ETSI TR 103 570 V1.1.1 (2017-10)

CYBER;
Quantum-Safe Key Exchanges

Reference

DTR/CYBER-QSC-007

Keywords

algorithm, confidentiality, quantum cryptography, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

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

Contents

Intellectual Property Rights

Essential patents

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

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

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document compares a selection of proposals for quantum-safe key exchanges taken from the academic literature. In particular, it includes key exchanges based on the Learning with Errors (LWE), Ring-LWE and Supersingular Isogeny Diffie-Hellman (SIDH) problems, as well as key exchanges constructed from the Niederreiter and NTRU key transport schemes.

The present document gives an overview of each key exchange, lists proposed parameters and gives software performance estimates on a range of processors. It also discusses various security and implementation considerations such as active attacks and side-channel vulnerabilities.

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.

user with regard to a particular subject area.

[i.1] ETSI QKD GS 002: "Quantum Key Distribution (QKD); Use cases".

[i.2] ETSI GR QSC 001: "Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework".

[i.3] IETF draft-ietf-tls-tls13-19: "The Transport Layer Security (TLS) protocol version 1.3", 10 March 2017.

[i.4] IETF RFC 7296: "Internet Key Exchange protocol version 2 (IKEv2)", October 2014.

[i.5] ETSI GR QSC 003: "Quantum Safe Cryptography; Case Studies and Deployment Scenarios".

[i.6] I. Biehl, B. Meyer and V. Müller: "Differential fault attacks on elliptic curve cryptosystems" in CRYPTO, 2000.

[i.7] E. Fujisaki and T. Okamoto: "Secure integration of asymmetric and symmetric encryption schemes" in CRYPTO, 1999.

[i.8] E. E. Targhi and D. Unruh: "Post-quantum security of the Fujisaki-Okamoto and OAEP transforms" in TCC, 2016.

[i.9] P. Kocher: "Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems" in CRYPTO, 1996.

[i.10] P. Kocher, J. Jaffe and B. Jun: "Differential power analysis" in CRYPTO, 1999.

[i.11] D. Brumley and D. Boneh: "Remote timing attacks are practical" Computer Networks, vol. 48, no. 5, pp. 701-716, 2005.

[i.12] J. Großschädl, E. Oswald, D. Page and M. Tunstall: "Side-channel analysis of cryptographic software via early-terminating multiplications" in ISIC, 2009.

[i.13] S. Mangard, E. Oswald and T. Popp: "Power analysis attacks: Revealing the secrets of smart cards", New York: Springer Science & Business Media, 2008.

[i.14] J. D. Golić and C. Tymen: "Multiplicative masking and power analysis of AES" in CHES, 2002.

[i.15] M. Rivain and E. Prouff: "Provably secure higher-order masking of AES" in CHES, 2010.

[i.16] M. Ajtai: "Generating hard instances of lattice problems" in STOC, 1996.

[i.17] M. Ajtai and C. Dwork: "A public-key cryptosystem with worst-case/average-case equivalence" in STOC, 1997.

[i.18] J. Hoffstein, J. Pipher and J. H. Silverman: "NTRU: A ring-based public key cryptosystem" in ANTS III, 1998.

[i.19] O. Regev: "On lattices, learning with errors, random linear codes, and cryptography" in STOC, 2005.

[i.20] D. Stehlé, R. Steinfeld, K. Tanaka and K. Xagawa: "Efficient public key encryption based on ideal lattices" in ASIACRYPT, 2009.

[i.21] V. Lyubashevsky, C. Peikert and O. Regev: "On ideal lattices and learning with errors over rings", Journal of the ACM (JACM), vol. 60, no. 6, p. 43, 2013.

[i.22] C. Peikert: "Some recent progress in lattice-based cryptography" in TCC, 2009.

[i.23] J. Ding, X. Xie and X. Lin: "A simple provably secure key exchange scheme based on the Learning with Errors problem", IACR ePrint Archive 2012/688, 2012.

[i.24] C. Peikert: "Lattice cryptography for the internet" in PQC, 2014.

[i.25] J. Bos, C. Costello, L. Ducas, I. Mironov, M. Naehrig, V. Nikolaenko, A. Raghunathan and D. Stebila: "Frodo: Take off the ring! Practical, quantum-secure key exchange from LWE", IACR ePrint Archive 2016/659, 2016.

[i.26] S. Battacharya, O. Garcia-Morchon, R. Rietman and L. Tolhuizen: "spKEX: An optimized lattice-based key exchange", IACR ePrint Archive 2017/709, 2017.

[i.27] E. Alkim, L. Ducas, T. Pöppelmann and P. Schwabe: "Post-quantum key exchange - A new hope" in USENIX Security, 2016.

[i.28] J. Bos, C. Costello, M. Naehrig and D. Stebila: "Post-quantum key exchange for the TLS protocol from the Ring Learning with Errors problem" in Security and Privacy, 2015.

[i.29] E. Alkim, P. Jukabeit and P. Schwabe: "A new hope on ARM Cortex-M", IACR ePrint Archive 2016/758, 2016.

[i.30] S. Fluhrer: "Cryptanalysis of Ring-LWE based key exchange with key share reuse", IACR ePrint Archive 2016/085, 2016.

[i.31] J. Ding, S. Alsayigh, R. V. Saraswathy and S. Fluhrer: "Leakage of signal function with reused keys in RLWE key exchange", IACR ePrint Archive 2016/1176, 2016.

[i.32] P. Hodgers, F. Regazzoni, R. Gilmore, C. Moore and T. Ode: "State-of-the-art in physical side-channel attacks and resistant technologies", SAFECrypto D7.1, 2016.

[i.33] L. Groot Bruinderink, A. Hülsing, T. Lange and Y. Yaro: "Flush, Gauss and reload - A cache attack on the BLISS lattice-based signature scheme" in CHES, 2016. .

[i.34] T. Espitau, P. A. Fouque, B. Gerard and M. Tibouch: "Side-channel attacks on BLISS lattice-based signatures", IACR ePrint Archive 2017/505, 2017.

[i.35] R. Primas, P. P. and S. Mangar: "Single-trace side-channel attacks on masked lattice-based encryption", IACR ePrint Archive 2017/594, 2017.

[i.36] S. Roy, O. Reparaz, F. Vercauteren and I. Verbauwhed: "Compact and side channel secure discrete Gaussian sampling", IACR ePrint Archive 2014/591, 2014.

[i.37] O. Reparaz, S. Roy, F. Vercauteren and I. Verbauwhede: "A masked Ring-LWE implementation" in CHES, 2015.

[i.38] T. Oder, T. Schneider, T. Pöppelmann and T. Güneys: "Practical CCA2-secure and masked Ring-LWE implementation", IACR ePrint Archive 2016/1109, 2016.

[i.39] V. Sing: "A practical key exchange for the internet using lattice cryptography", IACR ePrint Archive 138/2015, 2015.

[i.40] V. Singh and A. Chopr: "Even more practical key exchanges for the internet using lattice cryptography", IACR ePrint Archive 2015/1120, 2015.

[i.41] M. R. Albrecht, R. Player and S. Scot: "On the concrete hardness of learning with errors", Journal of Mathematical Cryptology, vol. 9, no. 3, pp. 169-203, 2015.

[i.42] L. Ducas, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler and D. Stehlé: "CRYSTALS - Dilithium: Digital signatures from module lattices", IACR ePrint Archive 2017/634, 2017.

[i.43] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck and D. Stehlé: "CRYSTALS - Kyber: A CCA-secure module-lattice-based KEM", IACR ePrint Archive 2017/634, 2017.

[i.44] A. Langlois and D. Stehlé: "Worst-case to average-case reductions for module lattices", Designs, Codes and Cryptography, vol. 75, no. 3, pp. 565-599, 2015.

[i.45] D. Jao and L. De Feo: "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies" in PQC, 2011.

[i.46] L. De Feo, D. Jao and J. Plût: "Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies", Journal of Mathematical Cryptography, vol. 8, no. 3, pp. 209-247, 2014.

[i.47] C. Costello, P. Longa and P. Naehrig: "Efficient algorithms for supersingular isogeny Diffie-Hellman" in CRYPTO, 2016.

[i.48] S. D. Galbraith, C. Petit, B. Shani and Y. B. Ti: "On the security of supersingular isogeny cryptosystems" in ASIACRYPT, 2016.

[i.49] S. D. Galbraith and F. Vercauteren: "Computational problems in supersingular elliptic curve isogenies", IACR ePrint Archive 2017/774, 2017.

[i.50] D. Kirkwood, B. Lackey, J. McVey, M. Motley, J. Solinas and D. Tuller: "Failure is not an option: Standardisation issues for post-quantum key agreement" in NIST Workshop on Cybersecurity in a Post-Quantum World, 2015.

[i.51] Y. B. Ti: "Fault attacks on supersingular isogeny cryptosystems" in PQC, 2017.

[i.52] A. Gélin and B. Wesolowski: "Loop-abort faults on supersingular isogeny cryptosystems" in PQC, 2017.

[i.53] C. Costello, D. Jao, P. Longa, M. Naehrig, J. Renes and D. Urbanik: "Efficient compression of SIDH public keys" in EUROCRYPT, 2017.

[i.54] A. Jalali, R. Azarderakhsh, M. Mozaffari-Kermani and D. Jao: "Supersingular isogeny Diffie-Hellman key exchange on 64-bit ARM", IEEE Transactions on Dependable and Secure Computing, vol. (to appear), 2017.

[i.55] B. Koziel, A. Jalali, R. Azarderakhsh, D. Jao and M. Mozaffari-Kermani: "NEON-SIDH: Efficient implementation of supersingular isogeny Diffie-Hellman key exchange protocol on ARM" in CANS, 2016.

[i.56] H. Niederreiter: "Knapsack-type cryptosystems and algebraic coding theory", Problems of Control and Information Theory, vol. 15, no. 2, pp. 159-166, 1986.

[i.57] R. McEliece: "A public key cryptosystem based on algebraic coding theory", DSN progress report 42.44, 1978.

[i.58] V. Shoup: "Fast construction of irreducible polynomials over finite fields", Journal of Symbolic Computation, vol. 17, no. 5, pp. 371-391, 1994.

[i.59] N. Patterson: "The algebraic decoding of Goppa codes", IEEE Transactions on Information Theory, vol. 21, no. 2, pp. 203-207, 1975.

[i.60] E. R. Berlekamp: "Algebraic coding theory", New York: McGraw-Hill, 1968.

[i.61] K. Kobara and H. Imai: "Semantically secure McEliece public-key cryptosystems - conversions for McEliece PKC" in PKC, 2001.

[i.62] E. Persichetti: "Secure and anonymous hybrid encryption from coding theory" in PQC, 2013.

[i.63] Q. Guo, T. Johansson and P. Stankovski: "A key recovery attack on MDPC with CCA security using decoding errors" in ASIACRYPT, 2016.

[i.64] S. Heyse, A. Moradi and C. Paar: "Practical power analysis attakcs on software implementations of McEliece" in PQC, 2010.

[i.65] R. Avanzi, S. Hoerder, D. Page and M. Tunstall: "Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems", Journal of Cryptographic Engineering, vol. 1, no. 4, pp. 271-281, 2011.

[i.66] D. J. Bernstein, T. Chou and P. Schwabe: "McBits: Fast constant-time code-based cryptography" in CHES, 2013.

[i.67] M. Georgieva and F. de Portzamparc: "Toward secure implementation of McEliece decryption" in COSADE, 2015.

[i.68] F. Strenzke: "Timing attacks against the syndrome inversion in code-based cryptosystems" in PQC, 2013.

[i.69] PQCrypto: "Initial recommendations of long-term secure post-quantum systems", 2015.

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

[i.70] D. J. Bernstein, T. Lange and C. Peters: "Attacking and defending the McEliece cryptosystem" in PQC, 2008.

[i.71] S. H. S. de Vries: "Achieving 128-bit security against quantum attacks in OpenVPN", MSc Thesis, University of Twente, 2016.

[i.72] D. J. Bernstein: "List decoding for binary Goppa codes" in International Conference on Coding and Cryptology, 2011.

[i.73] D. J. Bernstein: "Grover vs McEliece" in PQC, 2010.

[i.74] D. J. Bernstein and T. Lange: "eBACS: ECRYPT benchmarking of cryptographic systems".

NOTE: Available at https://bench.cr.yp.to.

[i.75] B. Biswas and N. Sendrier: "McEliece cryptosystem implementation: Theory and practice" in PQC, 2008.

[i.76] T. Chou: "McBits revisited" IACR ePrint Archive 2017/793, 2017.

[i.77] S. Heyse: "Low-reiter: Niederreiter encryption scheme for embedded microcontrollers" in PQC, 2010.

[i.78] W. Whyte: "EEES#1: Implementation aspects of NTRUEncrypt, Version 3.1", 2015.

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

[i.79] J. Hoffstein; J. Pipher, J. M. Schanck, J. H. Silverman, W. Whyte and Z. Zhang: "Choosing parameters for NTRUEncrypt" in CT-RSA, 2017.

[i.80] É. Jaulmes and A. Joux: "A chosen-ciphertext attack against NTRU" in CRYPTO, 2000.

[i.81] N. Howgrave-Graham, P. Nguyen, D. Pointcheval, J. Proos, J. Silverman and A. Singer: "The impact of decryption failures on the security of NTRU encryption" in CRYPTO, 2003.

[i.82] N. Gama and P. Q. Nguyen: "New chosen-ciphertext attacks on NTRU" in PKC, 2007.

[i.83] A. Hülsing, J. Rijnveld, J. Schanck and P. Schwabe: "High-speed key encapsulation from NTRU", IACR ePrint Archive 2017/667, 2017.

[i.84] N. Howgrave-Graham, J. Silverman, A. Singer and W. Whyte: "NAEP: Provable security in the presence of decryption failures", IACR ePrint Archive 2003/172, 2003.

[i.85] M. Stam: "A key encapsulation mechanism for NTRU" in Cryptography and Coding, 2005.

[i.86] J. H. Silverman and W. Whyte: "Timing attacks on NTRUEncrypt via variation in the number of hash calls" in CT-RSA, 2007.

[i.87] A. Atici, L. Batina, B. Grierlichs and I. Verbauwhede: "Power analysis on NTRU implementations for RFIDs: First results" in RFIDSec, 2008.

[i.88] A. Wang, X. Zheng and Z. Wang: "Power analysis attacks and countermeasures on NTRU-based wireless body area networks", KSII Transactions on Internet and Information Systems, vol. 7, no. 5, pp. 1094-1107, 2013.

[i.89] X. Zheng, A. Wang and W. Wei: "First-order collision attack on protected NTRU cryptosystem", Microprocessors and Microsystems, vol. 37, pp. 601-609, 2013.

[i.90] N. Howgrave-Graham: "A hybrid lattice-reduction and meet-in-the-middle attack against NTRU" in CRYPTO, 2007.

[i.91] O. M. Guillen, T. Pöppelmann, J. M. B. Mera, E. F. Bongenaar, G. Sigl and J. Sepulveda: "Towards post-quantum security for IoT endpoints with NTRU" in DATE, 2017.

[i.92] J. H. Cheon, J. Jeong and C. Lee: "An algorithm for NTRU problems and cryptanalysis of the GGH multilinear map without a low-level encoding of zero" in ANTS-XII, 2016.

[i.93] M. Albrecht, S. Bai and L. Ducas: "A subfield lattice attack on overstretched NTRU assumptions" in CRYPTO, 2016.

[i.94] D. J. Bernstein, C. Chuengsatiansup, T. Lange and C. van Vredendaal: "NTRU Prime", IACR ePrint Archive 2016/461, 2016.

[i.95] P. Kirchner and P.-A. Fouque: "Comparison between subfield and straightforward attacks on NTRU", IACR ePrint Archive 2016/717, 2016.

[i.96] B. Applebaum, D. Cash, C. Peikert and A. Sahai: "Fast cryptographic primitives and circular-secure encryption based on hard learning problems" in CRYPTO, 2009.

[i.97] L. Ducas and A. Durmus: "Ring-LWE in polynomial rings" in PKC, 2012.

[i.98] C. Peikert: "How (not) to instantiate Ring-LWE" in SCN, 2016.

[i.99] J. H. Cheon, K. Han, J. Kim, C. Lee and Y. Son: "A practical post-quantum public-key cryptosystem based on spLWE" in ICISC, 2016.

[i.100] L. Ducas, V. Lyubashevsky and T. Prest: "Efficient identity-based encryption over NTRU lattices" in ASIACRYPT, 2014.

[i.101] J. Fan and F. Vercauteren: "Somewhat practical fully homomorphic encryption", IACR ePrint Archive 2012/144, 2012.

[i.102] D. Micciancio and C. Peikert: "Hardness of SIS and LWE with small parameters" in CRYPTO, 2013.

[i.103] J. Buchmann, E. Gopfert, R. Player and T. Wunderer: "On the hardness of LWE with binary error: Revisiting the hybrid lattice-reduction and meet-in-the-middle attack" in AFRICACRYPT, 2016.

[i.104] M. Albrecht: "On dual lattice attacks against small-secret LWE and parameter choices in HElib and SEAL" in EUROCRYPT, 2017.

[i.105] A. Banerjee, C. Peikert and A. Rosen: "Pseudorandom functions and lattices" in EUROCRYPT, 2012.

[i.106] J. H. Cheon, D. Kim, J. Lee and Y. Song: "Lizard: Cut of the tail! Practical post-quantum public-key encryption from LWE and LWR", IACR ePrint Archive 2016/1126, 2016.

[i.107] T. Pöppelmann and T. Güneysu: "Towards practical lattice-based public-key encryption on reconfigurable hardware" in SAC, 2013.

[i.108] L. Tolhuizen, R. Rietman and O. Garcia-Morchon: "Improved key-reconciliations method" IACR ePrint Archive 2017/295, 2017.

[i.109] Z. Brakerski, A. Langlois, C. Peikert, O. Regev and D. Stehlé: "Classical hardness of learning with errors" in STOC, 2013.

[i.110] S. Chatterjee, N. Koblitz, A. Menezes and P. Sarkar: "Another look at tightness II: Practical issues in cryptography", IACR ePrint Archive 2016/360, 2016.

[i.111] K. Eisenträger, S. Hallgren and K. E. Lauter: "Weak instances of PLWE" in SAC, 2014.

[i.112] Y. Elias, K. E. Lauter, E. Ozman and K. E. Stange: "Provably weak instances of Ring-LWE" in CRYPTO, 2015.

[i.113] W. Castryck, I. Iliashenko and F. Vercauteren: "Provably weak instances of Ring-LWE revisited" in EUROCRYPT, 2016.

[i.114] H. Chen, K. E. Lauter and K. E. Stange: "Vulnerable Galois RLWE families and improved attacks", IACR ePrint Archive 2016/193, 2016.

[i.115] R. Lindner and C. Peikert: "Better key sizes (and attacks) for LWE-based encryption" in CT-RSA, 2011.

[i.116] A. Blum, A. Kalai and H. Wasserman: "Noise-tolerant learning, the parity problem, and the statistical query model", Journal of the ACM, vol. 50, no. 4, pp. 506-519, 2003.

[i.117] M. Abe, R. Gennaro, K. Kurosawa and V. Shoup: "Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM" in EUROCRYPT, 2005.

[i.118] J. Silverman, The arithmetic of elliptic curves, New York: Springer-Verlag, 1992.

[i.119] R. Bröker: "Constructing supersingular curves", J. Comb. Number Theory, vol. 1, no. 3, pp. 269-273, 2009.

[i.120] R. Azarderakhsh, D. Jao, K. Kalach, B. Koziel and C. Leonardi: "Key compression for isogeny-based cryptosystems" in AsiaPKC, 2016.

[i.121] A. Childs, D. Jao and V. Soukharev: "Constructing elliptic curve isogenies in quantum subexponential time", Journal of Mathematical Cryptology, vol. 8, no. 1, pp. 1-29, 2014.

[i.122] J.-F. Biasse, D. Jao and A. Sankar: "A quantum algorithm for computing isogenies between supersingular elliptic curves" in INDOCRYPT, 2014.

[i.123] C. Delfs and S. D. Galbraith: "Computing isogenies between supersingular elliptic curves over Fp" in Designs, Codes and Cryptography, 2014.

[i.124] C. Petit: "Faster algorithms for isogeny problems using torsion point images", IACR ePrint Archive 2017/571, 2017.

[i.125] D. Stebila and M. Mosca: "Post-quantum key exchange for the internet and the Open Quantum-Safe project", IACR ePrint Archive 2016/1017, 2016.

[i.126] P. Longa and M. Naehrig: "Speeding up the number theoretic transform for faster ideal lattice-based cryptography" in CANS, 2016.

3 Abbreviations

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

AES-NI	AES New Instructions
AMD	Advanced Micro Devices
ARM	Advanced RISC machine
AVX	Advanced Vector Extensions
BKZ	Block Korkine-Zolotarev algorithm
DH	Diffie-Hellman
DTLS	Datagram Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
GF	Galois Field
IKE	Internet Key Exchange
IoT	Internet of Things
KDF	Key Derivation Function
KEM	Key Encapsulation Mechanism
LWE	Learning With Errors
LWR	Learning With Rounding
NTT	Number-Theoretic Transform
QKD	Quantum Key Distribution
QSC	Quantum-Safe Cryptography
RSA	Rivest-Shamir-Adleman protocol
SIDH	Supersingular Isogeny Diffie-Hellman
SSH	Secure Shell
TLS	Transport Layer Security
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

4 Quantum-safe key exchanges

4.1 Introduction

Key establishment is a public-key cryptographic primitive which allows two parties to set up a shared secret key. In a key exchange, the shared secret key is securely derived from information contributed by both parties; for example, by exchanging public keys with each other. The standard examples of a key exchange are Diffie-Hellman (DH) and Elliptic Curve Diffie-Hellman (ECDH). In a key transport mechanism one party generates the secret key and securely shares it with the second party; for example, by sending it encrypted under the second party's public key. The standard example of a key transport mechanism is RSA encryption.

DH, ECDH and RSA will all be made insecure by the development of large-scale fault-tolerant quantum computing. The present document discusses proposals in the academic literature for quantum-safe key exchange primitives that could be used directly to replace DH and ECDH. The present document also includes examples of key exchanges constructed from key transport mechanisms.

NOTE 1: Quantum-safe key transport mechanisms that could be used to replace RSA will be considered in a separate document.

NOTE 2: The present document only considers algorithmic key exchange mechanisms. Other mechanisms, based on Quantum Key Distribution (QKD), are considered in ETSI QKD GS 002 [i.1].

Key exchanges can either use short-term ephemeral keys or long-term static keys.

- In ephemeral key exchanges both parties generate new short-term public keys that are only used in a single exchange.