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

Copyright Notification

Contents

Intellectual Property Rights 6

Foreword 6

Modal verbs terminology 6

1 Scope 7

2 References 7
2.1 Normative references 7
2.2 Informative references 7

3 Abbreviations 16

4 Primitives under consideration 17
4.1 Introduction 17
4.2 Primitive families 17
4.3 Primitive types 17
4.4 Application-specific or restricted-use cases 18
4.5 Other mechanisms 18

5 Assessment framework 18
5.1 Introduction 18
5.2 Assessment criteria 18
5.2.1 Security 18
5.2.2 Efficiency 19
5.2.3 Implementation and deployment issues 19
5.3 Security considerations 19
5.3.1 Classical security 19
5.3.2 Quantum security 19
5.3.3 Provable security 20
5.3.4 Forward security 20
5.3.5 Active security 20

6 Lattice-based primitives 21
6.1 Introduction 21
6.2 Provable security 21
6.3 Key establishment 22
6.3.1 Key agreement primitives 22
6.3.1.1 Peikert 22
6.3.1.2 Zhang et al 22
6.3.1.3 Ghosh-Kate 22
6.3.2 Key transport primitives 22
6.3.2.1 NTRUEncrypt 22
6.3.3 Other key establishment primitives 23
6.3.3.1 HIMMO 23
6.3.4 Forward security 23
6.3.5 Active security 23
6.4 Authentication 23
6.4.1 Fiat-Shamir signatures 23
6.4.1.1 Lyubashevsky 23
6.4.1.2 Güneysu-Lyubashevsky-Pöppelmann 23
6.4.1.3 BLISS 24
6.4.2 Hash-and-sign signatures 24
6.4.2.1 NTRU-MLS 24
6.4.2.2 Aguilar et al 24
6.4.2.3 Ducas-Lyubashevsky-Prest 24
6.4.3 Other authentication primitives 24
6.4.3.1 HIMMO 24
6.5 Quantum security 24

7 Multivariate schemes 25

7.1 Introduction 25
7.2 Provable security 25
7.3 Key establishment 26
7.3.1 Key transport primitives 26
7.3.1.1 Simple Matrix 26
7.3.1.2 HFE 26
7.3.1.3 ZHFE 26
7.3.1.4 Polly Cracker Revisited 26
7.3.2 Forward security 26
7.3.3 Active security 27
7.4 Authentication 27
7.4.1 Fiat-Shamir signatures 27
7.4.1.1 Sakumoto-Shirai-Hiwatari 27
7.4.2 Hash-and-sign signatures 27
7.4.2.1 Quartz 27
7.4.2.2 Gui 27
7.4.2.3 UOV 27
7.4.2.4 Rainbow 28
7.5 Quantum security 28

8 Code-based primitives 28
8.1 Introduction 28
8.2 Provable security 28
8.3 Key establishment 29
8.3.1 Key transport primitives 29
8.3.1.1 McEliece and Niederreiter 29
8.3.1.2 Wild McEliece 29
8.3.1.3 MDPC McEliece 29
8.3.1.4 LRPC McEliece 29
8.3.2 Forward security 29
8.3.3 Active security 29
8.4 Authentication 30
8.4.1 Fiat-Shamir signatures 30
8.4.1.1 Cayrel et al 30
8.4.2 Hash-and-sign signatures 30
8.4.2.1 CFS 30
8.4.2.2 RankSign 30
8.5 Quantum security 30

9 Hash-based primitives 30
9.1 Introduction 30
9.2 Provable security 31
9.3 Authentication 31
9.3.1 Stateful signatures 31
9.3.1.1 Merkle 31
9.3.1.2 XMSS 31
9.3.2 Stateless signatures 31
9.3.2.1 SPHINCS 31
9.4 Quantum security 32

10 Isogeny-based primitives 32
10.1 Introduction 32
10.2 Provable security 32
10.3 Key establishment 32
10.3.1 Key agreement primitives 32
10.3.1.1 Jao-De Feo 32
10.3.2 Forward security 33
10.3.3 Active security 33
10.4 Authentication 33
10.4.1 Other authentication primitives 33
10.4.1.1 Jao-Soukharev 33
10.4.1.2 Sun-Tian-Wang 33
10.5 Quantum security 33

11 Key length summary 33
11.1 Introduction 33
11.2 Key establishment 34
11.3 Authentication 35

12 Conclusions 36

Annex A: Classical key size comparison 38

A.1 Key establishment 38

A.2 Authentication 39

Annex B: Quantum key size comparison 40

B.1 Key establishment 40

B.2 Authentication 41

History 42

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.

[i.123] IACR ePrint Archive 2012/223 (2012): "A generalisation of the Rainbow band separation attack and its applications to multivariate systems", E. Thomae.

[i.124] SIAM Journal on Computing, vol. 26, no. 5, pp. 1519-1523 (1997): "Strengths and weaknesses of quantum computing", C. H. Bennett, E. Bernstein, G. Brassard and U. Vazirani.

[i.125] ISIT (2013): "MDPC-McEliece: New McEliece variants from moderate parity-check codes", R. Misoczki, J.-P. Tillich, N. Sendrier and P. S. Barreto.

[i.126] PQC (2009): "Code-based cryptography", R. Overbeck and N. Sendrier.

[i.127] Symbolic Computation and Cryptography (2008): "Cryptanalysis of McEliece cryptosystem based on quasi-cyclic LDPC codes", A. Otmani, J.-P. Tillich and L. Dallot.

[i.128] PQC (2010): "Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes", C. Wieschebrink.

[i.129] EUROCRYPT (2010): "Algebraic cryptanalysis of McEliece variants with compact keys", J.-C. Faugère, A. Otmani, L. Perret and J.-P. Tillich.

[i.130] Designs, Codes and Cryptography (2014): "Structural cryptanalysis of McEliece schemes with compact keys", J.-C. Faugère, A. Otmani, L. Perret, F. De Portzamparc and J.-P. Tillich.

[i.131] UPMC (2015): "Algebraic and physical security in code-based cryptography", PhD Thesis and F. Urvoy de Portzamparc.

[i.132] IEEE Transactions on Information Theory, vol. 34, no. 5, pp. 1354-1359 (1988): "A probabilistic algorithm for computing minimum weights of large error-correcting codes", J. S. Leon.

[i.133] Coding Theory and Applications (1988): "A method for finding codeworkds of small weight", J. Stern.

[i.134] EUROCRYPT (2015): "On computing nearest neighbours with applications to decoding of binary linear codes", A. May and I. Ozerov.

[i.135] PQC (2010): "Grover vs McEliece", D. J. Bernstein.

[i.136] IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 384-386 (1978): "On the inherent intractibility of certain coding problems", E. R. Berlekamp, R. J. McEliece and H. C. Van Tilborg.

[i.137] Foundations of Computer Science (2003): "More on average case vs approximation complexity", M. Alekhnovich.

[i.138] ITW (2011): "The tightness of security reductions in code-based cryptography", N. Sendrier.

[i.139] IEEE Transactions on Information Theory, pp. 59(10):6830-6844 (2013): "A distinguisher for high rate McEliece cryptosystems", J.-C. Faugère, V. Gauthier, A. Otmani, L. Perret and J.-P. Tillich.

[i.140] EUROCRYPT (2014): "Polynomial time attack on wild McEliece over quadratic extensions", A. Couvreur, A. Otmani and J.-P. Tillich.

[i.141] DSN progress report 42.44 (1978:) "A public key cryptosystem based on algebraic coding theory", R. McEliece.

[i.142] Problems of Control and Information Theory, vol. 15, no. 2, pp. 159-166 (1986): "Knapsack-type cryptosystems and algebraic coding theory", H. Niederreiter.

[i.143] PKC (2001): "Semantically secure McEliece public-key cryptosystem - Conversions for McEliece PKC", K. Kobara and H. Imai.

[i.144] PQC (2008): "Attacking and defending the McEliece cryptosystem", D. J. Bernstein, T. Lange and C. Peters.

[i.145] ASIACRYPT (2011): "Decoding random linear codes in O(2^0.054n)", A. May, A. Meurer and E. Thomae.

[i.146] EUROCRYPT (2012): "Decoding random binary linear codes in 2^n/20: How 1+1=0 improves information set decoding", A. Becker, A. Joux, A. May and A. Meurer.

[i.147] International Journal of Information Security, vol. 11, no. 3, pp. 137-147 (2012): "Selecting parameter sizes for secure McEliece-based cryptosystems", R. Niebuhr, M. Meziani, S. Bulygin and J. Buchmann.

[i.148] CHES (2013): "McBits: Fast constant-time code-based cryptography", D. J. Bernstein, T. Chou and P. Schwabe.

[i.149] SAC (2011): "Wild McEliece", D. J. Bernstein, T. Lange and C. Peters.

[i.150] PQC (2011): "Wild McEliece incognito", D. J. Bernstein, T. Lange and C. Peters.

[i.151] ASIACRYPT (2014): "Algebraic attack against variants of McEliece with Goppa polynomial of a special form", J.-C. Faugère, L. Perret and F. De Portzamparc.

[i.152] ACCT (2014): "On cellular code and their cryptographic applications", P. Loidreau.

[i.153] AFRICACRYPT (2016): "Weak keys for the quasi-cyclic MDPC public key encryption scheme", M. Bardet, V. Dragoi, J. G. Luque and A. Otmani.

[i.154] WCC (2013): "Low rank parity check codes and their applications to cryptography", P. Gaborit, G. Murat, O. Ruatta and G. Zémor.

[i.155] ArXiv Preprint 1404.3482 (2014): "On the hardness of the decoding and the minimum distance problems for rank codes", P. Gaborit and G. Zémor.

[i.156] ISIT (2015): "New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem", A. Hauteville and J.-P. Tillich.

[i.157] AFRICACRYPT (2014): "New results for rank-based cryptography", P. Gaborit, O. Ruatta, J. Schrek and G. Zémor.

[i.158] CRYPTO (1999): "Secure integration of asymmetric and symmetric encryption schemes", E. Fujisaki and T. Okamoto.

[i.159] SAC (2010): "A zero-knowledge identification scheme based on the q-ary syndrome decoding problem", P.-L. Cayrel, P. Véron and S. M. El Yousfi Alaoui.

[i.160] CRYPTO (1993): "A new identification scheme based on syndrome decoding", J. Stern.

[i.161] AFRICACRYPT (2012): "Extended security arguments for signature schemes", S. M. El Yousfi Alaoui, Ö. Dagdalen, P. Véron, D. Galindo and P.-L. Cayrel.

[i.162] Western European Workshop on Research in Cryptology (2011): "Efficient implementation of code-based identification schemes", P.-L. Cayrel, S. M. El Yousfi Alaoui, F. Günther, G. Hoffmann and H. Rother.

[i.163] ASIACRYPT (2001): "How to achieve a McEliece-based digital signature scheme", N. T. Courtois, M. Finiasz and N. Sendrier.

[i.164] Research in Cryptology (2008): "Towards a concrete security proof of Courtois, Finiasz and Sendrier signature scheme", L. Dallot.

[i.165] SAC (2011): "Parallel-CFS", M. Finiasz.

[i.166] PQC (2011): "Decoding one out of many", N. Sendrier.

[i.167] INDOCRYPT (2012): "Implementing CFS", G. Landais and N. Sendrier.

[i.168] PQC (2014): "RankSign: an efficient signature algorithm based on the rank metric", P. Gaborit, O. Ruatta, J. Schrek and G. Zémor.

[i.169] CRYPTO (2011): "McEliece and Niederreiter cryptosystems that resist quantum Fourier sampling attacks", H. Dinh, C. Moore and A. Russell.

[i.170] PQC (2009): "Hash-based digital signature schemes", J. Buchmann, E. Dahmen and M. Szydlo.

[i.171] draft-mcgrew-hash-sigs-04 (21 March 2016): "Hash-based signatures", D. McGrew and M. Curcio.

[i.172] draft-irtf-cfrg-xmss-hash-based-signatures-03 (15 February 2016): "XMSS: Extended hash-based signatures", A. Hülsing, D. Butin, S. Gazdag and A. Mohaisen.

[i.173] Stanford University (1979): "Secrecy, authentication and public-key systems", R. C. Merkle.

[i.174] CRYPTO (1989): "A certified digital signature", R. C. Merkle.

[i.175] IACR ePrint Archive 2016/357 (2016): "State management for hash based signatures", D. McGrew, P. Kampanakis, S. Fluhrer, S.-L. Gazdag, D. Butin and J. Buchmann.

[i.176] SHARCS (2009): "Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?", D. J. Bernstein.

[i.177] draft-mcgrew-hash-sigs-02 (4 July 2014): "Hash-based signatures", D. McGrew and M. Curcio.

[i.178] Cryptography and Coding (2005): "Hash based digital signature schemes", C. Dods, N. P. Smart and M. Stam.

[i.179] IACR ePrint Archive 2005/192 (2005): "On the security and efficiency of the Merkle signature scheme", L. C. C. Garcia.

[i.180] J. Katz (2015): "Analysis of a proposed hash-based signature standard".

NOTE: Available at https://www.cs.umd.edu/~jkatz/papers/HashBasedSigs.pdf.

[i.181] PQC (2011): "XMSS - A practical forward secure signature scheme based on minimal security assumptions", J. Buchmann, E. Dahmen and A. Hülsing.

[i.182] Security Engineering and Intelligence Informatics (2013): "Optimal parameters for XMSS^MT", A. Hülsing, L. Raush and J. Buchmann.

[i.183] draft-irtf-cfrg-xmss-hash-based-signatures-00 (8 April 2015): "XMSS: Extended hash-based signatures", A. Hülsing, D. Butin, S. Gazdag and A. Mohaisen.

[i.184] PKC (2016): "Mitigating multi-target attacks in hash-based signatures", A. Hülsing, J. Rijneveld and F. Song.

[i.185] EUROCRYPT (2015): "SPHINCS: Practical stateless hash-based signatures", D. J. Bernstein, D. Hopwood, A. Hülsing, T. Lange, R. Niederhagen, L. Papachristodoulou, M. Schneider, P. Schwabe and Z. Wilcox-O'Hearn.

[i.186] LATIN (1998): "Quantum cryptanalysis of hash and claw-free functions.", G. Brassard, P. Hoyer and A. Tapp.

[i.187] 2nd ACM Conference on Computer and Communications Security (1994): "Parallel collision search with application to hash functions and discrete logarithms", P. C. Van Oorschot and M. J. Wiener.

[i.188] CRC Press (2008): "Elliptic curves: number theory and cryptography", L. Washington.

[i.189] Norwegian Information Security Conference (2009): "Reductionist security arguments for public-key cryptographic schemes based on group action", A. Stolbunov.

[i.190] Applicable Algebra in Engineering, Communication and Computing, vol. 24, no. 2, pp. 107-131 (2013): "Improved algorithm for the isogeny problem for ordinary elliptic curves", S. Galbraith and A. Stolbunov.

[i.191] Designs, Codes and Cryptography (2014): "Computing isogenies between supersingular elliptic curves over Fp", C. Delfs and S. D. Galbraith.

[i.192] Journal of Mathematical Cryptology, vol. 8, no. 1, pp. 1-29 (2014): "Constructing elliptic curve isogenies in quantum subexponential time", A. Childs, D. Jao and V. Soukharev.

[i.193] INDOCRYPT (2014): "A quantum algorithm for computing isogenies between supersingular elliptic curves", J.-F. Biasse, D. Jao and A. Sankar.

[i.194] PQC (2011): "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", D. Jao and L. De Feo.

[i.195] Journal of Mathematical Cryptography, vol. 8, no. 3, pp. 209-247 (2014): "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", L. De Feo, D. Jao and J. Plût.

[i.196] IACR ePrint Archive 2016/229 (2016): "Key compression for isogeny-based cryptosystems", R. Azarderakhsh, D. Jao, K. Kalach, B. Koziel and C. Leonardi.

[i.197] IACR ePrint Archive 2016/413 (2016): "Efficient algorithms for supersingular isogeny Diffie-Hellman", C. Costello, P. Longa and M. Naehrig.

[i.198] PQC (2014): "Isogeny-based quantum-resistant undeniable signatures", D. Jao and V. Soukharev.

[i.199] Intelligent Networking and Collaborative Systems (2012): "Toward quantum-resistant strong designated verifier signature from isogenies", X. Sun, H. Tian and Y. Wang.

[i.200] PQC (2016): "Post-quantum security models for authenticated encryption", V. Soukharev, D. Jao and S. Seshadri.

[i.201] Theoretical Computer Science, vol. 510, no. 50, pp. 5285-5297 (2009): "Claw finding algorithms using quantum walk", S. Tani.

3 Abbreviations

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

BLISS	Bimodal Lattice Signature Schemes
BQP	Bounded error Quantum Polynomial time
CVP	Close Vector Problem
ECDH	Elliptic Curve Diffie-Hellman protocol
HFE	Hidden Field Equation
HIMMO	Hiding Information and Mixing Modular Operations
IACR	International Association for Cryptologic Research
ISG	Industry Specification Group
LRPC	Low Rank Parity Check
LWE	Learning With Errors
MDPC	Medium Density Parity Check
MQ	Multivariate Quadratic
NIST	National Institute of Standards and Technology
PQC	Post-Quantum Cryptography
PRNG	Pseudo-Random Number Generator
QC	Quasi-Cyclic
QKD	Quantum Key Distribution
QSC	Quantum-Safe Cryptography
QUAD	Quadratic stream cipher
RSA	Rivest Shamir Adleman protocol
SFLASH	Super fast multivariate signature algorithm
SIS	Short Integer Solution
SIVP	Short Independent Vector Problem
SVP	Short Vector Problem
TLS	Transport Layer Security
XOR	Exclusive OR
ZHFE	Zhuang-zi Hidden Field Equations

4 Primitives under consideration

4.1 Introduction

The present document considers a list of quantum-safe public key primitives which have been proposed for use in key establishment or authentication schemes. It is not comprehensive and does not list every quantum-safe cryptography (QSC) primitive that has ever been proposed. Instead, it identifies a representative selection (as of May 2016) of cryptographic primitives that have credibility in academia, are supported by currently-active research teams, may be practical for real-world applications and hence are suitable candidates for consideration by ETSI for standardization.

The references given are intended to provide useful starting points for the best and most current configurations, security analyses and parameter sizes. The claims and recommendations found in the references will need to be independently verified at a later stage once the initial list of candidates has been narrowed to a more manageable size.

NOTE: Narrowing the list of candidate primitives is out of scope of the present document, however clause 12 provides some preliminary conclusions and subsequent documents will give more detailed assessments of the most promising proposals.

4.2 Primitive families

The quantum-safe primitives under consideration all come from the following five families:

- Lattice-based primitives where the security depends on the difficulty of solving a short or close vector problem in a lattice.
- Multivariate primitives where the security depends on the difficulty of solving a system of multivariate polynomial equations.
- Code-based primitives where the security depends on the difficulty of solving a decoding problem in a linear code.
- Hash-based primitives where the security depends on the difficulty of finding collisions or preimages in cryptographic hash functions.
- Isogeny-based key primitives where the security depends on the difficulty of finding an unknown isogeny between a pair of supersingular elliptic curves.

4.3 Primitive types

It is possible to further categorize the key establishment and authentication primitives within each family. The key establishment primitives are mostly either:

- key agreement primitives where two parties securely generate a shared symmetric key from information contributed by both parties; for example, by exchanging public keys with each other; or
- key transport primitives where one party generates a symmetric key and securely shares it with a second party; for example, by sending it encrypted under the second party's public key.

Similarly, the authentication primitives are mostly either:

- Fiat-Shamir signature schemes which are constructed from interactive proof-of-knowledge protocols; or
- hash-and-sign signature schemes which are constructed from trapdoor one-way functions.

NOTE: This overview will not consider cryptographic primitives with more advanced functionality such as identity-based encryption or group signatures.

4.4 Application-specific or restricted-use cases

In addition to recommending one or more general-purpose primitives for key establishment and authentication applications, it may be necessary to identify and recommend primitives that are particularly well suited for application-specific use cases; for example, for constrained environments or to provide very short signatures. There will also be systems which are not affected by constraints on packet or handshake sizes that are imposed by some current communications protocols or interoperability requirements.

4.5 Other mechanisms

Although the present document will mainly focus on public-key primitives, it is important to note that it is possible to achieve quantum resistance via a range of other mechanisms. For example, authentication schemes such as MACs [i.5], Wegman-Carter [i.6], and Kerberos [i.7] can be built from block ciphers or hash functions and the stream cipher QUAD [i.8] is based on multivariate quadratic equations. Quantum key distribution (QKD) has also been proposed for generating symmetric keys or one time pad [i.1]. By far the most impressive existing quantum-safe system is the global 3GPP mobile network which achieves authentication via pre-shared keys embedded in SIMs at manufacture, and key agreement and message integrity via a complex set of symmetric protocols, see e.g. [i.9]. There are many other large systems that could be configured to rely on pre-shared keys or with key distribution centres, for example Transport Layer Security (TLS) [i.10] and the ZigBee® wireless mesh network for IoT applications [i.11], as well as protocols HIMMO (see clauses 6.3.3.1 and 6.4.3.1) and Kerberos.

NOTE: There will be more discussion of these mechanisms in other ETSI ISG QSC documents.

5 Assessment framework

5.1 Introduction

ETSI ISG QSC will assess candidate cryptographic primitives for suitability against the criteria below, organized under the headings of security, efficiency and deployment considerations. The following clauses of the present document will go into more detail on the security considerations, while the efficiency and deployment criteria will be covered in more detail in other documents.

5.2 Assessment criteria

5.2.1 Security

Relevant criteria under this heading would include considerations such as:

- Amount of public scrutiny and level of acceptance by the academic community.
- Confidence in the associated security proof or reduction to a hard problem by the academic community and relevance of the security model.
- Attacks that have been proposed against the primitive or underlying hard problem.
- Suitability for use in a forward secure key establishment protocol.
- Potential to provide or enable multiple security features (e.g. associated key establishment and authentication schemes).
- Ease of quantifying the claimed classical and quantum security levels.
- Certainty of the recommended key sizes for a given level of security (e.g. 80-bits, 112-bits, 128-bits or 256-bits).

NOTE: The present document will not cover side-channel attacks or any other implementation-specific considerations.

5.2.2 Efficiency

Relevant criteria under this heading would include considerations such as:

- Recommended parameter sizes for a given level of security.
- Speed and number of round trips required to establish a key or sign and verify on a representative set of platforms or processors.
- Speed of key generation and time required to distribute a new key.
- Other practical considerations such as the failure rate for key-establishment or the maximum number of signatures.

NOTE: These criteria will be covered in more detail in other ETSI ISG QSC documents.

5.2.3 Implementation and deployment issues

Relevant criteria under this heading would include considerations such as:

- Ease of implementation by non-experts.
- Size of implementation (particularly relevant to FPGAs and embedded devices).
- Memory requirements during execution (especially on resource-limited devices).
- Practicality of key and signature sizes for transmission or storage across a range of platforms, including resource-limited devices.
- Ease of integration into existing protocols or systems (e.g. is this drop-in replacement?).
- Cost of changing or upgrading.
- Re-use of code base (e.g. to provide authentication as well as key establishment).
- Interoperability considerations (e.g. flexibility in the choice of hash function in Merkle tree schemes).

NOTE: These criteria will be covered in more detail in other ETSI ISG QSC documents.

5.3 Security considerations

5.3.1 Classical security

Before a primitive can be considered quantum-safe, it should first be secure against classical attacks. Indeed, most primitives will have received substantially more classical cryptanalysis than quantum cryptanalysis. Confidence in the security of a quantum-safe primitive will therefore be largely based on the more detailed classical analysis together with a general assessment of how quantum computers might affect this.

Moreover, most of the parameters recommended in the various proposals are actually aimed against classical rather than quantum adversaries. The recommended key sizes against classical attackers are often based on assessing the best known attacks via various practical "crypto-challenges", see e.g. [i.12], [i.13] and [i.14].

5.3.2 Quantum security

It is not possible to give definitive work estimates for quantum attacks at this point in time, since it is not yet clear what a large scale future quantum computer will look like, which technologies it will be based on, or how to quantify the auxiliary resource requirements for things such as fault tolerance, error correction and memory look-ups. However for some primitives it does seem possible to give some reasonable "rules of thumb" based on the properties of the algorithms that will be run on a quantum computer.

Grover's algorithm provides a "square-root speed up" over a classical adversary when searching unstructured data sets, and this square root speed-up is known to be the best possible for unstructured search by quantum computers. In the context of cryptography this means that for a generic block cipher to maintain a given level of security (e.g. 128 bits) against a quantum adversary running Grover's algorithm to recover a key, the rule of thumb should be to "double the key size" (e.g. to 256 bits).

However it is important to note that Grover's algorithm is a "query" algorithm, meaning that computational cost is measured in queries to the data set instead of more basic operations such as AND, XOR, etc. In cryptographic applications, each individual query in Grover's algorithm typically corresponds to performing one encryption of the block cipher, which is typically equivalent to several thousand basic operations (AND, XOR, etc.) on a classical computer. Clearly, this measure of computational cost of Grover's algorithm is an underestimate of the true computational cost, and it is not yet understood what the true measure on a quantum computer should be.

Similarly, proofs of the optimality of Grover's algorithm also measure computational cost in queries to the data set. Thus, the "square root" rule of thumb should not be viewed as providing a precise cost analysis for running Grover's algorithm but rather as a very conservative estimate of the resources required for the attack.

Further, unlike classical exhaustion, Grover's algorithm does not parallelise efficiently. To halve the time taken by Grover's algorithm it is necessary to quadruple the number of quantum computers running in parallel.

NOTE: The rules of thumb described in clauses 6.5, 7.5, 8.5, 9.4 and 10.5 are intended only as a guide as to how quantum algorithms may affect parameter sizes and are not replacements for detailed quantum cryptanalysis. In particular, they should be not be used to set parameters for quantum-safe primitives if suitable parameters have not already been proposed in the literature.

5.3.3 Provable security

Security reductions can give confidence that the security of a scheme is based on a problem that is known to be hard. However, it is important to understand the precise security guarantees given by the reduction. In many cases it is unwise to derive parameter sizes directly from the provable security level [i.15]. In some cases it may be better to ignore the reduction if it allows a more efficient scheme, provided that it is possible to be sure that the practical security is not compromised. The question of how to extend classical security reduction techniques to quantum adversaries is a new topic of research [i.16].

5.3.4 Forward security

A key establishment protocol is forward secure if the compromise of a long-term private key does not affect the security of previously established symmetric keys. It is usually considered important for modern security protocols to provide forward security [i.17], particularly for widespread or general purpose applications. For example, the draft specification for TLS 1.3 [i.18] only supports forward secure cipher suites. Consequently, it will be necessary to identify quantum-safe key establishment primitives that are suitable for use in such protocols. As forward security generally involves ephemeral keys, this means that the quantum-safe primitives need to have efficient key generation and small public keys.

5.3.5 Active security

It is also important to consider security against active adversaries since quantum-safe primitives that are only passively secure could be weak when used in certain protocols [i.19]. This should not be a concern for most authentication primitives as the standard security notion for signatures is existential unforgeability against adaptively-chosen message attacks. However, there is a much wider range of security notions for key establishment primitives so it is necessary to understand their security against adaptively-chosen plaintext and ciphertext attacks. For example, malleable primitives can reveal information about a shared symmetric key (e.g. Bleichenbacher's padding attack against RSA [i.20]) and key establishment failures can reveal information about a static private key (e.g. invalid point attacks against ECDH [i.21]).

6 Lattice-based primitives

6.1 Introduction

A good introduction to lattice-based cryptography is [i.22]. This is a very active research field with several active research groups, dedicated conferences and more than 100 papers on the International Association for Cryptologic Research (IACR) ePrint server over the past two years.

The best generic attacks against key establishment are based around lattice reduction algorithms, such as LLL and BKZ, or lattice sieving, which are also active areas of research and supported by challenge problems such as [i.12].

Early proposals for lattice-based signatures such as GGHSign [i.23] and NTRUSign [i.24] suffered from private information leakage: each transcript revealed a point in the fundamental domain of the private basis for the lattice. By obtaining enough signature samples, an attacker was able to recover the parallelepiped for the underlying private basis and therefore break the signature scheme [i.25] and [i.26]. More recent schemes use rejection sampling to provide transcript security. Instead of outputting a signature directly, the signing algorithms modify the distribution of the signatures so that they follow a known distribution that is independent of the private key. This ensures that each transcript does not leak any information about the private key as any valid private key could potentially have produced that signature.

Resistance against quantum attacks has been specifically addressed in [i.27].

6.2 Provable security

The security of lattice-based key establishment and authentication primitives is based on the difficulty of solving lattice problems such as the Short Vector Problem (SVP) or the Closest Vector Problem (CVP) and their approximate versions.

The approximate SVP, and the related approximate Short Independent Vector Problem (SIVP), is known to be NP-hard in general lattices for small approximation factors, and easy for approximation factors that are exponential in the lattice dimension. For cryptographic purposes, an approximation factor that is polynomial in the lattice dimension is used. For these approximation factors, there is evidence that SIVP is *not* NP-hard. However, lattice problems have been intensively studied, only resulting in polynomial-time algorithms such as LLL for slightly subexponential approximation factors, or exponential-time and -space algorithms such as BKW for polynomial approximation factors.

Figure 1 (based on information from [i.28]) visualizes the above hardness results on SIVP.

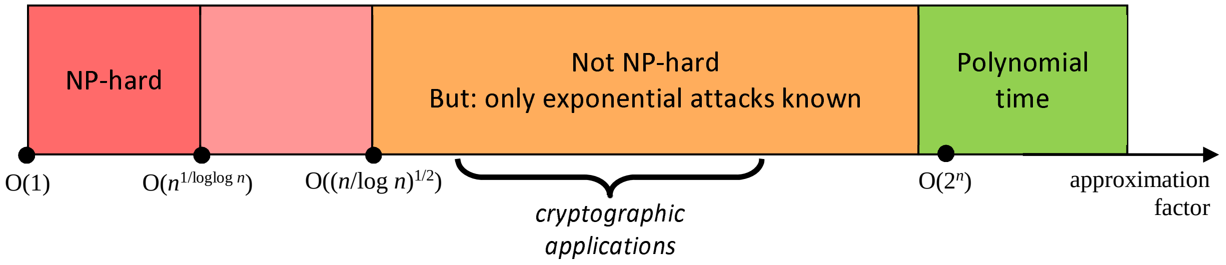

Figure 1: Complexity of the approximate short independent vector problem

Cryptosystems instantiated with generic lattices usually do not have the best performance due to the necessity of having to specify the lattice basis by a large matrix. In practice, lattice-based primitives often use ideal lattices [i.29], a class of structured, cyclic lattices where the lattice basis can be specified by a single vector or polynomial. Common problems that use ideal lattices are the Ring-Learning with Errors (Ring-LWE) problem [i.30] and the Ring-Short Integer Solution (Ring-SIS) problem.

One of the advantages of lattice-based cryptography is the existence of worst-case to average-case reductions. It is known that certain cryptographic problems such as Learning with Errors (LWE) and Short Integer Solutions (SIS) are as hard on average as certain lattice problems such as SVP and SIVP are in the worst case. In other words, if hard instances of SVP or SIVP exist at all then a random instance of LWE or SIS is hard with overwhelming probability [i.31]. Using this result, one can design cryptographic primitives and prove that any random instance of the cryptographic problem is as hard to break as the most difficult instance of the related lattice problem. Cryptographic schemes based on LWE or SIS typically have worst-case to average-case reductions.

The most important open problem for ideal lattices is whether the additional algebraic structure of ideals and modules over rings opens the door to any new kind of attacks on the relevant lattice problems. Research on exploiting the structure in special cases of ideal lattices is ongoing [i.32], [i.33] and [i.34].

6.3 Key establishment

6.3.1 Key agreement primitives

6.3.1.1 Peikert

Peikert [i.35] has described a state-of-the-art proposal for a general purpose key agreement based on Ring-LWE. It offers a worst-case to average-case security reduction, actively secure and authenticated modes, and forward security. The implementation in [i.36] gives suggested parameters for 128-bits of classical security and 80-bits of quantum security while references [i.37] and [i.38] include parameters for a range of classical and quantum security levels. A recent paper by Alkim et al [i.39] describes further optimizations for the unauthenticated key exchange and gives associated parameters for 128-bits of quantum security.

6.3.1.2 Zhang et al

Zhang et al [i.40] have described a promising idea for an efficient two-way authenticated key agreement scheme. It is presented as either a one-pass or a two-pass protocol and the two-pass version comes with a security reduction from Ring-LWE. The proposal is not as thoroughly worked out as Peikert or NTRUEncrypt and the two-pass protocol can only offer weak forward security. The parameters given are at the 140/160-bit and 350/360-bit security levels for the one-pass version and the 75/80-bit and 210/230-bit security levels for the two-pass version.

6.3.1.3 Ghosh-Kate

Ghosh-Kate [i.41] have described a hybrid one-way authenticated one-way anonymous key agreement designed for use in Tor. It combines a static-ephemeral ECDH key agreement with an ephemeral-ephemeral Ring-LWE key exchange. Authentication is provided by the non-quantum-safe exchange and forward security by the quantum-safe exchange. This means that there are a number of different security reductions to either the Diffie-Hellman or Ring-LWE problems depending on the type of adversary assumed. They give a single parameter set that they claim offers "high security", but since it involves a 256-bit elliptic curve it is at most 128-bits.

6.3.2 Key transport primitives

6.3.2.1 NTRUEncrypt

NTRUEncrypt [i.42] is a well-established scheme with very good efficiency properties. The NTRU lattice is a special type of ideal lattice with additional structure to further improve the efficiency. Problems over NTRU lattices are believed to be hard in practice and it is well regarded after receiving many years of public scrutiny. However, it lacks the worst-case to average-case security reductions of more modern Ring-LWE schemes. There is a variant of NTRUEncrypt that has been proven secure assuming the hardness of Ring-LWE [i.43], but this not particularly efficient.

Older versions of NTRUEncrypt are specified in [i.44], [i.45] and [i.46] suggests updated parameters for the 128-bits, 192-bits and 256-bit security levels. Recent theoretical papers giving the first subexponential algorithm for recovering NTRUEncrypt private keys [i.47] and proposing new quantum attacks [i.48] led to the parameters being updated once again in [i.49]. The best known attack in practice against NTRUEncrypt remains the hybrid attack from Howgrave-Graham [i.50] in 2007.

6.3.3 Other key establishment primitives

6.3.3.1 HIMMO

HIMMO [i.51] is an interesting new key pre-distribution scheme with good efficiency properties that can enable both key establishment and authentication in one-way communications settings. Although there is no formal security reduction, the authors argued that the main attacks against HIMMO appeared to lead to two related lattice sub-problems. [i.51] included provisional parameters, which were subject to revision by a crypto challenge on the website [i.13]. Almost all of the HIMMO challenge problems were solved following the discovery of an attack which finds an approximate solution to one of the lattice sub-problems. An updated HIMMO is described in [i.52] which rebalances parameters following the new attack and new challenge problems have been published on the website.

The underlying security mechanisms for HIMMO are new and would benefit from more academic scrutiny. [i.53] explicitly considers the quantum security of HIMMO.

6.3.4 Forward security

Lattice-based primitives have fast key generation and, when used with ideal lattices, small public keys. In particular, NTRUEncrypt and Peikert's key encapsulation mechanism could both be used in forward secure protocols. The authenticated key exchanges by Zhang et al and Ghosh-Kate are two-pass protocols so can only provide forward security against passive attackers [i.54]. Although HIMMO operates as a static-static key exchange and so would not be able to provide forward security by itself, it could be incorporated into an architecture where forward security is still feasible [i.55].

6.3.5 Active security

Lattice-based encryption schemes are naturally malleable which makes them good candidates for homomorphic encryption. Further, lattice-based key establishment primitives can be vulnerable when used with static keys [i.56]. For example, decryption failures in NTRUEncrypt lead to a key-recovery attack [i.57] so it needs to be used with a plaintext-aware padding scheme that blocks these [i.58]. Similarly, key exchange failures in Peikert's key encapsulation mechanism mean that for active security it needs to incorporate a key validation step [i.35].

The Ghosh-Kate and Zhang et al authenticated key agreements are shown to be secure against certain types of active attacker, but they may not block all active attacks. For example, the generic attacks against two-pass protocols will still apply [i.54]. As HIMMO operates as a static-static key exchange there is likely to be very little scope for active attacks.

6.4 Authentication

6.4.1 Fiat-Shamir signatures

6.4.1.1 Lyubashevsky

Lyubashevsky's Fiat-Shamir signature proposed in [i.59] was the first to introduce the now widespread technique of rejection sampling to remove information leakage from the signatures. This was updated in [i.60] to produce a more efficient signature with a security reduction from Ring-LWE rather than Ring-SIS. Dagdelen et al [i.61] also show that, with minor modifications, the signature is secure in the quantum random-oracle model. The EUROCRYPT paper [i.60] contains parameters for a fixed, but unspecified, security level and could be used to construct others.

6.4.1.2 Güneysu-Lyubashevsky-Pöppelmann

Güneysu-Lyubashevsky-Pöppelmann [i.62] described a version of Lyubashevky's Fiat-Shamir signature [i.60] with bounded uniform distributions. This simplifies the implementation but increases signature length and means that the security reduction is from a non-standard version of the decision Ring-LWE problem. The paper [i.62] includes parameters which they claim provide 100-bits and 256-bits of security, but Ducas et al [i.63] lower the estimate of the smaller parameters to around 80-bits.

Bai-Galbraith [i.64] were able to decrease the signature sizes using a better compression technique while retaining a security reduction from either the LWE or SIS problem. They proposed a variety of parameters for 128-bits of classical security. A more recent variant by Akleylek et al [i.65] achieves signature lengths comparable to the best hash-and-sign signatures and has a tight reduction from Ring-LWE. Reference [i.65] includes parameters for 80-bits and 128-bits of classical security.

6.4.1.3 BLISS

BLISS [i.63] is a Fiat-Shamir signature which uses bimodal Gaussian distributions and a modified rejection sampling process to reduce the signature size. The unusual construction needs more analysis and the security reduction is from the NTRU problem rather than standard Ring-SIS. Nevertheless, BLISS is the most widely cited of the recent lattice-based signature proposals. Reference [i.63] suggests 128-bits, 160-bits and 192-bit secure parameters.

BLISS-B [i.66] is a variant of BLISS which uses the same parameters, but has improved key generation and signing times. However, [i.67] notes that the quantum security of the scheme is reduced by the size of the output of the hash function and so adjusts the recommended parameters. Further, [i.67] introduces BLZZRD, a variant of BLISS-B which includes side-channel protection to block attacks such as [i.68].

6.4.2 Hash-and-sign signatures

6.4.2.1 NTRU-MLS

NTRU-MLS [i.69] is the most recent signature proposal from the designers of NTRUSign. It incorporates a form of rejection sampling and has a proof that the signatures do not leak information, but there is no formal security reduction and it has not had any published independent analysis. Reference [i.69] suggests parameters for the 112-bits, 128-bits, 192-bits and 256-bit security levels.

6.4.2.2 Aguilar et al

Aguilar et al [i.70] proposed a hash-and-sign signature which applies Lyubashevsky's rejection sampling directly to NTRUSign. It has a security reduction from Ring-SIS and provides suggested parameters for 100-bits, 128-bits and 160-bits of security.

6.4.2.3 Ducas-Lyubashevsky-Prest

The hash-and-sign signature from Ducas-Lyubashevsky-Prest [i.71] is presented as the key extraction step for an identity-based encryption scheme. It is a variant of NTRUSign which adjusts the distributions used during the signing process to avoid information leakage rather than using straightforward rejection sampling. It achieves very short signatures, but has had almost no independent analysis and does not come with a security reduction. They propose parameters for 80-bits and 192-bits of security.

6.4.3 Other authentication primitives

6.4.3.1 HIMMO

Key pre-distribution schemes based on identities such as HIMMO [i.51] and [i.52] can also provide authentication. Once a pairwise key has been established based on the keying material and identities, the peers can run a simple challenge-response mutual authentication handshake to verify that their computed key is equal, which authenticates their identities at the same time. Further extensions to the basic authentication handshake can enable credential verification and source authentication. For example, [i.55] describes an application of this method to verify public keys in a hybrid quantum-safe TLS handshake with minimal overhead.

6.5 Quantum security

The first connection between quantum computation and a lattice problem - the O(n5/2)-unique short vector problem - was described in [i.72] and the first quantum attack on a lattice-based cryptographic primitive was described in [i.32]. However, these both addressed somewhat special cases. So far, there are no generic quantum algorithms that perform significantly better than classical algorithms. This is despite the fact that lattice problems seem a natural candidate to attempt to solve using quantum algorithms; because of their periodic structure and because the Fourier transform, which is usually exploited in quantum algorithms, is tightly related to lattice duality. Attempts at attacking lattice problems using Shor-like techniques have failed so far.

The best reference for quantum approaches to solving general short vector problems appears in [i.27] where the authors describe several algorithms which combine lattice sieving with Grover's algorithm. In general, they were able to reduce the log-complexity of the lattice sieves by up to a quarter. The rough rule of thumb, at least for Ring-LWE distinguishing attacks using block reduction algorithms (see, for example, table 2 from [i.73]), is that parameter sizes scale linearly in the size of the block required to distinguish. This means that since quantum lattice sieves theoretically allow the size of the block to increase by a third for essentially the same cost then, to retain a given level of security, a Ring-LWE scheme may also need to increase the size of its public key by a third.

NTRU-based schemes are slightly more complicated as it depends on whether Grover's algorithm speeds up the meet-in-the-middle section of a hybrid lattice attack. If only quantum improvements to the lattice reduction are considered then a similar rule of thumb applies. Quantum speed-ups against HIMMO were explicitly considered in [i.53].

7 Multivariate schemes

7.1 Introduction

A good reference for multivariate cryptography is [i.74]. This is an active research field with multiple active research groups and dozens of conference presentations and IACR ePrints over the past two years.

The best known generic attacks on multivariate schemes are MinRank [i.75], Gröbner basis techniques [i.76], [i.77], [i.78] or linearization [i.79]. Simulations for small parameter sizes [i.80] suggest that the complexity of these attacks grows exponentially in the parameter size. This is still an active area of research and is supported by challenge problems [i.14].

There seems to have been a decline in confidence in the ability of multivariate systems to provide a secure key establishment after a series of earlier proposed schemes were broken, e.g. [i.81], [i.75], [i.82], [i.83] and [i.84]. However, there is slightly more acceptance of multivariate signatures despite the devastating attack against the NESSIE-selected signature SFLASH [i.85].

Resistance against quantum attacks does not appear to have been specifically addressed in the literature.

7.2 Provable security

Multivariate cryptosystems are based on the hardness of solving a non-linear system of multivariate polynomial equations. This problem is known to be NP-hard [i.86] and remains so even if it is restricted to a system of multivariate quadratic (MQ) equations.

The hardness of MQ depends on the ratio between the number of variables n and the number of equations m. For a random system of equations, MQ is exponential when m = O(n) [i.87] and [i.88], but it becomes polynomial when the system is heavily overdetermined (i.e. when m = O(n^2)) [i.89], [i.90] or heavily underdetermined (i.e. when n = O(m^2)) [i.91]. In between, a gradual transition occurs from exponential to polynomial complexity [i.89] and [i.92]. For example, the complexity of solving a system of quadratic equations over GF(2) is sub-exponential when m/n tends to infinity and m/n2 tends to zero [i.90]. Generally, MQ encryption schemes use an overdetermined system of equations, so $n < m < n^2$, while MQ signature schemes use an underdetermined system, so $m < n < m^2$.

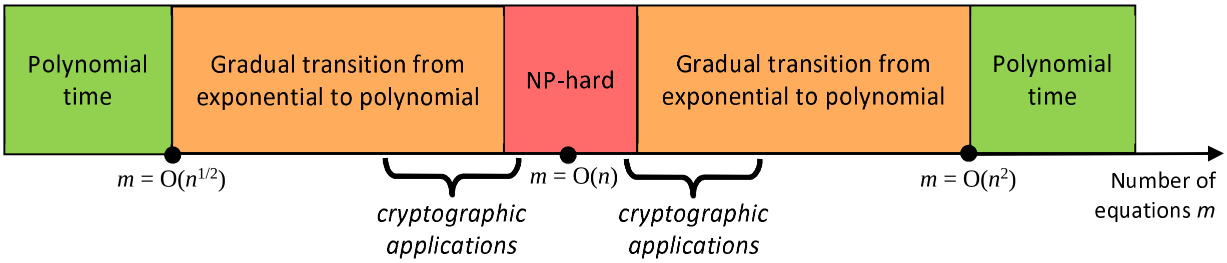
Polynomial time
Gradual transition from exponential to polynomial
NP-hard
Gradual transition from exponential to polynomial
Polynomial time
m = O($n^{1/2}$)
m = O(n)
m = O(n^2)
cryptographic applications
cryptographic applications
Number of equations m

Figure 2: Complexity of the multivariate quadratic problem

Almost no multivariate schemes come with worst-case to average-case reductions and very few have full security reductions from the generic NP-hard problem. More usually, there are reductions from the problem of solving the specific type of non-random trapdoor system used in the public key [i.93] or under restricted attack models [i.94].

Consequently, the security of most multivariate schemes is dependent on estimates of the computational difficulty of solving the public systems using the best known practical attacks.

7.3 Key establishment

7.3.1 Key transport primitives

7.3.1.1 Simple Matrix

Simple Matrix [i.95] is a recent proposal for a multivariate encryption scheme where the public system is constructed from products of square polynomial matrices. Analysis in [i.96] outlined a structural attack against the scheme and highlighted an issue with the decryption failure rate. The updated rectangular version [i.97] avoids the structural attack and reduces the probability of decryption failure. Unfortunately, another attempt to eliminate decryption failures completely [i.98] was shown to be flawed [i.99]. Reference [i.97] includes suggested parameters for 80-bits, 90-bits and 100-bits of security.

7.3.1.2 HFE

Hidden Field Equation (HFE) encryption schemes were proposed in 1996 by Patarin [i.100]. These construct a public multivariate system from a hidden univariate polynomial over a field extension. There is a long history of cryptanalysis of HFE schemes which includes message-recovery attacks using Gröbner basis techniques [i.101], [i.102] and key-recovery attacks via MinRank [i.75]. Although the initial proposals were broken, the most powerful attacks are exponential in the degree of the hidden polynomial so it is possible to choose parameters for which HFE is secure. Unfortunately, these parameters also lead to unacceptably slow decryption times.

There have been a number of different proposals for increasing the security of HFE such as dropping equations (HFE-) or adding vinegar variables (HFEv). In particular, it has recently been suggested that HFE- encryption schemes could offer an improved balance between security and efficiency [i.103]. However, full details of the HFEBoost scheme mentioned in [i.103] have not yet been released.

7.3.1.3 ZHFE

ZHFE [i.104] is a new idea for an encryption scheme which uses a pair of high-degree HFE polynomials in a way that still allows for efficient decryption. Although the authors of [i.104] argue that the scheme is secure against MinRank and direct algebraic attacks, [i.105] and [i.106] highlight an issue with key generation that can lead to ZHFE systems with lower rank than anticipated. In [i.105], Perlner and Smith-Tone suggest a modification for key generation to avoid this and give a variant, ZHFE-, which has slightly smaller key sizes. Reference [i.105] includes recommended parameters for 80-bits of security. Additionally, [i.106] describes a much more efficient key generation process which significantly reduces both the time and memory required to construct a key pair.

Extension field cancellation [i.107] is a related approach which uses a construction involving elements of the extension field to obtain the low-degree relation necessary for decryption. This offers better performance than ZHFE, but more study is require to be confident in its security.

7.3.1.4 Polly Cracker Revisited

Polly Cracker Revisited is a homomorphic encryption scheme proposed in [i.108] and [i.109]. Although it is presented as a symmetric algorithm, the authors describe a generic technique to convert it into a public-key algorithm. There is a security reduction to the problem of finding a Gröbner basis for an ideal given noisy samples from the ideal. Further, the underlying hard problem admits an average-case-to-worst-case reduction for certain choices of parameters including those recommended in [i.109]. However, the parameters proposed are intended for homomorphic applications so lead to large key sizes. More work would be required to identify practical parameters for simple encryption.

7.3.2 Forward security

The public keys for multivariate encryption schemes are large and key generation can be slow. This means that they would not be suitable for use in a forward secure protocol.

7.3.3 Active security

None of the multivariate key establishment primitives have been analysed in terms of their active security. Polly Cracker Revisited is a homorphic encryption scheme so is designed to be malleable. There are various generic ways that the security of the Simple Matrix, HFE- or ZHFE schemes can be reduced if it has not been suitably protected. For example, if a plaintext is partially known then the corresponding variables can be eliminated from the public multivariate system. Alternatively, if the same plaintext is encrypted under different public keys then this can be used to increase the number of equations in the multivariate system that needs to be solved.

Further, the Simple Matrix encryption scheme has a relatively high probability of decryption failure so more study is required to understand if this reveals any information about the private key. Consequently, multivariate encryption schemes should be used with a padding scheme such as [i.110] that can prevent these issues.

7.4 Authentication

7.4.1 Fiat-Shamir signatures

7.4.1.1 Sakumoto-Shirai-Hiwatari

Sakumoto-Shirai-Hiwatari [i.111] propose 3- and 5-pass identification schemes whose security is provably reducible to the MQ problem for random quadratic systems. The Fiat-Shamir transform can be used convert a parallel version of the 3-pass identification protocol into a signature scheme which also has a security reduction to the MQ problem. The public system can be generated pseudo-randomly from a small seed, but the communication cost for the identification scheme is relatively high so the signatures will be substantially longer than the multivariate hash-and-sign signature schemes. Reference [i.111] includes parameters for 80-bits of security.

7.4.2 Hash-and-sign signatures

7.4.2.1 Quartz

Quartz [i.112] is a multivariate signature scheme based on HFEs with both vinegar variables and dropped equations (HFEv-). This has exceptionally short signatures, but long signature generation times. There is a security reduction [i.93] for HFEv- signatures from the problem of inverting the public system. The Quartz proposal included 80-bit secure parameters and, although initial analysis appeared to reduce this estimate [i.113], recent work [i.77] has confirmed their security.

7.4.2.2 Gui

Gui [i.114], [i.115] is a new proposal for an HFEv- signature which improves the efficiency of signature generation by lowering the rank of the hidden polynomial. The security of the scheme is assessed against MinRank and direct algebraic attacks in [i.115]. Differential attacks are considered in [i.116] and a method for checking for differential symmetries during key generation is described. The authors of [i.115] provide parameters for 80-bits and 128-bits of security.

7.4.2.3 UOV

UOV [i.117] is a multivariate signature scheme constructed using a step-wise triangular system. There is a security reduction [i.93] for UOV signatures from the problem of inverting the public system and this behaves like a random quadratic system under a certain class of direct algebraic attacks [i.94]. However, improved approaches to solving underdetermined quadratic systems [i.78] [i.92] have lowered the security estimate of the original parameters. Newer parameters with 80-bits, 100-bits, 128-bits, 192-bits and 256-bits of security can be found in [i.118].

7.4.2.4 Rainbow

Rainbow [i.119] is a layered version of the UOV signature for faster signature generation and has a cyclic variant [i.120] for smaller public key sizes. There is no formal security reduction and a series of attacks [i.121], [i.122], [i.123] have exploited the additional structure provided by the layers. In particular, [i.123] appears to lower the security estimates for the larger-field parameters in [i.80] and may also apply to some of the more recent parameters suggested in [i.118].

7.5 Quantum security

The class of decision problems that can be deterministically solved in polynomial-time by a quantum computer with probability at least 1/3 is called BQP. It is suspected that there are no NP-complete problems in BQP which means that no polynomial-time quantum algorithms exist to solve MQ problems. Indeed, there seems to be no obvious way to apply Shor's algorithm and the general analysis in [i.124] implies that Grover's algorithm is essentially optimal for random MQ systems with $m = O(n)$.

In general, there does not seem to be a good rule of thumb for multivariate schemes. Applying Grover directly to invert the public system means that primitives that use small systems, such as the HFE- encryption scheme and HFEv- signature schemes, will need to double the number of polynomials and variables. This doubles the length of the ciphertext or signature, but increases the size of the public keys by a factor of 8 [i.115].

The situation for multivariate primitives that use large systems is less clear. It is possible to use Grover to obtain a square-root speed-up for some attacks such as MinRank. However, the security of at least the UOV and Rainbow signatures is determined by the cost of finding a collision in the hash function or attacking the system using Gröbner basis techniques, neither of which appears to be improved by quantum algorithms. More research is required and in the meantime the conservative approach is to assume that a square-root speed-up can be achieved. For both UOV and Rainbow this means doubling the length of the signature and increasing the size of the public keys by a factor of 8.

8 Code-based primitives

8.1 Introduction

Good references for code-based cryptography are the introduction to [i.125] and the survey [i.126]. This is an active research field supported by active research groups with a small but steady stream of presentations at conferences and papers on the IACR ePrint server.

The original McEliece encryption scheme, first proposed in 1978, and the more efficient Niederreiter scheme still look very secure when based on binary Goppa codes. However, the size of the public key has always been identified as a practical problem. Many ideas for reducing the size of the public keys by using different codes or structured public keys have been suggested, but most of these were broken via algebraic attacks [i.127], [i.128], [i.129], [i.130] and [i.131]. The best attacks on unstructured codes are based on information set decoding algorithms which have exponential complexity. These were first introduced by Leon [i.132] and Stern [i.133], and since then only gradual improvements have been made; for example: [i.134].

Resistance against quantum attacks has been specifically addressed in [i.135].

8.2 Provable security

Decoding *t* errors in a binary code is known to be NP-hard [i.136] and the decisional equivalent of this problem is NP-complete. However, the average-case complexity of decoding problems is only believed to be hard, not proven [i.137]. There exist codes for which decoding *t* errors is easy and these will result in weak instances of code-based cryptography.

Many code-based primitives require families of codes with efficient decoding algorithms. These codes have additional structure which needs to be hidden to prevent an adversary from also being able to decode efficiently. This means that any security reductions for these primitives would also need to involve indistinguishability results for the actual families of codes used and these may not always hold [i.138].

For example, binary Goppa codes have good error correction properties which make them good candidates for use in code-based primitives. Distinguishing a hidden Goppa code from a random code was long thought to be a difficult problem even though it was not proven to be NP-complete. However, the authors of [i.139] describe a polynomial-time distinguisher for high-rate Goppa codes. This distinguisher does not threaten the practical security of primitives that use binary Goppa codes, but it has been used to give a polynomial-time attack on primitives that use other families of codes such as wild Goppa codes over quadratic extensions [i.140].

On the other hand, distinguishing a medium density parity check (MDPC) code from a random code necessarily involves determining the existence of low weight codewords in its dual code.

8.3 Key establishment

8.3.1 Key transport primitives

8.3.1.1 McEliece and Niederreiter

The original McEliece [i.141] and Niederreiter [i.142] encryption schemes using binary Goppa codes are well established and trusted. They need to be transformed into semantically secure encryption schemes [i.143], but parameters have only been adjusted to account for gradual improvements to the information set decoding attack [i.133], [i.144], [i.145], [i.146] and [i.134]. [i.147] suggests parameters for up to 109-bits of security and reference [i.148] includes parameters at higher security levels.

8.3.1.2 Wild McEliece

Wild McEliece [i.149] and [i.150] was an initially promising proposal to reduce public key sizes by using wild Goppa codes. However, there is no security reduction and recent work [i.140] and [i.151] has begun to exploit the hidden algebraic structure. A range of parameters is suggested for the 128-bit security level.

8.3.1.3 MDPC McEliece

MDPC codes [i.125] are probably the best current proposal for reducing the size of the public keys used in McEliece. There is a security reduction from the decoding problem since distinguishing medium-density parity check codes from random requires the attacker to determine the existence of codewords of a given weight.

Although MDPC codes give larger public keys than binary Goppa codes, by reintroducing some structure and using quasi-cyclic (QC) codes it is possible to significantly reduce the key size. There is some evidence [i.152] that this additional structure also reduces the security of the scheme and [i.153] describes a class of weak keys so QC-MDPC McEliece could benefit from some additional academic scrutiny. Reference [i.125] suggests parameters for 80-bits, 128-bits and 256-bits of security.

8.3.1.4 LRPC McEliece

Low-rank parity check (LRPC) codes [i.154] are another interesting alternative to standard McEliece. The rank-metric decoding problem is NP-hard under a randomized reduction [i.155] and the authors of [i.154] claim that the security reduction for MDPC codes can be adapted to LRPC codes. However, the quasi-cyclic version suffers from a much more significant loss of security than QC-MDPC codes [i.156]. In general, LRPC codes require more academic scrutiny to understand how the attacks work under this new metric. Reference [i.157] provides updated parameters for 80-bits, 100-bits and 128-bits security levels.

8.3.2 Forward security

Key generation for code-based key establishment primitives can be fast, but the public keys are large when used with unstructured codes. This means that only the quasi-cyclic versions of MDPC McEliece or LRPC McEliece could be used in a forward secure protocol.

8.3.3 Active security

McEliece encryption is vulnerable to a variety of active attacks. For example, information set decoding can be significantly easier with partially known plaintexts or pairs of plaintexts with known linear relations. Further, by adding rows of the public matrix to a ciphertext an attacker can modify the plaintext in a predictable way. These properties mean that McEliece needs to be used with a semantically secure transformation such as [i.143].

In [i.154] it is also noted that decryption failures in LRPC McEliece can be prevented from leaking information by applying the Fujisaki-Okamoto transformation [i.158].

8.4 Authentication

8.4.1 Fiat-Shamir signatures

8.4.1.1 Cayrel et al

Cayrel et al [i.159] suggested an improvement of Stern's original code-based identification scheme [i.160] which can be converted into a signature scheme using a generalized Fiat-Shamir transform [i.161]. The scheme uses random q-ary codes to reduce the number of rounds required to achieve a given security level. It has a security reduction from the syndrome decoding problem and there is a quasi-cyclic version to reduce the size of the public keys. Signature generation is much more efficient than CFS (see below), although the signatures are significantly longer. [i.162] includes parameters for 80-bits and 143-bits secure signatures.

8.4.2 Hash-and-sign signatures

8.4.2.1 CFS

CFS [i.163] is a hash-and-sign signature based on the Niederreiter encryption scheme using binary Goppa codes. It achieves very small signature lengths, but the signature generation process is slow and it requires high-rate codes. This means that the public keys are large and the security reduction from the syndrome decoding problem given in [i.164] is invalidated by the high-rate Goppa code distinguisher from [i.139]. Parallel-CFS [i.165] is an updated version of the signature which blocks the decoding-one-out-of-many attacks [i.166] against the original. Reference [i.167] includes 80-bits and 120-bits secure parameters for Parallel-CFS.

8.4.2.2 RankSign

RankSign [i.168] is a hash-and-sign signature which is similar to CFS, but uses augmented LRPC codes to improve both signature generation times and public key sizes. The security reduction is from a non-standard approximate syndrome decoding problem which is assumed to be hard. There is also a cyclic version of RankSign which further decreases the size of the public keys. More analysis is required to gain confidence in the security of schemes based on LRPC codes. Reference [i.168] contains 90-bits, 120-bits and 130-bits secure parameters for cyclic-RankSign.

8.5 Quantum security

In [i.169] it is argued that although McEliece and Niederreiter reduce to a natural case of the hidden subgroup problem, they resist attacks based on strong Fourier sampling provided that they use Goppa codes which satisfy a mild restriction on the parameters. More precisely, [i.169] considers the hardness of the Goppa code distinguishing problem and there is a classical polynomial-time algorithm which solves this for high-rate codes [i.139]. However, Grover's algorithm can be used to give a quadratic speed-up for information set decoding [i.135].

The corresponding rule of thumb is that quantum algorithms halve the security level so to compensate the dimension of the code needs to doubled. For unstructured codes this corresponds to doubling the length of the ciphertext and quadrupling the size of the public key. On the other hand, for QC-MDPC codes this should only mean doubling the length of the ciphertext and public key although [i.135] does not specifically consider attacks against structured codes.

There is relatively little literature on attacking rank-metric systems [i.156] and it has already been noted above that these primitives would benefit from more academic assessment.

9 Hash-based primitives

9.1 Introduction

Although it does not cover the most recent proposals, a good reference for hash-based signatures is [i.170]. There has been a resurgence of interest in the field with a few active groups, several presentations at recent conferences and some early standardization work in the IETF [i.171] and [i.172].

The original Merkle signatures [i.173] and [i.174] are well understood and considered very secure, but potentially impractical due to the need to maintain state between signatures. Recent work has been focused on efficiency improvements and the issue of statefulness. For example, [i.175] discusses techniques for deploying stateful signatures which give some protection against state synchronization failures.

Quantum attacks are limited to using Grover's algorithm to speed up the search for hash-function preimages. The efficiency of using quantum computers to find hash-function collisions has been analysed in [i.176].

9.2 Provable security

The security of hash-based signatures depends on the security of the underlying hash function or hash function family. Many hash-based signature schemes have a security reduction from one or more of the standard properties for cryptographic hash functions: preimage resistance, second-preimage resistance, collision resistance and pseudo-randomness.

In some schemes a secure pseudo-random number generator (PRNG) is used to generate a large number of private values from a single seed. It seems most natural to use a hash-based PRNG whose security again depends on the preimage or collision resistance of the underlying hash function.

9.3 Authentication

9.3.1 Stateful signatures

9.3.1.1 Merkle

The original Merkle signature scheme [i.174] was proposed for standardization in the internet draft [i.177]. It has a security reduction in the random oracle model, [i.178] for the one-time signature together with [i.179] for the tree, from the collision resistance of the underlying hash function.

The draft RFC has recently been updated [i.171] to use the Leighton-Micali variant of the Merkle signature scheme. It has a security reduction in the random oracle model from the preimage resistance of the hash function [i.180]. Since it is harder to find preimages than collisions, this allows shorter signatures as the scheme is able to use smaller hash functions for the same security level. The draft RFC includes parameters for 128-bits and 256-bits of classical security.

In both schemes the number of messages that can be signed by a key pair is strictly limited by the number of one-time signatures available. The schemes are also stateful as the signer needs to keep a record of the number of messages that have been signed to avoid one-time signature reuse. These properties mean that the Merkle and Leighton-Micali signature schemes may not be suitable for all applications.

9.3.1.2 XMSS

XMSS [i.181], [i.182] is a newer hash-based signature which is still stateful, but uses tree chaining to increase the total number of signatures available. It has a tight security reduction in the standard model from the second-preimage resistance of the hash function family, although the precise reductions seem to differ between versions. Song [i.16] shows that this still holds against quantum adversaries.

Unfortunately, the version of XMSS initially proposed for standardization [i.183] was vulnerable to multi-target preimage attacks. The revised version [i.172] blocks the multi-target preimage attacks using a similar approach to Leighton-Micali. It also has a security reduction [i.184], but in this case it is in the random oracle model and involves some non-standard security notions for the hash function families. The current internet draft [i.172] includes parameters for 256-bits and 512-bits of classical security.

9.3.2 Stateless signatures

9.3.2.1 SPHINCS

SPHINCS [i.185] is a hash-based signature which avoids the need to retain state at the cost of significantly increasing the signature length and signing time. It includes a security reduction and an analysis of its security against quantum adversaries, but as it is built from the version of XMSS [i.183] that has been withdrawn more analysis is needed.

Further, SPHINCS is based on the non-standardized algorithms BLAKE and ChaCha12 so that better performance can be achieved. BLAKE was one of the finalists in the NIST SHA-3 hash function competition so has had a reasonable level of public scrutiny. While the ChaCha20 stream cipher has received some academic attention, ChaCha12 is a different variant of the same algorithm which might require additional analysis.

[i.185] includes parameters for 128-bits of quantum security.

9.4 Quantum security

The best quantum attacks for generic cryptographic hash algorithms come from versions of Grover's search algorithm.

A preimage for an *n*-bit output hash function can be found with $O(2^{n/2})$ iterations on a single quantum processor. This does not parallelise efficiently as finding the same preimage with 2^k quantum processor would require $O(2^{(n-k)/2})$ iterations. Nevertheless, the usual rule of thumb is that to retain the same level of preimage resistance the hash function output length needs to double. For signatures such as Leighton-Micali, XMSS or SPHINCS, whose security is based on the preimage resistance of the hash function, this doubles the public key size and quadruples the length of signatures.

Early estimates claimed that Grover would find collisions in an *n*-bit hash function with $O(2^{n/3})$ steps [i.186]. However, [i.176] notes that this requires a quantum computer of size $O(2^{n/3})$ which makes it less efficient than classical parallel collision finding algorithms [i.187]. This suggests that quantum algorithms do not pose a threat to the collision resistance of hash functions. For the original Merkle signature scheme, whose security is based on collision resistance, this means that it may not be necessary to increase the public key size or signature length to defend against quantum attacks.

10 Isogeny-based primitives

10.1 Introduction

A good general reference for isogenies and elliptic curves is [i.188]. This is a new research field with relatively few active research groups or publications.

The new isogeny-based primitives are interesting and have good properties such as small key sizes and forward security. They deserve more academic scrutiny to establish a consensus on their security properties, but are not supported by public challenge problems.

10.2 Provable security

The security of isogeny-based primitives depends on the difficulty of recovering an unknown isogeny between a pair of supersingular elliptic curves that are known to be isogenous. Isogeny-based key agreements have security reductions from Diffie-Hellman style problems in isogeny graphs. These reductions are special cases of a more general result [i.189] on semi-group actions. The underlying isogeny problems have not been proved to be difficult, but the classical [i.190] and [i.191] and quantum [i.192] and [i.193] complexity of recovering unknown isogenies between elliptic curves has been relatively well studied. In particular, for supersingular curves the best known algorithms are exponential unless the curves are both defined over a prime field.

10.3 Key establishment

10.3.1 Key agreement primitives

10.3.1.1 Jao-De Feo

Jao-De Feo [i.194] proposed a novel Diffie-Hellman style key-exchange using isogenies of supersingular curves. The extended paper [i.195] includes a more detailed security analysis, a reduction from a variant of the decision Diffie-Hellman problem for supersingular isogenies and improves the efficiency of a contribution of the original proposal. The code referred to in [i.194] contains suggested parameters for 128-bits, 192-bits and 256-bits of classical security with various choices of isogeny degrees.

Both [i.196] and [i.197] suggest methods for compressing the public keys and [i.197] describes an implementation which includes several performance improvements. [i.197] also gives recommended parameters for 128-bits of quantum security.

10.3.2 Forward security

The isogeny-based key agreement has small public keys and a reasonably efficient key generation process, although it is not as fast as some of the other primitives. It could therefore be used in a forward secure protocol.

10.3.3 Active security

The authors of [i.197] note that if one of the participants in the Jao-De Feo key agreement uses invalid public keys then they can force the shared secret to be independent of the other participant's private key. They propose a method of directly validating public keys which blocks such attacks, but suggest that static keys should be avoided due to the performance overhead of key validation.

10.4 Authentication

10.4.1 Other authentication primitives

10.4.1.1 Jao-Soukharev

Jao-Soukharev [i.198] proposed an undeniable signature scheme based on the supersingular isogeny key agreement from [i.194]. The signature length compares favourably to lattice-based signatures, but as it is an interactive protocol it will not be suitable for all applications. More security analysis is also required. Reference [i.198] includes parameters for 80-bits, 112-bits and 128-bits of quantum security. Reference [i.195] also includes a proposal for a zero-knowledge proof of identity.

10.4.1.2 Sun-Tian-Wang

Sun-Tian-Wang [i.199] propose a strong designated verifier signature scheme based on the supersingular isogeny key agreement from [i.194]. It is a non-interactive protocol, but only verifiers chosen in advance by the signer can verify the signature so again it will not be suitable for all applications. However, [i.200] describes an application of the signature to produce an authenticated encryption scheme with a security proof under the quantum random oracle model.

10.5 Quantum security

Biasse et al [i.193] describe a quantum algorithm for recovering an isogeny between two supersingular curves defined over a quadratic extension field. For the Jao-De Feo key agreement this is beaten by a quantum claw algorithm [i.201] which turns a fourth-root classical attack into a sixth-root quantum attack. To maintain the security level the rule of thumb should be to increase the size of the public keys by a half.

11 Key length summary

11.1 Introduction

It will eventually be necessary to recommend parameter sizes that will provide a required level of security (e.g. 80-bits, 112-bits, 128-bits and 256-bits) that is appropriate to the intended real-world use case. This is not entirely straightforward given the current level of understanding and confidence in the various methods proposed in academic papers.

Some primitives are well established but have relatively large key sizes (e.g. McEliece); newer primitives are much more efficient but less well analysed (e.g. Ring-LWE). Some primitives have formal security reductions to known hard problems (e.g. Ring-LWE and MQ); other primitives rely on the practical difficulty of key recovery or forgery attacks (e.g. NTRU and isogenies). Very few primitives have a reasonable rule of thumb for assessing their quantum security. This overview does not attempt to solve these problems, but notes them for future consideration, once the list of primitives has been narrowed down.

This clause gives an illustration of the key sizes for a subset of the primitives considered above. These are based on published parameters and are described in terms of their *classical* (n.b. not quantum) security level. Annex A contains a comparison of the suggested key sizes for all of the algorithms at the 128-bit classical security level wherever possible. Annex B gives estimated key sizes for all of the algorithms at the 128-bit quantum security level.

11.2 Key establishment

Figures 3 and 4 give the size of the public key and the length of the message for ten of the key establishment schemes. The message will either be the encrypted symmetric key for key transport schemes or the public key plus any additional fields for key agreements. In both figures the lengths are plotted on a *logarithmic* scale for clarity.

- The figures omit the Ghosh-Kate lattice-based key agreement as the parameters have no security estimates.
- For the multivariate key establishment schemes the figures omit HFE- as full details of the most recent proposal are not available and Polly Cracker Revisited as the public-key conversion is not completely specified.
- The figures include the quasi-variants of MDPC and LRPC McEliece, but omit their unstructured versions as they are significantly less efficient. Similarly, Wild McEliece has been omitted as it does not achieve the same reduction in key size as either QC-MDPC or QC-LRPC McEliece.
- HIMMO is included for completeness, however the quoted "public key" size for HIMMO corresponds to the length of the user's identifier and the "message" is the identifier plus the helper data used to establish a shared secret key. In general, large key sizes are of less concern in key pre-distribution schemes than in asymmetric key agreement schemes.

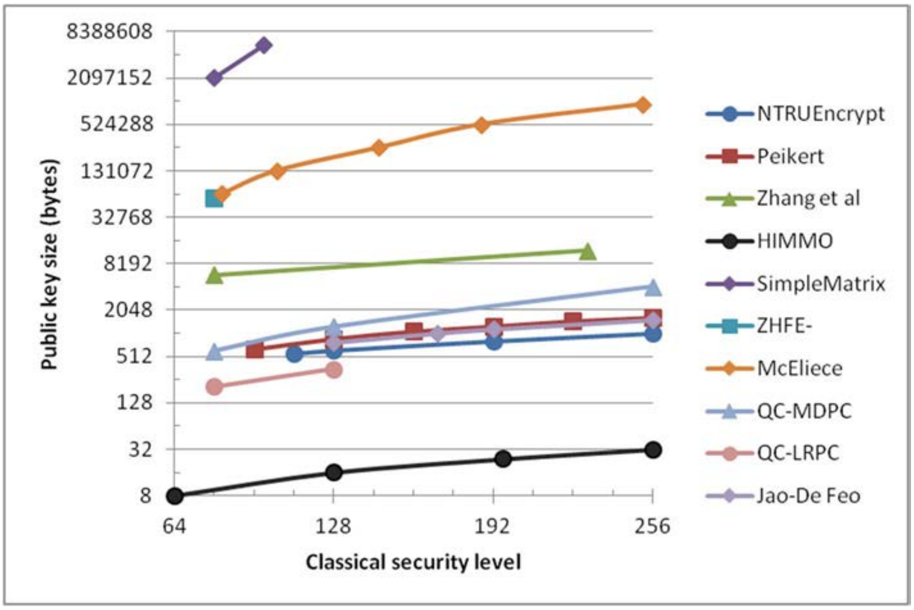

Figure 3: Public key sizes for key establishment

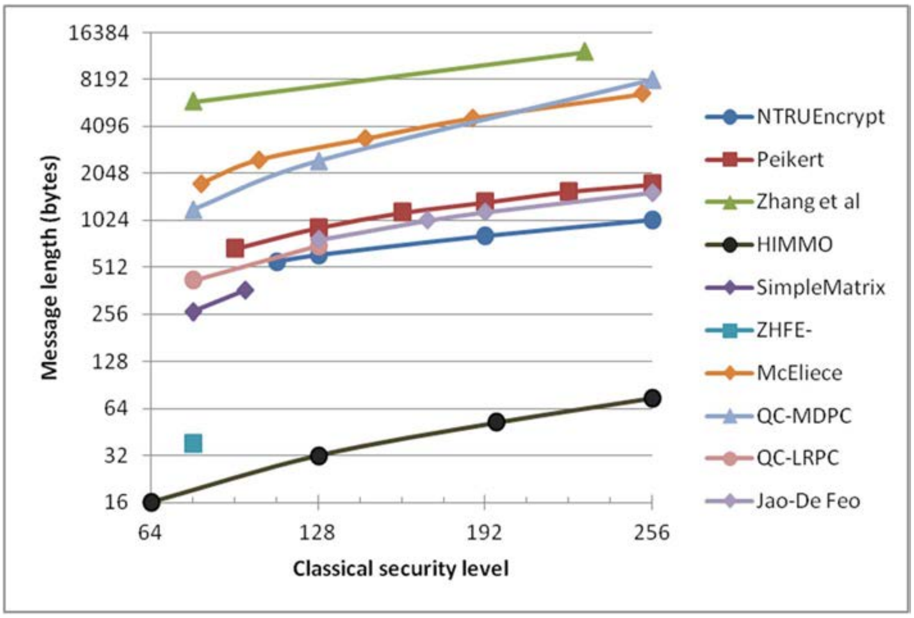

Figure 4: Message lengths for key establishment

11.3 Authentication

Figures 5 and 6 give the public key and signature sizes for ten of the authentication schemes. Again, in both figures the sizes are plotted on a logarithmic scale for clarity.

- The figures omit the lattice-based Lyubashevsky signature as there is no specific security estimate for the parameters; the signature by Aguilar et al as it will have similar public key sizes to, but larger signatures than, NTRU-MLS; BLISS as it is not as efficient as Ducas et al; and HIMMO as it cannot be used as a general purpose signature.

- For the multivariate schemes the figures include Gui and the cyclic versions of UOV and Rainbow, but omits QUARTZ as the keys sizes are similar to the 80-bit parameters for Gui and Sakumoto-Shirai-Hiwatari as it has substantially longer signatures.

- For code-based signatures the figures include the cyclic versions of Cayrel et al and RankSign, but omit Parallel-CFS as it has significantly larger key sizes.

- For hash-based schemes the figures include the Leighton-Micali signature over the original version of Merkle because of the smaller signature sizes and omit XMSS as it only has parameters for the higher security levels. Note that the Leighton-Micali parameters are limited to 2^{20} signatures and the SPHINCS parameters are limited to around 2^{60} signatures.

- Both isogeny-based schemes have been omitted as they cannot be used as general purpose signatures.

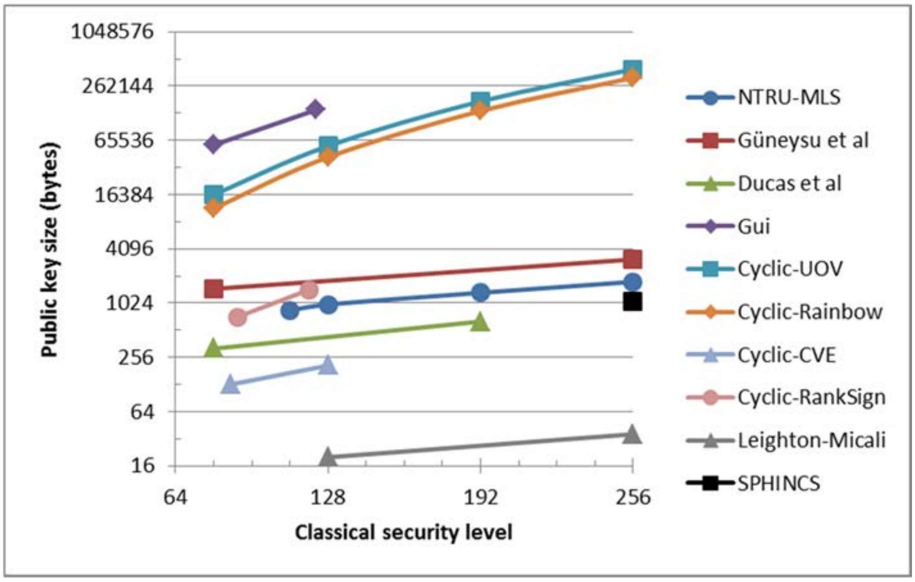

Figure 5: Public key sizes for authentication

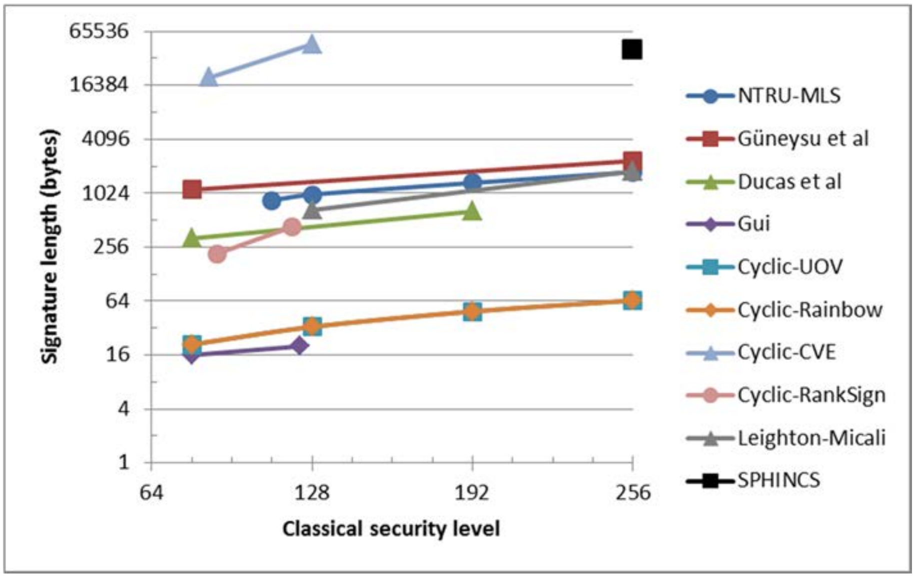

Figure 6: Signature lengths for authentication

12 Conclusions

The present document has given an overview and preliminary assessment of a representative range of quantum-safe primitives.

Some preliminary conclusions at this stage of the process are:

- There are a small number of lattice- and code-based key establishment schemes that should be considered in more detail by ETSI ISG QSC:
    - Lattice-based schemes offer good security, fast key generation for forward security and the flexibility to provide key agreement, key transport and key pre-distribution schemes.
    - Code-based schemes based on binary Goppa codes are well established and offer good security as basic key transport schemes. They are somewhat less flexible than lattices and may need supplementing to provide forward security or other features. The various proposals to reduce key sizes for code-based schemes are very interesting but would benefit from more academic assessment.

  - There has been a loss of confidence in multivariate schemes for key establishment and a move towards Ring-LWE.
  - Isogeny schemes appear to have good practical properties but more research is needed for a consensus to be established around their security.

- There is much more choice for authentication schemes where lattices, multivariate systems and hash trees all look likely to provide secure signature schemes:
  - Lattice-based signature schemes provide good options for general purpose applications and there are many different proposals to choose from. Key pre-distribution schemes are able to provide mutual authentication in peer-to-peer communications with very low overhead.
  - Code-based hash-and-sign schemes use high-rate Goppa codes which seem to be special or rank-metric codes which need further study. On the other hand, code-based Fiat-Shamir schemes can use random codes but suffer from long signatures.
  - Multivariate signature schemes uniquely offer very short signatures, which might be good for some use cases.
  - Isogeny-based signatures are not well developed and the existing proposals are not suitable for many applications.
  - Hash-based signature schemes offer good security but their practical requirements for bookkeeping and limits on the number of signatures available mean that they are not suitable for general-purpose applications.

- There are several promising new primitives including isogenies, structured McEliece schemes, rank metric coding schemes and HIMMO that would benefit from more independent academic assessment to build confidence and achieve a consensus on their security features and recommended key lengths.

- Formal security reductions, forward security and active security are important for general purpose, widely-used protocols. However it may be possible to relax these requirements for some restricted or application-specific use-cases.

- More work will be required on key sizes. Many of the "recommendations" in the citations should really be viewed as suggestions for further study than concrete proposals for standardization.

Following the initial assessment phase summarized in the present document, ETSI ISG QSC will narrow down the list of primitives given above to a more manageable size and provide a more detailed analysis and recommendations for a small number of proposals.

Annex A:
Classical key size comparison

A.1 Key establishment

Table A.1 compares the recommended key sizes for the candidate key establishment algorithms listed in the present document, based wherever possible on the author's suggestions for the 128-bit *classical* (i.e. not quantum) security level. Estimates for other security levels are given in clause 11. The size of the public key and the length of the message are listed. The message will either be the encrypted symmetric key for key transport schemes or the public key plus any additional fields for key agreements. The private key sizes are omitted as they can often be compressed by deriving them deterministically from a smaller seed.

NOTE: These tables are intended to provide informal guidance only. They have not been independently validated and are not endorsed by ETSI.

Table A.1: Key establishment key sizes for 128 bits of classical security

Type	Scheme	Security	Public key	Message	Comments
Lattice	NTRUEncrypt	128 bits	610 bytes	610 bytes	[i.49]
	Peikert	128 bits	864 bytes	918 bytes	[i.38], see note 1
	Zhang et al	140 bits	4 096 bytes	4 224 bytes	[i.40], see note 2
	Ghosh-Kate	---	1 344 bytes	1 440 bytes	[i.41], see note 3
	HIMMO	128 bits	16 bytes	16 bytes	[i.52], see note 4
Multivariate	Simple Matrix	100 bits	5 669 888 bytes	364 bytes	[i.97]
	HFE-	80 bits	132 112 bytes	16 bytes	[i.103]
	ZHFE	80 bits	58 403 bytes	39 bytes	[i.105], see note 5
	Polly Cracker Revisited	128 bits	---	78 644 bytes	[i.108], see note 6
Code	McEliece	129 bits	221 646 bytes	512 bytes	[i.148]
	Wild McEliece	128 bits	89 988 bytes	535 bytes	[i.150], see note 7
	MDPC McEliece	128 bits	12 142 592 bytes	2 464 bytes	[i.125]
	QC-MDPC McEliece	128 bits	1 232 bytes	2 464 bytes	[i.125]
	LRPC McEliece	128 bits	18 610 bytes	703 bytes	[i.157]
	DC-LRPC McEliece	128 bits	352 bytes	703 bytes	[i.157]
Isogeny	Jao-De Feo	128 bits	385 bytes	385 bytes	[i.196], see note 8

NOTE 1: The message size is for the passively secure key agreement from [i.34]. The additional field used for key validation in the actively secure agreement would likely lead to a 934-byte message.

NOTE 2: These parameters are only for the one-pass authenticated key establishment. There are no suggested 128-bits secure parameters for the two-pass protocol, but the 210-bits secure parameters have a 12 800-byte public key and a 13 056-byte message.

NOTE 3: Ghosh and Kate state that their parameters offer "high security" but do not give a specific security estimate. The listed public key and message sizes are only for the Ring-LWE component of their hybrid key establishment.

NOTE 4: These are 128-bits secure parameters where the identifiers are not hashed. The quoted size of the "public key" is the length of the user's identifier and the "message" is the identifier plus the helper data required to establish a shared symmetric key between a pair of users.

NOTE 5: These are the 80-bits secure parameters for ZHFE-.

NOTE 6: The message size is estimated using the smallest 128-bits secure parameters to encrypt a 128-bits symmetric key. The generic conversion to a public-key scheme described in [i.108] is not detailed enough to estimate the size of a public key.

NOTE 7: These are 128-bits secure parameters with $q = 31$.

NOTE 8: These are 128-bits secure parameters from [i.196] with public-key compression.

A.2 Authentication

Table A.2 compares the recommended key sizes for the candidate authentication algorithms listed in the present document, based wherever possible on the author's suggestions for the 128-bit *classical* (i.e. not quantum) security level. Estimates for other security levels are given in clause 11. The size of the public key and the length of the signature are listed.

NOTE: These tables are intended to provide informal guidance only. They have not been independently validated and are not endorsed by ETSI.

Table A.2: Authentication key sizes for 128 bits of classical security

Type	Scheme	Security	Public key	Signature	Comments
Lattice	Lyubashevsky	---	1 664 bytes	2 560 bytes	[i.60], see note 1
	NTRU-MLS	128 bits	988 bytes	988 bytes	[i.69]
	Aguilar et al	128 bits	1 082 bytes	1 894 bytes	[i.70], see note 2
	Güneysu et al	80 bits	1 472 bytes	1 120 bytes	[i.62], see note 3
	BLISS	128 bits	896 bytes	640 bytes	[i.63], see note 4
	Ducas et al	80 bits	320 bytes	320 bytes	[i.71]
	HIMMO	128 bits	32 bytes	16 bytes	[i.52], see note 5
Multivariate	Sakumoto et al	80 bits	16 bytes	9 762 bytes	[i.111], see note 6
	Quartz	80 bits	72 237 bytes	16 bytes	[i.112]
	Ding	123 bits	142 576 bytes	21 bytes	[i.115]
	UOV	128 bits	413 145 bytes	135 bytes	[i.118], see note 7
	Cyclic-UOV	128 bits	60 840 bytes	135 bytes	[i.118], see note 7
	Rainbow	128 bits	139 363 bytes	79 bytes	[i.118], see note 7
	Cyclic-Rainbow	128 bits	48 411 bytes	79 bytes	[i.118], see note 7
Code	Cayrel et al	128 bits	10 920 bytes	47 248 bytes	[i.159], see note 8
	Cyclic-Cayrel et al	128 bits	208 bytes	47 248 bytes	[i.159], see note 8
	Parallel-CFS	120 bits	503 316 480 bytes	108 bytes	[i.167]
	RankSign	130 bits	7 200 bytes	1 080 bytes	[i.168]
	Cyclic-RankSign	130 bits	3 538 bytes	1 080 bytes	[i.168]
Hash	Merkle	128 bits	32 bytes	1 731 bytes	[i.177], see note 9
	Leighton-Micali	128 bits	20 bytes	668 bytes	[i.171], see note 10
	XMSS	256 bits	64 bytes	8 392 bytes	[i.172], see note 11
	SPHINCS	256 bits	1 056 bytes	41 000 bytes	[i.185]
Isogeny	Jao-Soukharev	128 bits	768 bytes	1 280 bytes	[i.198], see note 12
	Sun-Tian-Wang	128 bits	768 bytes	16 bytes	[i.199], see note 13

NOTE 1: These are the parameters that are compatible with the Ring-LWE version of the signature. No specific security estimates are given in [i.60].
NOTE 2: These are the 128-bit secure size-optimized parameters.
NOTE 3: These are the smaller parameters from [i.62], but the estimate of their security was reduced to 80 bits in [i.63].
NOTE 4: These are the 128-bit secure size-optimized parameters and the quoted signature length includes the use of additional compression techniques.
NOTE 5: These are 128-bit secure parameters where the "public key" is a 256-bit hash of the user's credentials and the "message" is the MAC required to implicitly authenticate a pair of users.
NOTE 6: The signature length has been estimated by scaling the communication costs for the identification scheme to give a forgery cost of 80 bits.
NOTE 7: The 128-bit secure parameters for UOV, Cyclic-UOV, Rainbow and Cyclic-Rainbow are all over GF(256).
NOTE 8: The signature length has been estimated by scaling the communication costs for the identification scheme to give a forgery cost of 128 bits.
NOTE 9: These are the smallest 128-bit secure parameters with binary trees that allow up to 2^{20} signatures.
NOTE 10: These are the smallest 128-bit secure parameters that allow up to 2^{20} signatures.
NOTE 11: These are the smallest 256-bit secure parameters that allow up to 2^{60} signatures.
NOTE 12: The quoted "signature length" is the length of the commitment sent by the signer during the confirmation and disavowal protocols.
NOTE 13: This assumes that the signature uses the 128-bit secure parameters for the underlying isogeny-based key agreement [i.195] together with a 128-bit hash function.

Annex B: Quantum key size comparison

B.1 Key establishment

Tables B.1 and B.2 provide estimated key sizes for the candidate algorithms listed in the present document for the 128-bit *quantum* security level. When possible the figures are taken from the author's suggested parameters for 128-bits of quantum security. For primitives where these are not available, the key sizes are estimated by taking published parameters at appropriate classical security levels and adjusting them using the rules of thumb from clauses 6.5, 7.5, 8.5, 9.4 and 10.5.

NOTE: These tables are intended to provide informal guidance only. They have not been independently validated and are not endorsed by ETSI.

Table B.1: Key establishment key sizes for 128 bits of quantum security

Type	Scheme	Security	Public key	Message	Comments
Lattice	NTRUEncrypt	128 bits	610 bytes	610 bytes	[i.49], see note 1
	Peikert	128 bits	1 080 bytes	1 148 bytes	[i.38], see note 2
	Zhang et al	120 bits	3 840 bytes	3 968 bytes	[i.40], see note 3
	Ghosh-Kate	---	---	---	See note 4
	HIMMO	128 bits	32 bytes	43 bytes	[i.52], see note 5
Multivariate	Simple Matrix	---	---	---	See note 6
	HFE-	80 bits	1 052 704 bytes	32 bytes	[i.103], see note 7
	ZHFE	---	---	---	See note 6
	Polly Cracker Revisited	128 bits	---	419 431 bytes	See note 8
Code	McEliece	131 bits	1 046 739 bytes	870 bytes	[i.148], see note 9
	Wild McEliece	128 bits	424 899 bytes	1 070 bytes	[i.150], see note 10
	MDPC McEliece	128 bits	134 242 305 bytes	8 193 bytes	[i.125], see note 11
	QC-MDPC McEliece	128 bits	4 097 bytes	8 193 bytes	[i.125], see note 11
	LRPC McEliece	---	---	---	See note 12
	DC-LRPC McEliece	---	---	---	See note 12
Isogeny	Jao-De Feo	128 bits	564 bytes	564 bytes	[i.197], see note 13

NOTE 1: These are the 128-bit classically secure parameters which [i.49] suggests also provide 128-bits of quantum security.

NOTE 2: These are the 160-bit classically secure parameters which [i.38] suggests provide 128-bits of quantum security.

NOTE 3: These are the 160-bit classically secure one-pass parameters which the rule of thumb suggests have 120-bits of quantum security. Although they are smaller than the parameters in clause A.1, the probability of a key agreement failure has increased.

NOTE 4: The parameters suggested for the Ghosh-Kate authenticated key agreement do not come with a security estimate.

NOTE 5: These are the parameters for 256-bit symmetric keys with 256-bit identifiers.

NOTE 6: It is not clear how quantum algorithms will affect the security of Simple Matrix or ZHFE.

NOTE 7: The multivariate rule of thumb suggests that to maintain the level of security for HFE- the message length should double and the public key should increase by a factor of 8.

NOTE 8: These are the smallest 256-bit classically secure parameters which should provide 128-bits of quantum security. The message length is estimated for the encryption of a 256-bit symmetric key.

NOTE 9: These are the 263-bit classically secure parameters which should provide 131-bits of quantum security. They are also the parameters in the initial recommendations from the PQCrypto project [i.4].

NOTE 10: These are the 128-bit classically secure parameters for $q = 31$ with the length of the code doubled.

NOTE 11: These are the 256-bit classically secure parameters from [i.125] which should provide 128-bits of quantum security. The dimension of the code has more than tripled rather than doubling as suggested by the rule of thumb.

NOTE 12: It is not clear how quantum algorithms will affect the security of rank-based McEliece.

NOTE 13: These are the 128-bit quantum secure parameters from [i.197] with public-key compression.

B.2 Authentication

Table B.2: Authentication key sizes for 128 bits of quantum security

Type	Scheme	Security	Public key	Signature	Comments
Lattice	Lyubashevsky	----	----	---	See note 1
	NTRU-MLS	128 bits	1 138 bytes	1 138 bytes	[i.69], see note 2
	Aguilar et al	120 bits	1 238 bytes	2 100 bytes	[i.70], see note 3
	Güneysu et al	128 bits	2 300 bytes	1 800 bytes	[i.62], see note 4
	BLISS	120 bits	896 bytes	768 bytes	[i.63], see note 5
	Ducas et al	128 bits	580 bytes	580 bytes	[i.71], see note 6
	HIMMO	128 bits	32 bytes	32 bytes	[i.52], see note 7
Multivariate	Sakumoto et al	---	---	---	See note 8
	Quartz	80 bits	577 896 bytes	32 bytes	[i.112], see note 9
	Ding	123 bits	1 140 608 bytes	42 bytes	[i.115], see note 9
	UOV	128 bits	3 898 895 bytes	285 bytes	[i.118], see note 10
	Cyclic-UOV	128 bits	496 565 bytes	285 bytes	[i.118], see note 10
	Rainbow	128 bits	1 498 230 bytes	178 bytes	[i.118], see note 10
	Cyclic-Rainbow	128 bits	482 086 bytes	178 bytes	[i.118], see note 10
Code	Parallel-CFS	120 bits	2 013 265 920 bytes	216 bytes	[i.167], see note 11
	Cayrel et al	128 bits	43 680 bytes	94 496 bytes	[i.159], see note 11
	Cyclic-Cayrel et al	128 bits	416 bytes	94 496 bytes	[i.159], see note 11
	RankSign	---	---	---	See note 12
	Cyclic-RankSign	---	---	---	See note 12
Hash	Merkle	128 bits	32 bytes	1 731 bytes	[i.177], see note 13
	Leighton-Micali	128 bits	34 bytes	1 740 bytes	[i.171], see note 14
	XMSS	128 bits	64 bytes	8 392 bytes	[i.172], see note 15
	SPHINCS	128 bits	1 056 bytes	41 000 bytes	[i.185]
Isogeny	Jao-Soukharev	128 bits	1 152 bytes	1 152 bytes	[i.198]
	Sun-Tian-Wang	128 bits	1 152 bytes	32 bytes	[i.199], see note 16

NOTE 1: The parameters for Lyubashevksy's signature given in [i.60] do not come with security estimates.

NOTE 2: These are the 128-bit classicaly secure parameters scaled up by a third according to the rule of thumb for lattice-based primitives.

NOTE 3: These are the 160-bit classically secure size-optimized parameters which the lattice-based rule of thumb suggests provide 120-bits of quantum security.

NOTE 4: These are extrapolated from the 80- and 256-bit classically secure parameters which the lattice-based rule of thumb suggests should provide 60- and 192-bits of quantum security.

NOTE 5: These are the 160-bit classically secure size-optimized parameters which the lattice-based rule of thumb suggests provide 120-bits of quantum security.

NOTE 6: These are extrapolated from the 80- and 192-bit classically secure parameters which the lattice-based rule of thumb suggests should provide 60- and 144-bits of quantum security.

NOTE 7: These are the parameters for 256-bit symmetric keys with 256-bit hashed credentials.

NOTE 8: It is not clear how quantum algorithms will affect the security of the Sakumoto-Shirai-Hiwatari identification scheme.

NOTE 9: The multivariate rule of thumb suggests that to maintain the level of security for Quartz and Gui the signature length should double and the public key should increase by a factor of 8.

NOTE 10: These are the 256-bit classically secure UOV and Rainbow parameters over GF(256) which the multivariate rule of thumb suggests should provide 128-bits of quantum security.

NOTE 11: The rule of thumb for code-based primitives suggests that the signature lengths for Parallel-CFS and unstructured Cayrel et al should double and the public key sizes should quadruple whereas for cyclic Cayrel et al both should double.

NOTE 12: It is not clear how quantum algorithms will affect the security of RankSign.

NOTE 13: The rule of thumb is that no changes are needed for hash-based signatures whose security is based on the collision resistance of the hash function.

NOTE 14: These are the smallest parameters with 128-bits of quantum security that allow up to 2^{20} signatures.

NOTE 15: These are the smallest parameters with 128-bits of quantum security that allow up to 2^{60} signatures.

NOTE 16: This assumes that the signature uses the 128-bit quantum secure parameters for the underlying isogeny-based key agreement [i.195] together with a 256-bit hash function.

History

Document history		
V1.1.1	July 2016	Publication