ETSI GR QSC 001 V1.1.1 (2016-07)

**Quantum-Safe Cryptography (QSC);
Quantum-safe algorithmic framework**

Reference
DGR/QSC-001

Keywords
algorithm, authentication, confidentiality, security

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is 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 IPR Policy, no investigation, 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.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Quantum-Safe Cryptography (QSC).

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 gives an overview of the current understanding and best practice in academia and industry about quantum-safe cryptography (QSC). It focuses on identifying and assessing cryptographic primitives that have been proposed for efficient key establishment and authentication applications, and which may be suitable for standardization by ETSI and subsequent use by industry to develop quantum-safe solutions for real-world applications.

QSC is a rapidly growing area of research. There are already academic conference series such as PQC and workshops have been established by ETSI/IQC [i.1] and NIST. The European Commission has recently granted funding to two QSC projects under the Horizon 2020 framework: SAFEcrypto [i.2] and PQCrypto [i.3] and [i.4]. The present document draws on all these research efforts.

The present document will cover three main areas. Clauses 4 and 5 discuss the types of primitives being considered and describe an assessment framework; clauses 6 to 10 discuss some representative cryptographic primitives; and clause 11 gives a preliminary discussion of key sizes.

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 White Paper No. 8 (2015): "Quantum safe cryptography and security".

[i.2] NIST PQC workshop (2015): "SAFEcrypto Project", M. O'Niell.

[i.3] NIST Workshop on Cybersecurity in a Post-Quantum World (2015): "PQCrypto project", T. Lange.

[i.4] PQCrypto (2015): "Initial recommendations of long-term secure post-quantum systems".

NOTE: Available at http://www.pqcrypto.eu.org/.

[i.5] John Wiley and Sons (1996): "Applied cryptography", B. Schneier.

[i.6] ACM Symposium on Theory of Computing (1977): "Universal classes of hash functions", J. Carter and M. Wegman.

[i.7] IETF RFC 4120 (2005): "The Kerberos network authentication service (V5)", C. Neuman, T. Yu, S. Hartman and K. Raeburn.

[i.8] EUROCRYPT (2006): "QUAD: A practical stream cipher with provable security", C. Berbain, H. Gilbert and J. Patarin.

[i.9] C. Blanchard: "Security for the third generation (3G) mobile system", Information Security Technical Report, vol. 5, no. 3, pp. 55-65, 2000.

[i.10] IETF RFC 4279 (2005): "Pre-Shared Key Ciphersuites for TLS", P. Eronen and H. Tschofenig.

[i.11] ZigBee® (2015): "Zigbee alliance website".

NOTE 1: Available at http://www.zigbee.org/.

NOTE: 2 ZigBee is an example of a suitable porduct available commercially. This information is given for the convenience of users of the present document and does not constitute an endorsement by ETSI of this product.

[i.12] TU Darmstadt (2015): "Lattice challenge".

NOTE: Available at www.latticechallenge.org.

[i.13] Philips (2015): "HIMMO challenge".

NOTE: Available at www.himmo-scheme.com.

[i.14] ACM Communications in Computer Algebra, vol. 49, no. 3, pp. 105-107 (2015): "A multivariate quadratic challenge toward post-quantum generation cryptography", T. Yasuda, X. Dahan, Y.-J. Huang, T. Takagi and K. Sakurai.

[i.15] IACR ePrint Archive 2015/374 (2015): "On the impossibility of tight cryptographic reductions", C. Bader, T. Jager, Y. Li and S. Schäge.

[i.16] PQC (2014): "A note on quantum security for post-quantum cryptography", F. Song.

[i.17] CT-RSA (2003): "Forward-security in private-key cryptography", M. Bellare and B. Yee.

[i.18] draft-ietf-tls-tls13-012 (21 March 2016): "The Transport Layer Security (TLS) protocol version 1.3", E. Resorla.

[i.19] NIST Workshop on Cybersecurity in a Post-Quantum World (2015): "Failure is not an option: standardization issues for post-quantum key agreement", M. Motley.

[i.20] CRYPTO (1998): "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS#1", D. Bleichenbacher.

[i.21] CRYPTO (2000): "Differential fault attacks on elliptic curve cryptosystems", I. Biehl, B. Meyer and V. Müller.

[i.22] IACR ePrint Archive 2015/939 (2015): "A decade of lattice cryptography", C. Peikert.

[i.23] CRYPTO (1998): "Public-key cryptosystems from lattice reduction problems", O. Goldreich, S. Goldwasser and S. Halevi.

[i.24] CT-RSA (2003): "NTRUSign: Digital signatures using the NTRU lattice", J. Hoffstein, N. Howgrave-Graham, J. Pipher, J. Silverman and W. Whyte.

[i.25] EUROCRYPT (2006): "Learning a parallelepiped: Cryptanalysis of GGH and NTRU signatures", P. Q. Nguyen and O. Regev.

[i.26] ASIACRYPT (2012): "Learning a zonotope and more: Cryptanalysis of NTRUSign countermeasures", L. Ducas and P. Q. Nguyen.

[i.27] Designs, Codes and Cryptography (2014): "Finding shortest lattice vectors faster using quantum search", T. Laarhoven, M. Mosca and J. van de Pol.

[i.28] PQC Summer School (2014): "Lattice cryptography", D. Micciancio.

[i.29] FOCS (2002): "Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions", D. Micciancio.

[i.30] Journal of the ACM (JACM), vol. 60, no. 6, p. 43 (2013): "On ideal lattices and learning with errors over rings", V. Lyubashevsky, C. Peikert and O. Regev.

[i.31] Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing (1996): "Generating hard instances of lattice problems", M. Ajtai.

[i.32] 2nd ETSI Quantum Safe Workshop (2014): "Soliloquy: A cautionary tale", P. Campbell, M. Groves and D. Shepherd.

[i.33] CRYPTO (2015): "Provably weak instances of Ring-LWE", Y. Elias, K. E. Lauter, E. Ozman and K. E. Stange.

[i.34] IACR ePrint Archive 2016/351 (2016): "How (not) to instantiate Ring-LWE", C. Peikert.

[i.35] PQC (2014): "Lattice cryptography for the internet", C. Peikert.

[i.36] Security and Privacy (2015): "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem", J. W. Bos, C. Costello, M. Naehrig and D. Stebila.

[i.37] IACR ePrint Archive 138/2015 (2015): "A practical key exchange for the internet using lattice cryptography", V. Singh.

[i.38] IACR ePrint Archive 2015/1120 (2015): "Even more practical key exchanges for the internet using lattice cryptography", V. Singh and A. Chopra.

[i.39] IACR ePrint Archive 2015/1092 (2015): "Post-quantum key exchange - A new hope", E. Alkim, L. Ducas, T. Pöppelmann and P. Schwabe.

[i.40] EUROCRYPT (2015): "Authenticated key exchange from ideal lattices", J. Zhang, Z. Zhang, J Ding, M. Snook and O. Dagdelen.

[i.41] Applied Cryptography and Network Security (2015): "Post-quantum forward secure onion routing (future anonymity in today's budget)", S. Ghosh and A. Kate.

[i.42] ANTS III (1998): "NTRU: A ring-based public key cryptosystem", J. Hoffstein, J. Pipher and J. H. Silverman.

[i.43] EUROCRYPT (2011): "Making NTRU as secure as worst-case problems over ideal lattices", D. Stehlé and R. Steinfeld.

[i.44] IEEE 1363.1 (2008): "Public-key cryptographic techniques based on hard problems over lattices".

[i.45] ANSI X9.98 (2010): "Lattice-based polynomial public key establishment algorithm for the financial services industry".

[i.46] IACR ePrint Archive 2015/708 (2015): "Choosing parameters for NTRUEncrypt", J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte and Z. Zhang.

[i.47] CRYPTO (2015): "An improved BKW algorithm for LWE with applications to cryptography and lattices", P.A. Fouque and P. Kirchner.

[i.48] IACR ePrint Archive 2015/676 (2015): "Quantum cryptanalysis of NTRU", S. Fluhrer.

[i.49] W. Whyte (2015): "EEES#1: Implementation aspects of NTRUEncrypt, Version 3.1".

NOTE: Available at https://github.com/NTRUOpenSourceProject/ntru-crypto/blob/master/doc/EESS1-v3.1.pdf.

[i.50] CRYPTO (2007): "A hybrid lattice-reduction and meet-in-the-middle attack against NTRU", N. Howgrave-Graham.

[i.51] IACR ePrint Archive 2014/698 (2014): "HIMMO - A lightweight, fully collusion resistant key pre-distribution scheme", O. Garcia-Morchon, R. Rietman, L. Tolhuizen, D. Gomez and J. Gutierrez.

[i.52] IACR ePrint Archive 2016/152 (2016): "Attacks and parameter choices in HIMMO", O. Garcia Morchon, R. Rietman, L. Tolhuizen, J.-L. Torre-Arce, M. S. Lee, D. Gomez-Perez, J. Gutierrez and B. Schoenmakers.

[i.53] IACR ePrint Archive 2015/1003 (2015): "Results on polynomial interpolation with mixed modular operations and unknown moduli", O. Garcia-Morchon, R. Rietman , I. Shparlinski and L. Tolhuizen.

[i.54] CRYPTO (2005): "HMQV: A high performance secure Diffie-Hellman protocol", H. Krawczyk.

[i.55] IACR ePrint Archive 2016/410 (2016): "Efficient quantum-resistant trust infrastructure based on HIMMO", O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.-L. Torre-Arce, S. Bhattacharya and M. Bodlaender.

[i.56] IACR ePrint Archive 2016/085 (2016): "Cryptanalysis of Ring-LWE based key exchange with key share reuse", S. Fluhrer.

[i.57] CRYPTO (2003): "The impact of decryption failures on the security of NTRU encryption", N. Howgrave-Graham, P. Q. Nguyen, D. Pointcheval, J. Proos, J. H. Silverman, A. Singer and W. Whyte.

[i.58] IACR ePrint Archive 2003/172 (2003): "NAEP: Provable security in the presence of decryption failures", N. Howgrave-Graham, J. H. Silverman, A. Singer and W. Whyte.

[i.59] ASIACRYPT (2009): "Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures", V. Lyubashevsky.

[i.60] EUROCRYPT (2012): "Lattice signatures without trapdoors", V. Lyubashevsky.

[i.61] ASIACRYPT (2013): "The Fiat-Shamir transformation in a quantum world", Ö. Dagdelen, M. Fischlin and T. Gagliardoni.

[i.62] CHES (2012): "Practical lattice-based cryptography: A signature scheme for embedded systems", T. Güneysu, V. Lyubashevsky and T. Pöppelmann.

[i.63] CRYPTO (2013): "Lattice signatures and bimodal Gaussians", L. Ducas, A. Durmus, T. Lepoint and V. Lyubashevsky.

[i.64] CT-RSA (2014): "An improved compression technique for signatures based on learning with errors", S. Bai and S. D. Galbraith.

[i.65] AFRICACRYPT (2016): "An efficient lattice-based signature scheme with provably secure instantiation", S. Akleylek, N. Bindel, J. Buchmann, J. Krämer and G. Marson.

[i.66] IACR ePrint Archive 2014/874 (2014): "Accelerating BLISS: The geometry of ternary polynomials", L. Ducas.

[i.67] IACR ePrint Archive 2016/276 (2016): "Arithmetic coding and blinding countermeasures for Ring-LWE", M.-J. Saarinen.

[i.68] IACR ePrint Archive 2016/300 (2016): "Flush, Gauss and reload - A cache timing attack on the BLISS lattice-based signature scheme", L. G. Bruinderink, A. Hülsing, T. Lange and Y. Yarom.

[i.69] PQC (2014): "Transcript secure signatures based on modular lattices", J. Hoffstein, J. Pipher, J. M. Schanck, J. H. Silverman and W. Whyte.

[i.70] PQC (2014): "Sealing the leak on classical NTRU signatures", C. M. Aguilar, X. Boyen, J. C. Deneuville and P. Gaborit.

[i.71] ASIACRYPT (2014): "Efficient identity-based encryption over NTRU lattices", L. Ducas, V. Lyubashevsky and T. Prest.

[i.72] SIAM Journal on Computing, vol. 33, no. 3, pp. 738-760 (2004): "Quantum computation and lattice problems", O. Regev.

[i.73] Journal of Mathematical Cryptography, vol. 9, no. 3, pp. 169-203 (2015): "On the concrete hardness of learning with errors", M. R. Albrecht, R. Player and S. Scott.

[i.74] Gröbner Bases, Coding, and Cryptography (2009): "Overview of cryptanalysis techniques in multivariate public key cryptography", O. Billet and J. Ding.

[i.75] Designs, Codes and cryptography, pp. 69(1) p. 1-52 (2013): "Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic", L. Bettale, J.-C. Faugère and L. Perrett.

[i.76] ASIACRYPT (2010): "The degree of regularity of HFE systems", V. Dubois and N. Gama.

[i.77] PQC (2013): "Degree of regularity for HFEv and HFEv-", J. Ding and B. Y. Yang.

[i.78] Journal of Mathematical Cryptology, vol. 3, no. 3, pp. 177-197 (2009): "Hybrid approach for solving multivariate systems over finite fields", L. Bettale, J.-C. Faugère and L. Perret.

[i.79] IACR ePrint Archive 2010/596 (2010): "Solving systems of multivariate quadratic equations over finite fields or: From relinearization to MutantXL", E. Thomae and C. Wolf.

[i.80] PQC (2010): "Selecting parameters for the Rainbow signature scheme", A. Petzoldt, S. Bulygin and J. Buchmann.

[i.81] CRYPTO (1995): "Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt '88", J. Patarin.

[i.82] ASIACRYPT (2000): "Cryptanalysis of the TTM cryptosystem", L. Goubin and N. T. Courtois.

[i.83] EUROCRYPT (2005): "Differential cryptanalysis for multivariate schemes", P.-A. Fouque, L. Granboulan and J. Stern.

[i.84] PKC (2007): "Cryptanalysis of HFE with internal perturbation", V. Dubois, L. Granboulan and J. Stern.

[i.85] CRYPTO (2007): "Practical cryptanalysis of SFLASH", V. Dubois, P.-A. Fouque, A. Shamir and J. Stern.

[i.86] M. R. Garey and D. S. Johnson, Computers and intractibility: "A guide to the theory of NP-completeness", New York: W.H. Freeman (1979).

[i.87] Effective Methods in Algebraic Geometry (2005): "Asymptotic behaviour of the index of regularity of quadratic semi-regular polynomial systems", M. Bardet, J.-C. Faugère, B. Salvy and B. Y. Yang.

[i.88] Information and Communications Security, pp. 356-368 (1997): "Trapdoor one-way permutations and multivariate polynomials", J. Patarin and L. Goubin.

[i.89] EUROCRYPT (2000): "Efficient algorithms for solving overdefined systems of multivariate polynomial equations", N. Courtois, A. Klimov, J. Patarin and A. Shamir.

[i.90] INRIA Research Report 5049 (2003): "Complexity of Gröbner basis computations for semi-regular overdetermined sequences over F-2 with solutions in F-2", M. Bardet, J.-C. Faugère and B. Salvy.

[i.91] PKC (2002): "Solving underdefined systems of multivariate quadratic equations", N. Courtois, L. Goubin, W. Meier and J. D. Tacier.

[i.92] PKC (2012): "Solving underdetermined systems of multivariate quadratic equations revisited", E. Thomae and C. Wolf.

[i.93] PQC (2011): "On provable security of UOV and HFE signature schemes against chosen-message attack", K. Sakumoto, T. Shirai and H. Hiwatari.

[i.94] INDOCRYPT (2010): "Towards provable security of the Unbalanced Oil and Vinegar signature scheme under direct attacks", S. Bulygin, A. Petzoldt and J. Buchmann.

[i.95] PQC (2013): "Simple Matrix scheme for encryption", C. Tao, A. Diene, S. Tang and J. Ding.

[i.96] PQC (2014): "An optimal structural attack on the ABC multivariate encryption scheme", D. Moody, R. Perlner and D. Smith-Tone.

[i.97] Finite Fields and their Applications, vol. 35, pp. 352-368 (2015): "Simple Matrix - A multivariate public key cryptosystem (MPKC) for encryption", C. Tao, H. Xiang, A. Petzoldt and J. Ding.

[i.98] IACR ePrint Archive 2016/010 (2016): "Eliminating decryption failures from the Simple Matrix encryption scheme", A. Petzoldt, J. Ding and L.-C. Wang.

[i.99] IACR ePrint Archive 2016/065 (2016): "A note on Tensor Simple Matrix Encryption scheme", Y. Hashimoto.

[i.100] EUROCRYPT (1996): "Hidden field equations (HFE) and isomorphisms of polynomials (IP): Two new families of asymmetric algorithms", J. Patarin.

[i.101] CRYPTO (2003): "Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases", J.-C. Faugère and A. Joux.

[i.102] CRYPTO (2011): "Inverting HFE systems is quasi-polynomial for all fields", J. Ding and T. J. Hodges.

[i.103] PQC Winter School (2016): "Gröbner basis techniques in post-quantum cryptography", L. Perret.

[i.104] PQC (2014): "ZHFE, a new multivariate public key encryption scheme", J. Porras, J. Baena and J. Ding.

[i.105] PQC (2016): "Security analysis and key modification for ZHFE", R. Perlner and D. Smith-Tone.

[i.106] PQC (2016): "Efficient ZHFE key generation", J. B. Baena, D. Carbacas, D. E. Escudero, J. Porras-Barrera and J. A. Verbel.

[i.107] PQC (2016): "Extension field cancellation: A new central trapdoor for multivariate quadratic systems", A. Szepieniec, J. Ding and B. Preneel.

[i.108] ASIACRYPT (2011): "Polly Cracker, revisited", M. R. Albrecht, P. Farshim, J.-C. Faugère and L. Perret.

[i.109] IACR ePrint Archive 2011/289 (2011): "Polly Cracker, revisited", M. R. Albrecht, J.-C. Faugère, P. Farshim, G. Herold and L. Perret.

[i.110] Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (2006): "On achieving chosen ciphertext security with decryption errors", Y. Cui, K. Kobara and H. Imai.

[i.111] CRYPTO (2011): "Public-key identification schemes based on multivariate quadratic polynomials", K. Sakumoto, T. Shirai and H. Hiwatari.

[i.112] CT-RSA (2001): "Quartz, 128-bit long digital signatures", J. Patarin, N. Courtois and L. Goubin.

[i.113] PKC (2003): "On the security of HFE, HFEv- and Quartz", N. T. Courtois, M. Daum and P. Felke.

[i.114] NIST Workshop on Cybersecurity in a Post-Quantum World (2015): "Gui: Revisiting multivariate digital signature schemes based on HFEv- (draft)", J. Ding.

[i.115] ASIACRYPT (2015): "Design principles for HFEv- based multivariate signature schemes", A. Petzoldt, M. S. Chen, B. Y. Yang, C. Tao and J. Ding.

[i.116] PQC (2016): "On the differential security of the HFEv- signature primitive", R. Cartor, R. Gipson, D. Smith-Tone and J. Vates.

[i.117] EUROCRYPT (1999): "Unbalanced Oil and Vinegar signature schemes", A. Kipnis, J. Patarin and L. Goubin.

[i.118] TU Darmstadt (2013): "Selecting and reducing key sizes for multivariate cryptography", A. Petzoldt.

[i.119] Applied Cryptography and Network Security (2005): "Rainbow, a new multivariable polynomial signature scheme", J. Ding and D. Schmidt.

[i.120] INDOCRYPT (2010): "CyclicRainbow - A multivariate signature scheme with a partially cyclic public key", A. Petzoldt, S. Bulygin and J. Buchmann.

[i.121] Security and Cryptography for Networks (2006): "Cryptanalysis of Rainbow", O. Billet and H. Gilbert.

[i.122] Applied Cryptography and Network Security (2008): "New differential-algebraic attacks and reparametrization of Rainbow", J. Ding, B.-Y. Yang, C. H. O. Chen, M. S. Chen and C. M. Cheng.