ETSI TR 103 965 V1.1.1 (2024-10)

CYBER; Quantum-Safe Cryptography (QSC);
Impact of Quantum Computing on
Cryptographic Security Proofs

Reference
DTR/CYBER-QSC-0020

Keywords
Quantum Safe 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

Modal verbs terminology

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

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

Executive summary

There is a common misconception that to make a classically secure cryptosystem quantum-safe, it suffices to replace its underlying computational-hardness assumptions with "quantum-hard" assumptions. However, this is not always the case. The present document provides an overview of the impact of quantum computing on cryptographic security proofs; it illustrates how for certain classes of cryptographic systems the security proofs need to be adapted, for which classes this has already successfully been done, and what the practical implications of these adaptations are.

The present document is meant for cryptographic experts who want to get insight into practical changes that need to be made to existing systems to make those systems quantum-safe, or who want to understand the fundamental challenges in proving security against a quantum adversary.

Introduction

The advent of a cryptographically-relevant quantum computer (or CRQC for short) will severely impact most currently-used cryptographic systems. Notably, a CRQC can factor integers and compute discrete logarithms in polynomial time, thereby breaking systems based on the hardness of these problems.

However, simply replacing these problems by others which are (believed to be) impervious even to a quantum computer does not completely solve the issue. This is due to the fact that many security proofs of cryptographic systems are no longer valid in the presence of a quantum-capable attacker; while this does not automatically imply that the affected systems would be broken by a quantum computer, it does raises questions on the exact security guarantees that the systems can provide.

The present document analyses the impact of quantum computers on cryptographic security proofs, describing the current knowledge on the topic and the expected effects on security.

1 Scope

The present document is intended to provide an overview of the impact of quantum computing on the security proofs of several cryptographic protocols. It focuses on cryptographic protocols that can be run on classical hardware; further, it discusses which security proofs are invalidated, or otherwise affected, in the presence of an attacker with access to a CRQC, and discusses for each affected system whether:

a) an alternative proof has been found that does provide security against quantum attacks, but possibly with a reduced security level;

b) no alternative proof has been found, but security is expected to still hold;

c) the cryptographic system is expected to be broken by quantum attacks, in a way which is not captured by the classical security proof, although no concrete quantum attack exists yet; or

d) a concrete quantum attack that breaks security, in a way which is not captured by the classical proof, is available.

In terms of the security proofs and problems under consideration, the present document includes the following:

1) The quantum random oracle model, and in particular its usage in:

   a) The Fiat-Shamir transformation.

   b) The Fujisaki-Okamoto transformation.

2) The rewinding technique for zero-knowledge proof systems.

3) The binding property of commitment schemes.

4) The universal-composability framework.

5) The indifferentiability framework.

6) Security proofs of pseudo-random functions.

In addition to presenting the theoretical developments on these topics, the present document elaborates on the practical consequences. In some cases, the security of classically secure schemes is uncertain in the face of a quantum adversary. In other cases, the security of the scheme holds, but the parameters need to be adjusted to retain the same level of security.

NOTE: The present document does not discuss so-called "quantum-annoying" schemes, which still base their security on computational problems that can be solved (relatively) efficiently by a quantum computer, but force such an attack to perform a high number of operations, hence making it impractical for the expected first generation of quantum computers.

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] IETF RFC 2313 (1998): "PKCS# 1: RSA encryption version 1.5".

[i.2] D. Bleichenbacher: "Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1". Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1998.

[i.3] N. Koblitz, A.J. Menezes: "The random oracle model: a twenty-year retrospective". Designs, Codes and Cryptography 77.2 (2015): pp. 587-610.

[i.4] R. Canetti, et al.: "The random oracle methodology, revisited". Journal of the ACM (JACM) 51.4 (2004): pp. 557-594.

[i.5] J. Coron, et al.: "Universal padding schemes for RSA". Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2002.

[i.6] J. Van De Graaf: "Towards a formal definition of security for quantum protocols". Université de Montréal, 1997.

[i.7] D. Unruh: "Quantum proofs of knowledge". Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 2012.

[i.8] J. Watrous: "Zero-knowledge against quantum attacks". Proceedings of the 38th annual ACM symposium on Theory of Computing. 2006.

[i.9] J. Don, et al.: "Security of the Fiat-Shamir transformation in the quantum random-oracle model". Advances in Cryptology-CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II 39. Springer International Publishing, 2019.

[i.10] V. Lyubashevsky et al.: "Crystals-dilithium". Algorithm Specifications and Supporting Documentation (2020).

[i.11] R. El Bansarkhani and A. El Kaafaran: "Post-quantum attribute-based signatures from lattice assumptions." Cryptology ePrint Archive (2016).

[i.12] D. Pointcheval, and J. Stern: "Security arguments for digital signatures and blind signatures". Journal of cryptology 13 (2000): pp. 361-396.

[i.13] C. Schnorr: "Efficient signature generation by smart cards". Journal of cryptology 4 (1991): pp. 161-174.

[i.14] Q .Liu and M. Zhandry: "Revisiting post-quantum fiat-shamir". Advances in Cryptology-CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II 39. Springer International Publishing, 2019.

[i.15] M. Barbosa et al.: "Fixing and mechanizing the security proof of fiat-shamir with aborts and dilithium". Cryptology ePrint Archive (2023).

[i.16] E. Fujisaki and T. Okamoto: "Secure integration of asymmetric and symmetric encryption schemes". In CRYPTO'99, volume 1666 of LNCS, pp. 537-554. Springer, Heidelberg, August 1999.

[i.17] E. Fujisaki and T. Okamoto: "Secure integration of asymmetric and symmetric encryption schemes". Journal of Cryptology, 26(1): pp. 80-101, January 2013.

[i.18] D. Hofheinz, et al: "A modular analysis of the Fujisaki-Okamoto transformation". In TCC 2017, Part I, volume 10677 of LNCS, pp. 341-371. Springer, Heidelberg, November 2017.

[i.19] J. Duman et al.: "Faster Kyber and Saber via a generic Fujisaki-Okamoto transform for multi-user security in the Q-ROM". 2021.

[i.20] J. Bos et al.: "CRYSTALS - Kyber: A CCA-secure module-lattice-based KEM". 2018 IEEE European Symposium on Security and Privacy (EuroS P), pp. 353-367.

[i.21] M. Bellare et al.: "Public-key encryption in a multi-user setting: Security proofs and improvements". In EUROCRYPT 2000, volume 1807 of LNCS, pp. 259-274. Springer, Heidelberg, May 2000.

[i.22] A. Ambainis et al.: "Quantum attacks on classical proof systems: The hardness of quantum rewinding". In 2014 IEEE 55th Annual Symposium on Foundations of Computer Science, pages 474-483, Oct 2014.

[i.23] D. Unruh: "Computationally Binding Quantum Commitments". In Proceedings, Part II, of the 35th Annual International Conference on Advances in Cryptology. 2016 pp. 497-527.

[i.24] D. Unruh: "Collapse-binding quantum commitments without random oracles". In Advances in Cryptology-ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II 22 (pp. 166-195). Springer Berlin Heidelberg.

[i.25] J. Czajkowski, et al.: "Post-quantum security of the sponge construction". In International Conference on Post-Quantum Cryptography (pp. 185-204). Cham: Springer International Publishing.

[i.26] S. Fehr: "Classical proofs for the quantum collapsing property of classical hash functions". In Theory of Cryptography: 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II 16 (pp. 315-338). Springer International Publishing.

[i.27] M. Zhandry: "New constructions of collapsing hashes". In Annual International Cryptology Conference (pp. 596-624). Cham: Springer Nature Switzerland.

[i.28] J. Czajkowski: "Quantum Indifferentiability of SHA-3". In IACR Cryptol. ePrint Arch. 2021.

[i.29] T. Saito et al.: "Tightly-secure key-encapsulation mechanism in the quantum random oracle model". IACR Cryptology ePrint Archive report 2017/1005. 2017.

[i.30] N. Bindel et al.: "Tighter proofs of CCA security in the quantum random oracle model". In TCC 2019, Part II, volume 11892 of LNCS, pp. 61-90. Springer, Heidelberg, December 2019.

[i.31] J. Håstad: "Solving simultaneous modular equations of low degree". SIAM J. Comput., 17(2): pp. 336-341, 1988.

[i.32] R. Cramer and V. Shoup: "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack". SIAM Journal on Computing 33(1), pp. 167-226. 2003.

[i.33] K. Hövelmanns et al.: "Generic authenticated key exchange in the quantum random oracle model". In PKC 2020. LNCS, vol. 12111, pp. 389-422. Springer, Cham (2020).

[i.34] U. Maurer et al.: "Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology". In Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings, volume 2951 of Lecture Notes in Computer Science, pp. 21-39. Springer, 2004.

[i.35] T. Carstens et al.: "On quantum indifferentiability". IACR Cryptol. ePrint Arch., 2018: pp. 257, 2018.

[i.36] T. Ristenpart et al.: "Careful with composition: Limitations of the indifferentiability framework". In Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings, volume 6632 of Lecture Notes in Computer Science, pp. 487-506. Springer, 2011.

[i.37] J. Coron et al.: "Merkle-Damgård Revisited: How to Construct a Hash Function". In Advances in Cryptology CRYPTO 2005, volume 3621, pp. 430-448. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005. Series Title: Lecture Notes in Computer Science.

[i.38] M. Zhandry: "How to construct quantum random functions". In 53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012, pp. 679-687. IEEE Computer Society, 2012.

[i.39] O. Goldreich et al.: "How to construct random functions (extended abstract) ". In 25th Annual Symposium on Foundations of Computer Science, West Palm Beach, Florida, USA, 24-26 October 1984, pp. 464-479. IEEE Computer Society, 1984.

[i.40] H. Kuwakado and M. Morii: "Quantum distinguisher between the 3-round feistel cipher and the random permutation". In IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings, pp. 2682-2685. IEEE, 2010.

[i.41] H. Kuwakado and M. Morii: "Security on the quantum-type even-mansour cipher". In Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012, pp. 312-316. IEEE, 2012.

[i.42] D. Boneh and M. Zhandry: "Quantum-secure message authentication codes". In Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings, volume 7881 of Lecture Notes in Computer Science, pp. 592-608. Springer, 2013.

[i.43] M. Kaplan et al.: "Breaking symmetric cryptosystems using quantum period finding". In Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II, volume 9815 of Lecture Notes in Computer Science, pp. 207-237. Springer, 2016.

[i.44] NIST: "Post-Quantum Cryptography Standardization - Post-Quantum Cryptography". Csrc.nist.gov. 3 January 2017. Retrieved 24 November 2023.

[i.45] E. Fujisaki et al.: "RSA-OAEP is secure under the RSA assumption". J. Cryptology, 17(2): pp. 81-104, 2004.

[i.46] E. Ebrahimi: "Post-quantum Security of Plain OAEP Transform". In Public-Key Cryptography - PKC 2022. PKC 2022. Lecture Notes in Computer Science, vol 13177. Springer, Cham.

[i.47] C. Peikert: "Lattice cryptography for the Internet". Cryptology ePrint Archive, Report 2014/070, 2014.

[i.48] J. Coron et al.: "GEM: A generic chosen-ciphertext secure encryption method". In CT-RSA 2002, volume 2271 of LNCS, pp. 263-276. Springer, Heidelberg, February 2002.

[i.49] M. Bellare and P. Rogaway: "Optimal Asymmetric Encryption -- How to encrypt with RSA (Extended abstract) ". In Advances in Cryptology - Eurocrypt '94 Proceedings, Lecture Notes in Computer Science Vol. 950, A. De Santis ed, Springer-Verlag, 1995.

[i.50] J. Czajkowskiet al.: "Quantum Indifferentiability of SHA-3". IACR Cryptol. ePrint Arch., 192.

[i.51] D. Unruh: "Universally Composable Quantum Multi-party Computation". In Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings (pp. 486-505). Springer.

[i.52] A. Fiat and A. Shamir: "How to prove yourself: Practical solutions to identification and signature problems". In Advances in Cryptology - CRYPTO' 86, pp. 186-194.