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

GROUP REPORT

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

Disclaimer

The present document has been produced and approved by the Quantum-Safe Cryptography (QSC) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

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

Important notice

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

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

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

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

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

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

Modal verbs terminology

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

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

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".

[i.11] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger (2013): "Biclique analysis of the full AES".

[i.12] Daniel J. Bernstein (May 2009): "Cost analysis of hash collisions: will quantum computers make SHARCS obsolete?".

[i.13] Simon J. Devitt, William J. Munro, and Kae Nemoto (June 2013): "Quantum Error Correction for Beginners", Rep. Prog. Phys. 76 (2013) 076001, arXiv:0905.2794.

[i.14] European Commission D-G for Research and Innovation: "Global Europe 2050", European Union 2012, DOI: 10.2777/79992.

[i.15] Arjen K. Lenstra and Eric R. Verheul (2001): "Selecting Cryptographic Key Sizes", Journal of Cryptology 14, 4, pp 255-293, Springer Berlin Heidelberg.

[i.16] Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland (September 2012): "Surface codes: Towards practical large-scale quantum computation", Phys. Rev. A 86, 032324.

3 Symbols and abbreviations

3.1 Symbols

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

$	US Dollar
d	days
EHz	exahertz
h	hours
Hz	hertz
nm	nanometre
PHz	petahertz
pm	picometre
y	years

3.2 Abbreviations

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

AES	Advanced Encryption Standard
DSA	Digital Signature Algorithm
EC	Elliptic Curve
EU	European Union
GDP	Gross Domestic Product
GSM	Global System for Mobile communications
MAC	Message Authentication Code
MIPS	Million Iterations Per Second
QC	Quantum Computer
QEC	Quantum Error Correction
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
TETRA	Terrestrial Trunked Radio
USA	United States of America

4 Background

4.1 Asymmetric cryptography and quantum computing

If a large quantum computer is built, it would pose a threat to several cryptographic primitives. Most notably, RSA, (EC) Diffie-Hellman, and (EC)DSA would be completely broken by Shor's algorithm [i.7]. Here completely broken means that, given complete quantum control over a sufficient number of qubits, a reasonable size (O(n^3)) quantum circuit can break the underlying mathematical problem in reasonable (O(n^3)) time for a private key of O(n) bits. This ignores the fact that the cryptographic primitive needs to be implemented in a quantum circuit and also ignores *quantum error correction* (QEC) to avoid decoherence. Both would introduce a polynomial overhead. QEC is a technique that allows stable computation with unstable qubits. Since reading out qubits destroys their quantum properties this technique is more involved than normal error correction techniques. QEC introduces a significant overhead in the circuit size and computation time [i.8], [i.9]. Most types of qubits tend to be unstable so it seems likely that QEC will be needed in a large quantum computer. For a more in-depth treatment of QEC see [i.13].

4.2 Symmetric cryptography and quantum computers

For symmetric algorithms the impact of quantum computers is less clear. A rule of thumb says that Grover's algorithm effectively halves the key size for these algorithms [i.6]. However, the aforementioned 'polynomial overhead' considerably increases the complexity of this algorithm: breaking a 128-bit AES key costs about 2^{87} gates and takes the time of 2^{81} gate operations [i.8] rather than 2^{64} operations predicted by the rule of thumb. Finding pre-images for SHA-2 and SHA-3 also has a considerable overhead, costing the time equivalent to 2^{166} hash function calls for both SHA-2 and SHA-3 [i.9], where the rule of thumb would predict 2^{128}. The footprint of QEC further increases the number of qubits from a few thousand to more than 10 million [i.9]. Since [i.8] attempts to minimize the number of qubits, while [i.9] attempts to minimize the T-gate depth, different qubit and operation counts can be obtained for different implementations.

Existing symmetric algorithms might be vulnerable to other quantum attacks. For example [i.10] demonstrates that several MAC and authenticated encryption modes can be broken with a quantum computer if an attacker has access to a *quantum implementation* of the primitive and can query it with *superpositions*, which seems quite a strong assumption. The present document assumes the use of algorithms that have no structural weaknesses that can be exploited by a (quantum) adversary. This means that breaking such an algorithm is the same as solving the general search problem.

Grover's algorithm is optimal for solving the general search problem. It solves the general search problem on a set of size N in $O\left(\sqrt{N}\right)$ time, while no quantum algorithm exists that solves this problem faster [i.3]. In addition, implementing Grover's algorithm in parallel results in a classical time-memory trade-off: m quantum computers can solve the general search problem in no less than $O\left(\sqrt{N/m}\right)$ time, which can trivially be achieved by partitioning the problem into m problems of size N/m. The total cost of this parallel computation is $O\left(\sqrt{Nm}\right)$ so it is more efficient not to parallelise the computation. As an example, one quantum computer could find a 256-bit AES key in about 2^{128} time, while 2^{32} parallel quantum computers could find this key in about 2^{112} time. The overall cost of the latter computation is about 2^{144} which is much more than the 2^{128} cost of the single quantum computer. Nevertheless, parallelisation might still be a sensible choice because no adversary is willing to wait longer than a few years for a decryption.

4.3 Number of qubits

As stated before, possibly millions of physical qubits are needed to break a 256-bit symmetric key. In classical computers, the amount of available memory also follows a version of Moore's Law. For the number of qubits a different behaviour is expected.

While qubits can be built, the main challenge is creating qubits that are both stable, and can be used for quantum computations. The world record of 14 entangled qubits was set in 2011 [i.2]. Significant progress in this area is not expected until a stable logical qubit is created. This stable qubit could be constructed from multiple physical qubits using error correction, or it could be inherently physically stable. Once this is achieved, the number of qubits can grow very rapidly. There is no reason to expect that this growth is limited by Moore's Law, or at least not until millions or billions of qubits have been reached. Therefore, once stable qubits are available, the number of qubits is not a limiting factor for any cryptographic attacks.

4.4 Outline of the present document

Assuming a symmetric algorithm is used without structural weaknesses and that the algorithm is not implemented as a quantum random oracle, can it be broken by a quantum computer? What key lengths are safe to use? What if qubits become more stable and QEC techniques are improved? What if Moore's Law applies to quantum computers? The present document positively answers these questions based on worst-case assumptions. Two scenarios are analysed in clause 5: this clause estimates the capabilities of the fastest quantum computer that could ever be built, and it gives an optimistic estimate of the commercially available quantum computing power around 2050. Clause 6 analyses which key sizes are still safe in 2050, and clause 7 gives the conclusions. All examples will focus on finding a 256-bit symmetric key, but general expressions will be derived to address general key sizes of *k* bits.

5 Quantum computers in 2050

5.1 Approach

This clause analyses two scenarios for quantum computers: the *commercial quantum computer* and the *worst case quantum computer*. The *commercial quantum computer* is a very optimistic estimate of a quantum computer that could be commercially available in 2050. It is much faster than today's regular computers, costs about the same, and needs only a single clock cycle per Grover iteration. Its qubits are arranged on a flat surface and its computations are kept stable with QEC. The *worst case quantum computer* is a special-purpose extremely optimized quantum computer where the qubits are inherently stable and QEC is not needed. Its qubits are packed together as closely as possible to maximize the clock speed.

For each type of quantum computer, its cost is estimated by a version of Moore's Law. Assuming that an attacker has a limited budget this gives an upper bound for an attacker's computing power. This upper bound is used in clause 6 to derive which symmetric key sizes are safe for the foreseeable future.

5.2 Moore's Law

Moore's Law is a well-recognized trend that enables making rough estimates of future computing power. Current technology is reaching the limits of Moore's Law. Some further miniaturization may be possible through clever engineering, but transistors cannot be made smaller than the size of a single atom. Even that size will not be reached, because transistors rely on bulk behaviour, which is only possible in systems that are significantly larger than the single atom scale.

Vendors are shipping their products with an increasing number of processing cores to keep up the illusion of Moore's Law. Due to cheaper production techniques this can be done without a significant increase in product price. So the processing power per dollar still manages to follow Moore's Law. According to [i.1] the processing power per dollar follows the following equation:

$$\text{MIPS/\$ (year)} = 10^{-360{,}109288 + \text{year} * 0{,}178929} \qquad (1)$$

In other words: Moore's Law will cease to be an accurate measure of processing power per square millimetre of silicon but may remain relevant when estimating the processing capability per dollar in the future. Since Grover's algorithm does not parallelise well, clock speeds are also relevant. Commercial chips have increased their clock speed for decades, but are now stagnating around a maximum of about 4 GHz. THz clock speeds are achievable, but these are hard to realize in practice because they require more heat dissipation. Therefore, these speeds do not seem interesting for commercial applications. Increasing clock speeds even further, beyond the THz regime, is currently inconceivable but not fundamentally impossible.