quantum submission.

[i.25] A. Kipnis, J. Patarin and L. Goubin: "Unbalanced Oil and Vinegar Signature Schemes". EUROCRYPT 1999, LNCS, Vol. 1592. Springer, pages 206-222.

[i.26] A. Petzoldt, S. Bulygin, and J. Buchmann: "CyclicRainbow - a Multivariate Signature Scheme with a Partially Cyclic Public Key". INDOCRYPT 2010, LNCS, vol. 6498, pages 33 - 48. .

[i.27] A. Casanova, J.-C. Faugère, G. Macario-Rat, J. Patarin, L. Perret and J. Ryckeghem: "GeMSS: A Great Multivariate Signature Scheme". NIST round 3 post-quantum submission.

[i.28] T. Matsumoto and H. Imai: "Public Quadratic Polynomial-Tuples for Efficient Signature-Verification and Message-Encryption". EUROCRYPT 1988, LNCS, Vol. 330. Springer, pages 419-453.

[i.29] J. Patarin: "Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithm". EUROCRYPT 1996, LNCS, Vol. 1070. Springer, pages 33-48.

[i.30] J. von zur Gathen and J. Gerhard: "Modern Computer Algebra (3. Ed.)". Cambridge University Press 2013.

[i.31] J.-C Faugère, L. Perret and J. Ryckeghem: "Software Toolkit for HFE-based Multivariate Schemes". IACR Trans. Cryptogr. Hardw. Embed. Syst. 2019, Vol. 3., pages 257-304.

[i.32] G. Zaverucha, M. Chase, D. Derler, S. Goldfeder, C. Orlandi, S. Ramacher, C. Rechberger and D. Slamanig: "The Picnic Algorithm Signature Specification". NIST round 3 post-quantum submission.

[i.33] I. Giacomelli, J. Madsen and C. Orlandi: "ZKBoo : Faster Zero-Knowledge for Boolean Circuits". USENIX Security 2016, USENIX Association, pages 1069-1083.

[i.34] J. Katz, V. Kolesnikov and X. Wang: "Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures". ACM CCS 2018, ACM, pages 525-537.

[i.35] M. R. Albrecht, C. Rechberger, T. Schneider, T. Tiessen and M. Zohner: "Ciphers for MPC and FHE". EUROCRYPT 2015. LNCS, Vol. 9056. Springer, pages 430-454.

[i.36] D. Unruh: "Non-Interactive Zero-Knowledge Proofs in the Quantum Random Oracle Model". EUROCRYPT 2015. LNCS, Vol. 9056. Springer, pages 430-454.

[i.37] A. Hulsing, D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M. M Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe and J.-P. Aumasson: "SPHINCS+: Submission to the NIST Post-Quantum Project". NIST round 3 post-quantum submission.

[i.38] S. Kölbl, M. Lauridsen, F. Mendel and C. Rechberger: "Haraka v2 - Efficient Short-Input Hashing for Post-Quantum Applications". IACR Trans. Symmetric Cryptol., volume 2016, number 2, pages 1-29, 2017.

[i.39] W. Beullens: "Improved Cryptanalysis of UOV and Rainbow". EUROCRYPT 2021, LNCS, Vol. 12696. Springer, 348-373. 2021.

[i.40] C. Tao, A. Petzoldt and J. Ding: "Improved Key Recovery of the HFEv- Signature Scheme". Cryptology ePrint Archive: Report 2020/1424.

NOTE: Available at https://eprint.iacr.org/2020/1424.

[i.41] J.O. Shallit, G.S. Frandsen, and J.F. Buss: "The Computational Complexity of some Problems of Linear Algebra". BRICS series report, Aarhus, Denmark, RS-96-33, 1996.

[i.42] M. Øygarden and D. Smith-Tone and J. Verbel: "On the Effect of Projection on Rank Attacks in Multivariate Cryptography". Cryptology ePrint Archive: Report 2021/655.

NOTE: Available at https://eprint.iacr.org/2021/655.

[i.43] I. Dinur: "Cryptanalytic Applications of the Polynomial Method for Solving Multivariate Equation Systems over GF(2)". EUROCRYPT 2021, LNCS, Vol. 12696. Springer, 374-403.

[i.44] The Rainbow Team: "Response to Recent Paper by Ward Beullens", NIST PQC Forum, December 2020.

NOTE: Available at http://precision.moscito.org/by-publ/recent/response-ward.pdf.

[i.45] ETSI TR 103 823: "CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation".

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:

$x := y$	Variable x is assigned the value of y
$x = y$	The values of x and y are equal
$x \neq y$	The values of x and y are not equal
$x \parallel y$	The concatenation of x and y
$\mathbb{F}$	A finite field
$\mathbb{F}_q$	A finite field modulo q
$\mathbb{Z}$	The ring of integers
$\mathbb{Z}_q$	The ring of integers modulo q
R	A ring of polynomials
R_q	A ring of polynomials modulo q
$R_q^{k \times k}$	The set of $k \times k$ matrices with coefficients in R_q
R_q^k	The set of $1 \times k$ matrices with coefficients in R_q
B_η	Centered binomial distribution of width η
$\mathrm{GL}_{n \times n}(\mathbb{F}_q)$	The set of $n \times n$ invertible matrices whose coefficients are over $\mathbb{F}_q$

3.3 Abbreviations

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

AES	Advanced Encryption Standard
CMA	Chosen Message Attack
CPU	Central Processing Unit
CTR	CounTeR
EUF	Existential Unforgeability
FFT	Fast Fourier Transform
FIPS	Federal Information Processing Standards
FORS	Forest Of Random Subsets
FS	Fiat-Shamir
GPV	Gentry-Peikert-Vaikuntanathan
GR	Group Report
HFE	Hidden Field Equation
IDS	Identification Scheme
KEM	Key Encapsulation Mechanism
KMA	Known Message Attack
KOA	Key Only Attack
MLWE	Module Learning With Errors
MPC	Multi-Party Computation
MQ	Multivariate Quadratic
NIST	National Institute of Standards and Technology
NTT	Number Theoretic Transform
OTS	One-Time Signature
PKE	Public-Key Encryption
PoSSo	Polynomial System Solving
PQC	Post-Quantum Cryptography
PRF	Pseudo Random Function
QROM	Quantum Random Oracle Model
QSC	Quantum-Safe Cryptography
ROM	Random Oracle Model
SHA	Secure Hash Algorithm
SHAKE	Secure Hash Algorithm and KECCAK
SIS	Short Integer Solution
SUF	Strong existential Unforgeability
UOV	Unbalanced Oil and Vinegar
UUF	Universal Unforgeability
WOTS	Winternitz One-Time Signature
XOF	eXtendable Output Function

XOR	eXclusive OR
ZK	Zero-Knowledge

4 Introduction

The National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce, is responsible for producing cryptographic standards for the protection of sensitive U.S. Federal Government information. NIST standards, such as the Advanced Encryption Standard (AES) [i.1] and Secure Hash Algorithm (SHA) standards [i.2] and [i.3], are used globally in many different protocols and products.

In April 2016, NIST announced their intention [i.4] to augment their existing portfolio of public-key cryptography standards [i.5], [i.6] and [i.7] by developing new standards for post-quantum cryptography. In December 2016, they initiated the so-called NIST Post-Quantum Cryptography (PQC) standardization process; a competition-like process with a call for proposals [i.8] for digital signatures, Public Key Encryption (PKE) schemes, and Key Encapsulation Mechanisms (KEMs), that will remain secure even in the presence of a cryptographically relevant quantum computer. The goal of the process is to perform several rounds of public evaluation over a three- to five-year period, and select one or more acceptable algorithms for standardization based on that evaluation.

NIST's deadline for submissions was November 2017. They received 69 candidates that met the minimum acceptance criteria and submission requirements: 20 digital signature schemes and 49 PKE/KEMs. Five submissions were quickly broken and formally withdrawn from the process by their designers. This left a total of 64 first round candidates [i.9]. In January 2019, NIST announced [i.10] that 26 of the first round candidates would progress to the second round of evaluation: 9 digital signature schemes and 17 PKE/KEMs [i.11].

In July 2020, NIST announced [i.12] that 15 candidate algorithms would progress to the third round of evaluation. These were split into seven finalists and eight alternate candidates. NIST described the finalists as the algorithms they consider to be the most promising for the majority of use cases, and the most likely to be ready for standardization soon after the end of the third round. The seven finalists [i.13] included three digital signature schemes and four PKE/KEMs. The alternate candidates were described as having potential for future standardization, but most likely after a fourth round of evaluation. The eight alternate candidates included three digital signature schemes and five PKE/KEMs.

In June 2021, NIST declared that the third round will be finalized by the beginning of 2022. Following recent attacks against multivariate schemes [i.39] and [i.40], NIST also announced that they were considering selecting an alternate signature for standardization at the end of third round and issuing a call for new digital signature submissions in 2022.

The purpose of the present document is to give concise descriptions of the six signature schemes remaining in the third round of NIST's standardization process. ETSI TR 103 823 [i.45] provides similar descriptions of the nine remaining PKE/KEMs.

The three digital signature finalists are:

- **Dilithium** (see clause 6.1)
- **FALCON** (see clause 6.2)
- **Rainbow** (see clause 6.3)

The three digital signature alternate candidates are:

- **GeMSS** (see clause 7.1)
- **Picnic** (see clause 7.2)
- **SPHINCS+** (see clause 7.3)

Each of these schemes has a different profile in terms of security properties and performance characteristics, so it is expected that some of these schemes will be more suited to specific deployment scenarios than others.

The descriptions provided in the present document are not intended to be substitutes for the detailed specifications submitted to NIST. Instead, the emphasis is on clear mathematical descriptions that facilitate easy comparison of the different schemes. Implementation details, such as how to encode polynomials as bit-strings, have been omitted wherever possible. As such, some of the descriptions differ from the submitted specifications, in terms of level of abstraction, use of notation, and choice of variable names.

It is expected that details of some of the schemes, such as specific parameter choices, will change during the third round of evaluation, so for consistency the descriptions are based on the official submission packages provided to NIST at the beginning of the third round [i.13].

5 Background

5.1 Terminology

A digital signature scheme consists of a triple of algorithms:

- **Key generation (KeyGen).** Outputs a new public and private key pair.
- **Sign.** Takes a private key and message as input and outputs a signature.
- **Verify.** Takes a public key, a message and a signature as input and outputs either 'accept' or 'reject'.

5.2 Families of post-quantum algorithms

The cryptosystems that have progressed to the third round of the NIST process can be classified into the following families:

- **Code-based schemes.** The security of code-based schemes depends on the difficulty of decoding vectors to find the closest codeword or shortest error vector. Code-based cryptography lends itself more naturally to the construction of PKE schemes and KEMs than to digital signature algorithms.
- **Isogeny-based schemes.** The security of isogeny-based schemes depends on the difficulty of recovering a secret isogeny between a pair of elliptic curves. Isogeny-based cryptography lends itself more naturally to the construction of PKE schemes and KEMs than to digital signatures, though there has been some progress in this area.

- **Lattice-based schemes.** The security of lattice-based schemes depends on the difficulty of finding vectors in a lattice that are relatively short, or relatively close to some target vector. Lattice-based signature schemes generally fall into two categories: NTRU-style [i.22] schemes, such as FALCON, which use lattices that have been specifically constructed to contain private short vectors, and Module Learning With Errors (MLWE) schemes such as Dilithium which use particular classes of random lattices. In many cases lattice-based schemes admit worst-case to average-case security reductions, though these reductions are often not relevant to proposed parameter sets (see ETSI TR 103 823 [i.45]).
- **Multivariate schemes.** The security of multivariate schemes depends on the difficulty of solving systems of quadratic or higher degree multivariate polynomials (PoSSo problem, also known as the MQ problem for quadratic equations). Multivariate cryptography lends itself more naturally to the construction of digital signatures than to PKE schemes or KEMs. Rainbow and G*e*MSS are multivariate-based signature schemes.
- **Symmetric schemes.** The security of such schemes depends on the security of symmetric cryptographic primitives such as hash functions and block ciphers. Symmetric cryptography only lends itself to the construction of digital signatures. Examples include SPHINCS+ and Picnic.

5.3 Security categories

NIST have provided guidance on the evaluation criteria they intend to apply to candidate submissions [i.8]. As part of this guidance they have defined the following security categories in terms of the (classical or quantum) resources required to attack different NIST-approved symmetric primitives:

- **Category 1.** Resources equivalent to or greater than key recovery for AES-128.
- **Category 2.** Resources equivalent to or greater than collision search for SHA3-256.
- **Category 3.** Resources equivalent to or greater than key recovery for AES-192.

- **Category 4.** Resources equivalent to or greater than collision search for SHA3-384.
- **Category 5.** Resources equivalent to or greater than key recovery for AES-256.

NIST recommended that submissions include parameter sets that meet the requirements for categories 1, 2 and/or 3, as they believe that these categories will provide sufficient security for the foreseeable future. However, to demonstrate flexibility, and to protect against future cryptanalytic breakthroughs, NIST also recommended that submissions include at least one parameter set that provides a substantially higher level of security. Submitters were asked to include justifications for the security categories claimed for their proposed parameter sets.

5.4 Security properties

Digital signatures are typically intended to provide authentication, integrity and non-repudiation of data. The main security goal that is relevant for signatures is existential unforgeability under chosen message attack (see annex A for further discussions on security goals). This is usually modelled as a game:

- **Existential Unforgeability under Chosen Message Attack (EUF-CMA) for signatures.** The attacker can request valid signatures of messages of their choice. The attacker's goal is to exhibit a valid signature for any message not previously queried. The scheme is EUF-CMA secure it the attacker cannot do this using less resources than the security level.

To construct some proofs of security it is necessary to make assumptions about or use idealized versions of certain cryptographic primitives; this can mean the proof does not apply to a concrete implementation. In particular, in the Random Oracle Model (ROM) hash functions are modelled as ideal entities, referred to as random oracles, which respond to new queries with answers selected uniformly at random from the output domain, and respond to previously seen queries with the answer that was given the first time the query was received.

In the ROM it is assumed that adversaries interact classically with random oracles, but in the Quantum Random Oracle Model (QROM) it is assumed that adversaries can query a random oracle in a quantum superposition of states. Although the QROM affords an adversary more computational power, it can be hard to compare proofs in the ROM to proofs in the QROM, particularly if it is possible to construct a tight proof in the ROM but not the QROM.

NIST have stated that they intend to standardize at least one EUF-CMA signature scheme. It is further assumed that an attacker has access to no more than 2^{64} chosen signed messages (though attacks requiring more messages will be taken into consideration). NIST place more emphasis on the ROM model rather than QROM. NIST has not required proof of EUF-CMA security as part of a submission, but does give consideration to such proofs.

5.5 Frameworks for constructing digital signatures

The digital signature algorithms that have progressed to the third round of the NIST process can be classified by family: lattice-based, multivariate-based or symmetric (see clause 5.2). Another way to categorize these schemes is to consider the framework used to construct these primitives (see also Table 1):

- **Hash-and-sign**. These schemes are constructed from trapdoor one-way functions. FALCON [i.20], G*e*MSS [i.27] and Rainbow [i.24] are examples of schemes within this framework.
- **Hash-based**. These schemes follow the work of Lamport [i.14] and Merkle [i.15] and construct a signature from a hash function. SPHINCS+ [i.37] is an example of a scheme within this framework.
- **Fiat-Shamir**. These schemes are constructed by using the Fiat-Shamir transform [i.16] together with a post-quantum Identification Scheme (IDS). Dilithium [i.18] and Picnic [i.32] are examples of schemes within this framework.

Table 1: Categorization of digital signature schemes based on their underlying hard problems and design frameworks

	Lattice-based	Multivariate-based	Symmetric-based
Hash-and-sign	FALCON	GeMSS Rainbow	
Hash-based			SPHINCS+
Fiat-Shamir	Dilithium		Picnic