ETSI GR QSC 006 V1.1.1 (2017-02)

Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes

Reference
DGR/QSC-006

Keywords
cyber security, 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

Contents

Intellectual Property Rights

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.

Executive summary

The present document analyses the impact of a quantum computer on symmetric cryptographic primitives. A worst-case estimate is derived for the maximum available quantum computing power in 2050. This leads to the conclusion that 256-bit symmetric ciphers and hash functions will still be unbroken in 2050.

Introduction

A quantum computer will require an enormous change in the cryptographic landscape [i.7]. This is why research and standardization effort is put into finding quantum-safe asymmetric alternatives for RSA, (EC) Diffie-Hellman, and (EC)DSA. Significant effort from industry will be put into preparing for the necessary transition to these new asymmetric primitives.

However, symmetric primitives like AES, SHA-2, and SHA-3 are equally integrated into the numerous information security solutions that exist worldwide. Since a quantum computer can also speed up attacks on symmetric primitives [i.6], it is important to analyse how long these symmetric primitives - and their most-used key sizes - will remain secure.

The present document studies the long-term security of symmetric primitives such as AES-256, SHA-2, and SHA-3. A scientific approach shows that attacks cannot continue to improve at an exponential rate forever. Moore's Law may assert that transistors become twice as small roughly every 1,5 years, but this trend cannot continue and in fact has already stopped. While it is unknown whether a similar trend will appear for quantum computers, it is possible to put an upper bound on the quantum computing power that could be developed in the foreseeable future. The analysis in the present document is based on conservative assumptions and estimates. This does not result in exact dates on when each primitive will be broken, but it does assert their security for at least a certain period of time.

The present document concludes that there are existing and widely used symmetric (AES-256) and hash primitives (SHA-2 and SHA-3 with an output length of at least 256 bits) that will withstand quantum computer attacks until way after 2050. It is reassuring to know that for these symmetric primitives there is no need to find and heavily scrutinize alternatives within the next few years, like is done for the asymmetric primitives.

Note that this does not mean that there is no need to look into symmetric algorithms when it comes to the threat of a quantum computer. On the contrary, industry does have to worry about symmetric algorithms, since there are billions of devices in the world that rely on a symmetric cipher with a key length of 128 bits or less. Examples include mobile communication with e.g. GSM or TETRA. Unfortunately, the calculations that are used in the present document to assert that AES-256 will remain secure until way after 2050 cannot be used to predict when a quantum computer can attack AES-128, or any other cipher with a short key length. Therefore, industry is advised to identify where their products rely on smaller key and hash output lengths, and to start investigating the necessary steps for a transition to primitives with key lengths that will withstand quantum computer attacks like the ones investigated in the present document.

1 Scope

The present document gives information on the long-term suitability of symmetric cryptographic primitives in the face of quantum computing.

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] AI Impacts (March 2015): "Trends in the cost of computing".

NOTE: Available at http://www.aiimpacts.org/trends-in-the-cost-of-computing.

[i.2] Thomas Monz et al (2011): "14-Qubit Entanglement: Creation and Coherence", Phys. Rev. Lett. 106, 130506.

[i.3] Christof Zalka: "Grover's quantum searching algorithm is optimal", Phys. Rev. A 60, 2746, 1999, arXiv.

NOTE: Available at http://www.arxiv.org/abs/quant-ph/9711070.

[i.4] PriceWaterhouseCoopers, The world in 2050 (February 2015): "Will the shift in global economic power continue?".

NOTE: Available at www.pwc.com/gx/en/issues/the-economy/assets/world-in-2050-february-2015.pdf.

[i.5] World Bank, Data: "Research and development expenditure" (% of GDP).

NOTE: Available at http://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS.

[i.6] Lov K. Grover: "A fast quantum mechanical algorithm for database search", STOC 1996, pp 212-219, ACM 1996.

[i.7] Peter W. Shor: "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM Journal on Computing, 26(5):1484-1509, 1997.

[i.8] Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt (December 2015): "Applying Grover's Algorithm to AES: quantum resource estimates".

[i.9] Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, and John Schanck (March 2016): "Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA3".

[i.10] Marc Kaplan, Gactan Leurent, Anthony Leverrier, and María Naya-Plasencia (February 2016): "Breaking symmetric cryptosystems using quantum period finding".