ETSI TR 103 967 V1.1.1 (2025-01)

Cyber Security (CYBER);
Quantum-Safe Cryptography (QSC);
Impact of Quantum Computing
on Symmetric Cryptography

Reference

DTR/CYBER-QSC-0022

Keywords

cyber security, quantum safe cryptography

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 repository.

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.

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 IPR online database.

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™**, **LTE™** and **5G™** logo 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.

1 Scope

The present document gives an overview of the impact of quantum computing on symmetric algorithms such as block ciphers and hash functions. It discusses the practicality of parallelising Grover's algorithm, the effect of limiting quantum circuit depth, and the overhead from quantum error correction.

The present document supplements ETSI GR QSC 006 [i.1] by summarizing quantum resource estimates for attacks against widely used symmetric algorithms with reasonable circuit depth assumptions. It also provides guidance on the need to increase symmetric key lengths for a range of different use cases.

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 GR QSC 006: "Quantum-Safe Cryptography (QSC); Limits to quantum computing applied to symmetric key sizes".

[i.2] NIST SP 800-56B Rev. 2: "Recommendation for Pair-Wise Key-Establishment Using Integer Factorization Cryptography".

[i.3] NIST SP 800-56A Rev. 3: "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography".

[i.4] NIST FIPS 186-4: "Digital Signature Standard (DSS)".

[i.5] P.W. Shor: "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35^{th} Annual Symposium on Foundations of computer Science, 1994.

[i.6] C. Gidney and M. Ekerå: "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits". Quantum, 2021.

[i.7] M. Webber, V. Elfving, S. Weidt and W.K. Hensinger: "The impact of hardware specifications on reaching quantum advantage in the fault tolerant regime". AVS Quantum Science, 2022.

[i.8] NIST IR 8413: "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process".

[i.9] NIST FIPS 197: "Advanced Encryption Standard (AES)".

[i.10] NIST FIPS 180-4: "Secure Hash Standard (SHS)".

[i.11] NIST FIPS 202: "SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions".

[i.12] L.K. Grover: "A fast quantum mechanical algorithm for database search". Proceedings 28^{th} Annual ACM Symposium on Theory of Computing, 1996.

[i.13] C. Zalka: "Grover's quantum searching algorithm is optimal". Physical Review A 60.4 (1999).

[i.14] M. Boyer et al: "Tight bounds on quantum searching". Fortschritte der Physik: Progress of Physics 46.4-5 (1998).

[i.15] NIST: "Submission requirements and evaluation criteria for the post-quantum cryptography standardization process".

[i.16] A.G. Fowler et al: "Surface codes: Towards practical large-scale quantum computation". Physical Review A 86.3 (2012).

[i.17] B. Eastin and E. Knill: "Restrictions on transversal encoded quantum gate sets". Physical Review Letters 102.11 (2009).

[i.18] Shin-Yi Lin and Chih-Tsun Huang: "A High-Throughput Low-Power AES Cipher for Network Applications". Asia and South Pacific Design Automation Conference (2007).

[i.19] Kyungbae Jang et al. "Quantum analysis of AES". Cryptology ePrint Archive (2022).

[i.20] Matthew Amy et al. "Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3". International Conference on Selected Areas in Cryptography. Springer 2016, pp. 317-337.

[i.21] Brassard et al.: "Quantum Algorithm for the Collision Problem". Third Latin American Symp. on Theoretical Informatics (LATIN'98), pp. 163-169, 1998.

[i.22] S. Kutin: "Quantum Lower Bound for the Collision Problem with Small Range", THEORY OF COMPUTING, Volume 1 (2005), pp. 29–36.

[i.23] P.C. van Oorschot and M.J. Wiener: "Parallel Collision Search with Cryptanalytic Applications". Journal of Cryptology 12, 1–28 (1999).

[i.24] Y. Oh et al.: "Depth-optimized implementation of ASCON quantum circuit". Cryptology ePrint Archive (2023).

[i.25] Kyungbae Jang et al.: "Improved Quantum Analysis of Speck and LowMC". INDOCRYPT 2022: pp. 517-540.

[i.26] Z. Chen et al.: "Exponential suppression of bit or phase errors with cyclic error correction". In: Nature 595 (July 2021), pp. 383–387.

[i.27] C. Ryan-Anderson et al.: "Realization of real-time fault-tolerant quantum error correction". In: Physical Review X 11 (December 2021).

[i.28] S. Jaques et al.: "Implementing Grover oracles for quantum key search on AES and LowMC". In: Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30. 2020, pp. 280–310.

[i.29] A.G. Fowler, S.J. Devitt and C. Jones: "Surface code implementation of block code state distillation". In: Scientific Reports 3.1 (June 2013).

[i.30] Bravyi and A. Kitaev.: "Universal quantum computation with ideal Clifford gates and noisy ancillas". In: Physical Review A 71.2 (Febuary 2005).

[i.31] D. Litinski: "Magic state distillation: Not as costly as you think". In: Quantum 3 (Dec. 2019), p. 205.

[i.32] BSI: "Status of quantum computer development" v2.0. 2023.

[i.33] L. Lao and B. Criger: "Magic state injection on the rotated surface code". In: Proceedings of the 19th ACM International Conference on Computing Frontiers. 2022, pp. 113–120.

[i.34] C. Gidney et al.: "Yoked surface codes". 2023. arXiv: 2312.04522 [quant-ph].

[i.35] Bathe, B., Anand, R. & Dutta, S.: "Evaluation of Grover's algorithm toward quantum cryptanalysis on ChaCha". *Quantum Inf Process* 20, 394 (2021).

[i.36] Kyungbae Jang et al.: "Quantum Implementation and Analysis of SHA-2 and SHA-3". Cryptology ePrint Archive (2024).

[i.37] Chailloux, A., Naya-Plasencia, M., Schrottenloher, A. (2017): "An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography". In: Takagi, T., Peyrin, T. (eds) Advances in Cryptology - ASIACRYPT 2017. ASIACRYPT 2017. Lecture Notes in Computer Science, vol 10625. Springer, Cham.

[i.38] Bernstein, D. J. (2009): "Cost analysis of hash collisions: will quantum computers make SHARCS obsolete?". In SHARCS'09 Workshop Record (Proceedings 4th Workshop on Special-purpose Hardware for Attacking Cryptograhic Systems, Lausanne, Switzerland, September 9-10, 2009) (pp. 105-116).

[i.39] Bravyi, S., Cross, A.W., Gambetta, J.M. et al.: "High-threshold and low-overhead fault-tolerant quantum memory". Nature 627, 778–782 (2024).

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

circuit depth: number of sequential operations that are performed during the execution of a quantum circuit

circuit width: maximum number of operational qubits required during the execution of a quantum circuit

coherence time: length of time two qubits will remain in an entangled state before the external environment introduces errors

magic state distillation: process for producing quantum states known as 'magic states', which are required to effect particular quantum gates under a given Quantum Error Correction (QEC) scheme

EXAMPLE: When applying the surface code for QEC, magic state distillation is used to produce T-gates, which can then be composed to other more complex gates, such as the Toffoli gate.

oracle function: black box quantum operator that transforms a quantum state $|x\rangle \rightarrow |f(x)\rangle$

qubit (logical): unit of quantum information analogous to a bit in classical computing

qubit (physical): physical device that behaves as a two-state quantum system

surface code: widely studied quantum error correction scheme that lays out physical qubits in a grid of data and measurement qubits to produce a single logical qubit

NOTE: See Annex A.

T-gate: 2-qubit gate that can be composed to produce more complex gates, such as the Toffoli gate

Toffoli gate: 3-qubit gate that is an analogue of the AND gate in classical computing

uncomputation: process of reversing steps in a quantum circuit to cancel out intermediate quantum states that may have been produced during calculations

3.2 Symbols

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

O(f(x))	Big O notation. If g(x) = O(f(x)), then g(x) is bounded above asymptotically by f(x), up to a constant multiple. More precisely, there is some x_0 and some positive value M such that $\lvert g(x)\rvert < Mf(x)$ for all $x > x_0$.
Ω(f(x))	Big Omega notation. If g(x) = Ω(f(x)), then g(x) is bounded below asymptotically by f(x), up to a constant multiple. More precisely, there is some x_0 and some positive value M such that $\lvert g(x)\rvert > Mf(x)$ for all $x > x_0$.
$\lfloor x \rfloor$	Floor of x: the largest integer less than or equal to x.
$\oplus$	Logical exclusive or (XOR) operation.
$\lvert\varphi\rangle$	A ket in bra-ket notation. Denotes a quantum state.

EXAMPLE 1: $\lvert 0\rangle$ denotes a single qubit in the collapsed basis state corresponding to a classical value of '0'.

EXAMPLE 2: $\frac{1}{\sqrt{2}}(\lvert 0\rangle + \lvert 1\rangle)$ denotes a single qubit in equal superposition between the basis states $\lvert 0\rangle$ and $\lvert 1\rangle$.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
ASIC	Application Specific Integrated Circuit
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
NIST	National Institute of Standards and Technology
QEC	Quantum Error Correction
RSA	Public key algorithm invented by Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm

4 Introduction

Traditional public-key algorithms such as RSA [i.2], [i.4], Elliptic Curve Diffie-Hellman (ECDH) [i.3] and the Elliptic Curve Digital Signature Algorithm (ECDSA) [i.4] are known to be vulnerable to polynomial-time quantum attacks via Shor's algorithm [i.5]. It has been estimated that 2048-bit RSA could be broken in 8 hours on a device with 20 million physical qubits [i.6] and that 256-bit ECDSA could be broken in a day on a device with 13 million physical qubits [i.7]. As a consequence, the US National Institute for Standards and Technology (NIST) are currently standardizing the next generation of public-key algorithms [i.8].

Symmetric algorithms such as the AES [i.9] block cipher and the SHA-2 [i.10] and SHA-3 [i.11] hash functions are believed to be immune to Shor. In most cases, the best-known quantum attack uses Grover's algorithm [i.12]. Grover provides a generic square-root speed-up in the number of queries needed in an unstructured search problem (see clause 5.1). This means that Grover could be used to find the 256-bit key for AES-256 with around 2^{128} quantum queries to the AES algorithm compared to the 2^{256} queries expected for classical exhaustion.

However, assessing the cost of Grover in terms of the number of queries to the symmetric algorithm can be misleading. It neglects overheads from:

- The cost of implementing the algorithm queried by Grover as a reversible quantum circuit (see clause 5.2);
- The cost of parallelising Grover so that a solution is found in a reasonable amount of time (see clause 5.3); and
- The cost of quantum error correction so that Grover succeeds with high enough probability (see clause 5.5).

ETSI GR QSC 006 [i.1] argues that 256-bit block ciphers and hash functions will remain secure until at least 2050 by making conservative assumptions about the algorithm implementation, quantum error correction and quantum hardware performance, and then estimating the amount of parallelisation available if an adversary is willing to spend a fraction of their Gross Domestic Product on the attack.

The present document takes a different approach. It estimates the resources required to attack standardized block ciphers (see clause 6.2) and hash functions (see clause 6.3) in a reasonable amount of time using the current state-of-the-art for algorithm implementations and the most well-studied quantum error correction scheme (the surface code).

The present document also considers the impact of other quantum attacks on symmetric cryptography such as quantum collision finding (see clause 7.1) and Simon's algorithm (see clause 7.2). Finally, it includes an assessment of the overall threat to symmetric algorithms from quantum computing and concludes that migration efforts should be focused on asymmetric cryptography (see clause 8).

5 Grover's algorithm

5.1 Overview

Grover's search algorithm is a quantum algorithm that can be applied to generic unstructured search problems to give an asymptotic square-root speed-up over classical algorithms in terms of the number of queries needed. It has been shown to be asymptotically optimal for such problems [i.13].

Let $f: X \to \{0,1\}$ be a function defined on a set X of size $|X| = N$. The unstructured search problem is to find an input value $x \in X$ such that $f(x) = 1$, when the function f does not have any properties that allow the input set to be searched more efficiently than simply evaluating f at values from X. If $f(x) = 1$ for a unique $x \in X$, then it would take classical search algorithms $N/2$ queries on average to find the solution x. Grover's algorithm, on the other hand, will find x with high probability after around $(\pi/4)\sqrt{N}$ quantum queries to f.

NOTE 1: If there are M solutions to $f(x) = 1$, then a classical search algorithm will take $O(N/M)$ queries to f to find any such solution x and Grover's algorithm will find a solution with high probability after $(\pi/4)\sqrt{N/M}$ quantum queries [i.14].

This setup can be applied naturally to the key recovery problem for block ciphers where a matched pair of input plaintext and output ciphertext values is known; that is, where $\mathrm{Enc}(K, P) = C$ for an unknown key K. Let X be the set of all possible key values and define the function $f: X \to \{0,1\}$ by:

$$f(x) = \begin{cases} 1 & \text{if } \mathrm{Enc}(x, P) = C, \\ 0 & \text{otherwise.} \end{cases}$$

EXAMPLE: For AES-128, the set of all possible key values has size $N = 2^{128}$ so Grover's algorithm would require on the order of 2^{64} quantum queries to recover the key.

NOTE 2: Multiple matched input plaintext and output ciphertext pairs might be needed to uniquely determine the key (see clause 6.2.1.3).

However, comparing the headline figures of 2^{128} classical queries with 2^{64} quantum queries neglects significant details of implementing Grover's algorithm on a quantum computer. The remainder of this clause will describe these details and discuss the impact they have on estimating the required resources for an attack.

5.2 Oracle implementation

Grover's algorithm involves iterated queries to the oracle function f, which needs to be implemented on the quantum computer.

The internal state of a quantum computer is often described in terms of qubits; that is, the quantum analogue of bits in a classical computer. A quantum algorithm is then described as a quantum circuit built out of fundamental quantum gates that operate on a few qubits at a time. The depth of a quantum circuit is the maximum number of sequential gate operations that are performed during the computation.

The laws of quantum physics mean that all quantum gates, and all quantum circuits, need to be reversible. This means that while some fundamental classical gates, such as XOR, translate directly to fundamental quantum gates, others, such as AND, do not. Instead, the quantum analogue of the classical AND gate is the 3-qubit Toffoli gate which is in turn constructed from several 1- and 2-qubit gates.

NOTE: The set of fundamental quantum gates supported, and their relative costs, will be dependent on the underlying hardware so optimized implementations will need to be tailored to specific platforms.

The reversibility of quantum circuits also means that any qubits used for intermediate calculations cannot simply be zeroed before re-use or the final measurement step; they need to be carefully uncomputed. This typically involves performing the inverse circuit which adds further overheads to the implementation of the quantum oracle, both in the number of required qubits and the depth of the circuit.

5.3 Parallelisation

In a classical brute force search, the probability of success is directly proportional to the runtime of the search: reducing the runtime by a factor of S reduces the probability of success by the same factor, because the proportion of the input space that can be explored is reduced by a factor of *S*. From a different perspective, the input space could be divided between *S* processors, with each having a probability of success reduced by a factor of *S*. This means that parallelising classical search by increasing the computational resources can reduce the time it takes to find a solution without changing the total amount of work needed.

The same is not true for Grover's algorithm: it finds a solution with high probability in $O\left(\sqrt{N}\right)$ sequential iterations of the oracle function. There are two approaches for parallelising Grover's algorithm: inner and outer parallelisation.

- Inner parallelisation partitions the search space and performs a separate run of Grover's algorithm for each partition. Reducing the runtime by a factor of S allows searching a space of size N/S^2 with high success probability, therefore requiring S^2 processors to search the entire space.

- Outer parallelisation reduces the number of iterations of the oracle function for each instance, reducing the probability of success of each individual instance and increasing the overall number of required instances. For large S, reducing the number of oracle iterations by a factor of S in a Grover run reduces the probability of success by a factor of S^2 [i.13], so it would require S^2 processors to achieve the same overall success probability.

For both approaches, in order to reduce the time it takes to find a solution by a factor of S, it is necessary to increase the computational resources by a factor of S^2. That is, the total amount of work increases as more parallelisation is applied.

One advantage of inner parallelisation is that it reduces the impact of spurious results (see clause 6.2.1.3) since each instance recovers its own potential solution. If the work is partitioned in such a way that the correct key is in a different section of the search space from any spurious results, then it will still be recovered.

5.4 Maximum depth

During a single Grover instance, queries to the oracle function are made sequentially so the time taken to recover a solution depends on the circuit depth for Grover; that is, the maximum number of sequential operations. When estimating the security implications of Grover's algorithm, it is reasonable to place bounds on the length of time an adversary will be prepared to wait. In combination with estimates for plausible cycle times (see clause 5.6), this bounds the maximum depth of a single Grover run.

The total depth of a Grover run can be estimated as the depth of the circuit for a single query multiplied by the number of iterations of the circuit. NIST [i.15] have suggested the following maximum circuit depths achievable under various assumptions:

- 2^{40}, which NIST cl [i.15]aimed approximately corresponded to the number of gates that near-term quantum computing architectures could be expected to serially perform in one year;

- 2^{64}, which NIST cl [i.15]aimed approximately corresponded to the number of gates that current classical computing architectures could perform serially in 10 years; and

- 2^{96}, which NIST cl [i.15]aimed approximately corresponded to the number of gates that atomic scale qubits with speed of light propagation times could perform in 1 000 years.

In later clauses, the overheads introduced by quantum error correction, and estimates for a single cycle time are discussed. Estimating a plausible cycle time of 200 ns [i.16], the following maximum circuit depths are included as useful comparison points: