ETSI GR QSC 004 V1.1.1 (2017-03)

GROUP REPORT

Quantum-Safe Cryptography; Quantum-Safe threat assessment

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-004

Keywords

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.

Introduction

Quantum Computers (QC) represent a paradigm shift in computing and the result of having any quantum computer of reasonable size, and availability, is that the existing hard problems upon which the asymmetric cryptography domain is built will not be considered hard anymore. The simple result is that asymmetric cryptography, using Elliptic Curves, or number factorization, will be invalidated. Similarly, there will be an impact on the security level afforded by symmetric cryptographic schemes. Much of the this is well known and documented in ETSI's White Paper [i.2], and in the ETSI Guide on the impact of quantum computing on business continuity [i.4] and many other places. The purpose of the present document is to expand a little on the previous publications in this field but with a general reflection that the concern (worry) regarding a quantum computing attack is not going to have the same impact across all users of quantum vulnerable cryptography.

The present document gives a very simplified consideration of the attack likelihood for when a viable QC exists and reflects that risk against the business sectors' requirements, in order to know how to use cryptographic technology in the sector. This is used to assist industry in determining how long they have to respond to the availability of QC and retain trust and security in their operations.

1 Scope

The present document presents the results of a simplified threat assessment following the guidelines of ETSI TS 102 165-1 [i.3] for a number of use cases. The method and key results of the analysis is described in clause 4.

The present document makes a number of assumptions regarding the timescale for the deployment of viable quantum computers, however the overriding assertion is that quantum computing will become viable in due course. This is examined in more detail in clause 5.

The impact of quantum computing attacks on the cryptographic deployments used in a number of existing industrial deployment scenarios are considered in clause 7.

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 Quantum Safe Cryptography V1.0.0 (2014-10): "Quantum Safe Cryptography and Security; An introduction, benefits, enablers and challenges"; ISBN 979-10-92620-03-0.

[i.2] Selecting Cryptographic Key Sizes, Arjen K. Lenstra and Eric R. Verheul, Journal Of Cryptology, vol. 14, p. 255-293, 2001.

[i.3] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.4] ETSI EG 203 310 (V1.1.1): " CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.5] ISO/HL7 21731:2014 Health informatics -- HL7 version 3 -- Reference information model -- Release 4.

[i.6] Digital Living Network Alliance: DNLA Guidelines.

NOTE: Available from http://www.dlna.org/guidelines/

[i.7] Advanced Access Content System (AACS): Introduction and Common Cryptographic Elements.

NOTE: Available from http://www.aacsla.com/specifications/specs091/AACS_Spec_Common_0.91.pdf

[i.8] ETSI TS 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".

3 Abbreviations

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

AACS	Advanced Access Control System
AACSLA	Advanced Access Content System Licensing Authority
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
CA	Certificate Authority
CAM	Co-operative Awareness Message
CIA	Confidentiality Integrity Availability
DEM	Event Notification Message
DH	Diffie Hellman
DHCP	Dynamic Host Configuration PRotocol
DLNA	Digital Living Network Alliance
DSA	Digital Signature Algorithm
DTCP	Digital Transmission Content Protection
DTLA	Digital Transmission Licensing Authority
DTS	Datagram TLS
EAP	Extensible Authentication Protocol
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithms
EV	Extended Validation (Certificate)
HRNG	Hardware Random Number Generator
ICT	Information & Communication Technology
IKE	Internet Key Exchange
IP	Internet Protocol
ITS	Intelligent Transport System
ITS-S	Intelligent Transport System Station
LAN	Local Area Network
MAC	Message Authentication Code
PKI	Public Key Infrastructure
QC	Quantum Computer or Quantum Computing
QSC	Quantum-Safe Cryptography
RSA	Rivest Shamir Adleman
TCP	Transmission control Protocol
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAP	Wi-Fi Protected Access
XML	eXtensible Markup Language

4 Overview of approach to threat assessment

Threat assessment in most environments consider 2 metrics: Likelihood of an attack and impact of the attack. Underlying these metrics are a further set of metrics addressing such issues as availability requirements (i.e. time needed to access the vulnerability), equipment (i.e. the complexity or cost of equipment needed to launch the attack) and so forth which are described in some detail in ETS TS 102 165-1 [i.3]. The calculation of risk is taken most often as the product of likelihood and impact and categorized as high, medium or low (different risk management systems may use more than 3 classifications but ETSI's approach has only considered 3 with a view to defining countermeasures against high and medium risk vulnerabilities).

The considerations behind the security of most cryptographic systems is that the security strength of an algorithm is optimal when the only feasible attack is brute force evaluation of the key space.

ETSI EG 203 310 [i.4] states (with some editorial extensions):

"… if the promise of quantum computing holds true then the following impacts will be immediate on the assumption that the existence of viable quantum computing resources will be used against cryptographic deployments:

- *Symmetric cryptographic strength will be halved, e.g. AES with 128 bit keys giving 128 bit strength will be reduced to 64 bit strength (in other words to retain 128 bit security will require to implement 256 bit keys).*
- *Elliptic curve cryptography will offer no security.*
- *RSA based public key cryptography will offer no security.*
- *The Diffie-Hellman-Merkle key agreement protocol will offer no security.*

NOTE: The common practice is to refer to the key agreement protocol developed by Messrs Diffie, Hellman and Merkle as simply the Diffie-Hellman or DH protocol as the formal recognition of Merkle's role was made after DH became the accepted term.

With the advent of realizable Quantum Computers, everything that has been transmitted or stored and that has been protected by one of the known to be vulnerable algorithms, or that will ever be stored or transmitted, will become unprotected and thus vulnerable to public disclosure."

The purpose of threat assessment is, in part, to identify where protective measures should be applied for countering the threat. The quantification of risk assists this by addressing those parts of the system most vulnerable and recommending where countermeasures should be applied. For the specific case of the impact of quantum Computing on the security of ICT systems as addressed by ETSI EG 203 310 [i.4] the broad assertion for business continuity is that systems have to be developed and deployed to be crypto-agile. The intent is to ensure that processes are in place that allow algorithms and keys to be changed across the business quickly enough to counter the viable introduction of quantum computers.

The factors to be considered in assessment of the likelihood element in determining the potential of an attack are the following:

- System knowledge:

  For the majority of crypto-systems under consideration, it should be assumed that the algorithms are public knowledge (e.g. RSA, ECC (various modes)).

- Time:

  For those systems open to attack by quantum computing, it is assumed that no new vulnerability is exposed, rather than a quantum computer invalidates the core assertion of a solution to the underlying problem is infeasible without access to the key itself. Thus the time factor for access to material to retrieve the private key of an asymmetric pair is treated as essentially null (using the formulation given in ETSI TS 102 165-1 [i.3] the term is "an attack can be identified or exploited in less than an hour").

- Expertise:

  There is comparatively little expertise in the programming of quantum computers even if some algorithms, like Shor's and Grover's, have been well described. However, the ability to take the data from a public key certificate and feed it into a well-defined instance of Shor's algorithm and to retrieve the private key is likely to be trivial and to tend towards the laymen end of the expertise scale.

- Opportunity:

  Only access to the public key certificate is required and this is public by default, hence there is no barrier to opportunity to the input data to an attack.

- Equipment:

  Assuming access to the input data, the barrier to breaking existing asymmetric cryptography is the existence of a viable quantum computer. For the current assessment equipment has to be categorized as at least specialized, more likely bespoke, and expensive. However there are schemes where public access to a shared quantum computer will be made available which may reduce the assessment to simply that of specialized.

The assessment of impact for any attack on cryptographic tools that a business is reliant upon is assessed as high - the dependent parties are unable to continue to operate securely. Taking account of the assessment factors above, and the impact assessment outlined in ETSI EG 203 310 [i.4], the risk to systems should be considered as critical (using the terminology of ETSI TS 102 165-1 [i.3]). However, in the absence of a quantum computer, an attack that reveals the private key, given only knowledge of the public key certificate, is infeasible with the current level of understanding. Thus the threat assessment to any vulnerable algorithm and protocol can be restricted to only understanding the timeline for deployment of a viable quantum computer that can address the factoring of very large numbers. Further consideration of the time factor is illustrated in ETSI EG 203 310 [i.4] to consider the time for which systems will be vulnerable by considering the time required to arrive at a QC safe deployment of cryptography:

- X = the number of years the public-key cryptography needs to remain unbroken.
- Y = the number of years it will take to replace the current system with one that is quantum-safe.
- Z = the number of years it will take to break the current tools, using quantum computers or other means.
- T = the number of years it will take to develop trust in quantum-safe algorithms.

If "X + Y + T > Z" any data protected by that public key cryptographic system is at risk and immediate action needs to be taken. The Y factor is very dependent on the nature of the cryptographic deployment. Similarly, the X factor is dependent on the nature of the data being protected with some data (e.g. eHealth records) requiring protection for decades, whereas signalling data (e.g. DHCP derived IP addresses) may only require protection for a few minutes (e.g. the lease period of a DNCP derived IP address).

Some assessment is made for values to assign to the "Y" factor in clause 7. The core message however is that even with crude assessments the sum of X, Y and T will exceed Z if a viable large scale quantum computer is available in 15 or 20 years.

5 Assessment of Quantum Computing timetable

5.1 Overview

There are many approaches to quantum computation, including super-conducting qubits, ion traps, nuclear magnetic resonance, quantum annealing and others. The purpose of the present document is not to assess the relative strengths and weaknesses of each of these approaches, in particular in relation to maintenance of the support to the security suite of CIA capabilities offered by cryptography. Whilst in mid-2016 quantum computers indeed exist, they are sufficiently under-powered that they are unable to solve complex cryptographic problems in reasonable periods of time and thus pose no threat to information security at present, it is already possible to observe their efficiency in solving certain classes of mathematical problems. This is to say that for certain types of math problems, even small quantum computers are claimed to be far more efficient than conventional computers although some experts dispute such findings.

There is no guarantee of the time at which quantum computing will become viable, and in particular for addressing the key algorithms that are suggested to make existing public key (asymmetric) cryptography obsolete. Thus the timetable for a viable quantum computer to implement each of Shor's and Grover's algorithms is the purpose of this assessment. Based on available knowledge (see also the assessment given in ETSI's Quantum Cryptography white paper [i.1]) this will be within 15 years of publication of the present document, thus in approximately calendar year 2031.

The more difficult question is how many qubits are required for a viable quantum computer to be used against cryptographically protected data? The comparison of quantum computers to classical computers is not quite straightforward either. The general view is that an n-bit QC can work on 2^n states simultaneously whereas a classical computer can work on $2n$ states but there are many doubts regarding that view and the practicality of the calculation. For real time recovery of the private key from asymmetrically encrypted data with knowledge of the public key it is widely reported that for keys of size n a QC with at least n-qubits is required. However, one of the other questions is how vulnerable is data that has been encrypted with asymmetric keys to any form of attack via QC (i.e. not just a real time attack but an attack on data that has been captured and stored in its encrypted form in order to decrypt it when large-scale fault-tolerant quantum computing resources are available)?

5.2 QC requirements for Shor's algorithm

Shor's algorithm consists of two parts:

- A reduction, which can be done on a classical computer, of the factoring problem to the problem of order-finding.

- A quantum algorithm to solve the order-finding problem.

It should be noted that actual implementations of Shor's algorithm are few and they have not been able to prove themselves against large numbers. It is reported that Shor's algorithm has successfully factored numbers 15 (in the year 2001 using a 7-qubit machine), and 21 (in the year 2012 using a 12-qubit machine) with a true quantum computer. Thus it can be reasonably asserted that Shor's algorithm is implementable and works, what cannot be reasonably asserted for now is the ability to build a realistic machine to work with large numbers.

5.3 QC requirements for Grover's algorithm

Grover's algorithm is a search algorithm against an abstract database where for a given search input a given discrete output will be given. The impact of Grover's algorithm is generally considered a giving an increase in search times of N^2 such that a suitably sized QC will cut the time required to perform a brute force attack on key space will be substantially reduced (the crude figures suggest that the effective key size will be cut in half, from (say) 128 bits to 64 bits. There are a number of ways of assessing the number of qubits required to search a particular space but the general assertion is based on the idea that n bits can index 2^n items. A classical computer with n bits of memory can search through all 2^n inputs, using at most 2^n calls. A quantum computer with n qubits of memory can search through all 2^n inputs using at most $\sqrt{}2^n = 2^{n/2}$ calls.

More qubits means a faster search but as for Shor's algorithm whilst it can be asserted that Grover's algorithm is implementable and works it is unreasonable to assert when a large n qubit machine will exist that will outstrip current brute force search.

6 Threat assessment against aspects of QC deployments

6.1 Algorithm vulnerabilities

6.1.1 Overview

As stated in clause 4, it is seen that the cryptographic techniques that are in use today are vulnerable to the attacks using quantum computers.

Clause 4 lists symmetric cryptographic algorithms and three public key cryptosystems, Rivest-Shamir-Adelman (RSA), Elliptic Curve Cryptosystem (ECC), and Diffie-Hellman (DH). Symmetric cryptographic algorithms typically include block ciphers, stream ciphers, and hash algorithms.

Attacks by quantum computers using Grover's algorithm or Simon's algorithm are believed to reduce the security of symmetric algorithms. These quantum algorithms enable more efficient search to find the secret key, collisions, and pre-image.

Public key cryptography is also known to be vulnerable to the quantum attacks using Shor's algorithm. Shor's algorithm enables quantum computers to calculate private key, which is secret, from the public key efficiently.

6.1.2 Symmetric algorithms

For symmetric ciphers, i.e. block ciphers and stream ciphers, the quantum attack focuses on finding the secret symmetric key. Grover's algorithm shows that it is possible for a scalable quantum computer to speed up the search. Furthermore, when certain structure exists in a symmetric cipher, Simon's algorithm can be applied to improve the search. Although theoretical speed up is deemed twice, in reality, it may not be as much due to the implementation challenges. However, with conservative measures, it is recommended to double the key size to cope with quantum attacks.

For hash algorithms, the goal of attacks may be to find collision or pre-image. In the use of hash algorithm where pre-image resistance is required, such as pseudo random generation, it is deemed sufficient if the output size is doubled. In the use where collision resistance is required, such as message digest computation of a digital signature algorithm, it is already known that the output size has to be doubled even in the classical settings. Therefore, in order to achieve quantum resistance, the output size has to be four times larger. However, it should be noted that by introducing randomization, requirement of hash algorithms can be reduced from collision resistance to second pre-image resistant. Thus, addition of randomization will allow the output size to be only twice as large.

Compared with the quantum vulnerabilities of public key cryptography discussed in clause 6.1.3, symmetric cryptography algorithms seem more resistant against quantum attacks because it simply requires the key and output sizes to be doubled.

6.1.3 Public key cryptography

RSA bases its security on the difficulty of integer factorization. Currently, the best known classical attack is number field sieve, which reduces the attack complexity to sub-exponential time, which is faster than the ideal exponential time.

It is understood that integer factorization can be solved in polynomial time by using Shor's algorithm. Although the size of constant may actually have some impact on the actual time for calculation, polynomial time implies that it can be solved in short amount of time such that increase of key size does not help as much. Due to this, it is deemed dangerous to use algorithms that can be solved in polynomial time. Thus, such a quantum attack invalidates the security of RSA.

DH algorithm and Digital Signature Algorithm (DSA) base their security on the difficulties of integer discrete logarithm. Similar to RSA, the best known classical attack is number field sieve. Often the same approach such as number field sieve applies to both integer factorization and integer discrete logarithm. Since number field sieve is applicable, an integer discrete logarithm problem can be solved in sub-exponential time. For quantum attacks, Shor's algorithm allows to solve the problem in polynomial time, which invalidates the security.

Algorithms of ECC such as ECDH and ECDSA base their security on the difficulty of elliptic curve discrete logarithm. Unlike integer discrete logarithm, no sub-exponential time attack by classical computers has been found. Thus the attack complexity of ECC remains to be exponential time. Unfortunately, Shor's algorithm is also applicable to the elliptic curve discrete logarithm. Thus, the complexity is reduced to polynomial time, invalidating ECC security as well.

In conclusion, quantum attacks can invalidate security of currently used public key cryptography. Thus, it is necessary to introduce different public key cryptography that resists attacks by quantum computers.

6.1.4 Random number generation

Random number generation is a critical component to establish cryptographic security. A number of security breaches have been caused by insecure random number generation. In general, a cryptographically secure random number generator consists of good entropy sources, secure conditioner of entropy data, and cryptographic pseudo random number generator.

Security cannot be established without sufficient amount of entropy. In order to collect sufficient amount of entropy within a reasonable amount of time, it is preferred to use a dedicated hardware random number generator (HRNG).