ETSI TR 104 171 V1.1.1 (2026-03)

TECHNICAL REPORT

Cyber Security (CYBER); Implementation Guidelines for Quantum Random Number Generators

Reference
DTR/CYBER-00163

Keywords
cyber 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

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.

Executive summary

There have been many QRNGs introduced to the commercial market in recent years, each with its own particular set of advantages and limitations. The purpose of the present document is to present a set of reasonable guidelines for implementing Quantum Random Number Generators (QRNGs), and to give the user of such devices a survey of the various characteristics between different implementations. The present document examines each principal aspect of QRNG implementation and discusses in detail the various options and consequences of implementation choices.

Introduction

Random Number Generators (RNGs) are essential in applications requiring security, fairness, and unpredictability. Deterministic Random Number/Bit Generators (DRNGs/DRBGs), also called Pseudo-Random Number Generators (PRNGs), simulate randomness using deterministic algorithms. Physical True Random Number Generators (PTRNGs), on the other hand, rely on indeterministic physical processes to produce statistically random outcomes. Finally, Quantum Random Number Generators (QRNGs), a proper subclass of PTRNGs, exploit inherently quantum phenomena to produce outputs which are not only statistically random but also unpredictable given any prior side-information.

Following, certain key aspects and uses for QRNGs are discussed.

Use cases:

a) Cryptographic Security

Modern cryptography relies on random keys, nonces, and Initialization Vectors (IVs).

Unpredictable random numbers are necessary for:

1) Secure key generation in classical encryption protocols such as RSA, AES and ECC as well as Post-Quantum Cryptography algorithms [i.19] such as ML-DSA, ML-KEM and SLH-DSA.

2) State preparation and/or measurement basis choice in Quantum Key Distribution (QKD) protocols.

b) High-Security Applications

Industries like finance, healthcare, and government communications demand randomness that meets the highest integrity standards. QRNG devices, such as photon-based or vacuum fluctuation-based systems, ensure true unpredictability, essential for long-term security [i.2].

c) Scientific Research and Simulations

QRNGs can provide random sequences critical for high-precision applications, such as Monte Carlo simulations in physics, chemistry, and financial modelling.

Key aspects:

1) Cost and Hardware Requirements

One of the principal obstacles to scaling QRNG technology is the requirement for specialized hardware. Classical hardware-based RNGs are readily available and PRNGs can be implemented purely in software and run on virtually any standard computing device. Instead, QRNGs rely on quantum systems like photon detectors, beam splitters, or quantum vacuum fluctuation detectors to generate random numbers.

These quantum components are currently more expensive to produce and maintain than conventional hardware used for classical RNGs. The higher cost of manufacturing and maintaining QRNG systems limits their use primarily to high-security environments, such as government communications, financial institutions, and military applications, although the learning curve (the inverse-exponential relationship between the number of units built and the number of defects) is reducing the cost of integrated QRNG systems-on-a-chip as the industry goes forward. Today, there are several such commercially available devices being marketed as of 2025.

2) Speed and Throughput

In theory, QRNGs can generate entropy at a significantly higher rate than classical RNGs [i.25]. However, QRNGs have comparatively lower speed and throughput than classical RNGs used in conjunction with a PRNG, because QRNGs are bound by the rate at which quantum phenomena can be measured and processed. Although recent advancements have significantly increased the bit rates of QRNGs - reaching hundreds of megabits per second - they still fall short of the throughput achievable by the combination of classical RNGs and PRNGs, especially in applications that require large volumes of random numbers in real-time, such as large-scale simulations or high-frequency trading.

While significant advancements have improved their speed, QRNGs alone are still currently slower than the classical alternative in use today, High-throughput applications (e.g. simulations) may require hybrid QRNG-PRNG systems, which are in development at the present time.

3) Integration with Existing Systems

Current cryptographic infrastructure is optimized for entropy from classical RNGs that is expanded by PRNGs. Integrating QRNGs requires modifying Hardware Security Modules (HSMs), cryptographic libraries, and communication protocols to accommodate quantum randomness. HSMs are specialized hardware devices designed to safeguard and manage cryptographic keys. QRNGs are increasingly being incorporated into HSMs to improve the quality of the random numbers used for key generation and other cryptographic functions. By using QRNGs, HSMs can provide greater security assurances in environments where cryptographic operations are intended to be highly secure and resistant to attack, such as in financial services, healthcare, and critical infrastructure.

4) Scalability

Miniaturization of QRNG devices is improving, but scaling them for widespread consumer applications (e.g. IoT devices or mobile hardware) remains a challenge. Reducing power consumption and production costs is essential for broader adoption.

5) Lack of interface and control plane standards

There are no generally applicable standards for interface to quantum random generators, and this is a problem that can be solved by participation in a standards body such as ETSI, to make quantum random number generators accessible across a broad base of applications. The industry may want to develop a set of common interface standards or even a common command interface and set of common opcodes for controlling the quantum random number generator and a real-world deployment. Organizations like the National Institute of Standards and Technology (NIST) in the United States are already exploring ways to integrate quantum technologies into cryptographic standards as part of their post-quantum cryptography initiative.

1 Scope

The scope of the present document is limited to discussion of the implementation guidelines and characteristics of Quantum Random Number Generators (QRNGs), with an emphasis on what may require standardization and why. A set of informative annexes is also included in the present document to provide a survey of the current state of the art and some real-world examples and experimental results in order to provide some additional aspects that may be of help to the implementer.

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 may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] Ma, X., Yuan, X., Cao, Z., Qi, B., & Zhang, Z. (2016): "Quantum random number generation", NPJ Quantum Information, 2, 16021.

[i.2] Pironio, S., Acin, A., Massar, S., de la Giroday, A. B., Matsukevich, D. N., Maunz, P. & Monroe, C. (2010): "Random numbers certified by Bell's theorem", Nature, 464(7291), 1021-1024.

[i.3] Sanguinetti, B., Martin, A., Zbinden, H., & Gisin, N. (2014): "Quantum Random Number Generation on a Mobile Phone", Physical Review X, 4(3), 031056.

[i.4] M. J. Applegate, O. Thomas, J. F. Dynes, Z. L. Yuan, D. A. Ritchie, A. J. Shields (2015): "Efficient and robust quantum random number generation by photon number detection", Applied Physics Letters, 107(7).

[i.5] Shen, Y., Tian, L., Zou, H. (2010): "Practical quantum random number generator based on measuring shot noise of vacuum states", Physical Review A, 81(6), 063814.

[i.6] Symul, T., Assad, S. M., & Lam, P. K. (2011): "Real time demonstration of high bitrate quantum random number generation with coherent laser light", Applied Physics Letters, 98(23), 231103.

[i.7] Jofre, M., Curty, M., Fernández, V., Martínez, A., Ortiz, J., Torres, J. P., & Pruneri, V. (2011): "True random numbers from amplified quantum vacuum", Optics Express, 19(21), 20665-20672.

[i.8] Abellán, C., Amaya, W., Mitrani, D., Pruneri, V., & Mitchell, M. W. (2014): "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode", Optics Express, 22(2), 1645-1654.

[i.9] Marangon, D. G., Vallone, G., & Villoresi, P. (2017): "Source-Device-Independent Ultrafast Quantum Random Number Generation", Physical Review Letters, 118(6), 060503.

[i.10] Frauchiger, D., Renner, R., & Troyer, M. (2013): "True randomness from realistic quantum devices", arXiv preprint arXiv:1311.4547.

[i.11] Müller-Quade, J., & Renner, R. (2009): "Composability in quantum cryptography", New Journal of Physics, 11(8), 085006.

[i.12] Tomamichel, M. (2015): "Quantum information processing with finite resources: mathematical foundations", vol. 5, Springer.

[i.13] Senno, G., Strohm, T., & Acín, A. (2023): "Quantifying the intrinsic randomness of quantum measurements", Physical Review Letters, 131(13), 130202.

[i.14] Meng, S., Curran, F., Senno, G., Wright, V. J., Farkas, M., Scarani, V., & Acín, A. (2024): "Maximal intrinsic randomness of a quantum state", Physical Review A, 110(1), L010403.

[i.15] Curran, F., Moradi, M., Senno, G., Stobinska, M., & Acín, A. (2025): "Maximal intrinsic randomness of noisy quantum measurements", arXiv preprint arXiv:2506.22294.

[i.16] Foreman, C., Yeung, R., Edgington, A., & Curchod, F. J. (2025): "Cryptomite: A versatile and user-friendly library of randomness extractors", Quantum, 9, 1584.

[i.17] Zhang, X., Nie, Y. Q., Liang, H., & Zhang, J. (June 2016): "FPGA implementation of Toeplitz hashing extractor for real time post-processing of raw random numbers", In 2016 IEEE™-NPSS Real Time Conference (RT) (pp. 1-5).

[i.18] Quside Technologies: "Quantum Random Number Generators (QRNGs)".

[i.19] NIST FIPS 204: "Module-Lattice-Based Digital Signature Standard", 13 August 2024.

[i.20] NIST SP 800-22 Rev. 1: "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications".

[i.21] ISO/IEC 18031:2025: "Information technology — Security techniques — Random bit generation".

[i.22] NIST SP 800-90A Rev.1: "Recommendation for RNG using Deterministic Random Bit Generators", June 2015.

[i.23] NIST SP 800-90B: "Recommendation for the Entropy Sources Used for Random Bit Generation", January 2018.

[i.24] NIST SP 800-90C: "Recommendation for Random Bit Generator (RBG) Constructions".

[i.25] United Kingdom National Cyber Security Centre (NCSC): "Quantum Networking Technologies". Version 1.0, 5 August 2025.

[i.26] ETSI TS 131 101 (V16.0.0): "Universal Mobile Telecommunications System (UMTS); LTE; 5G; UICC-terminal interface; Physical and logical characteristics (3GPP TS 31.101 version 16.0.0 Release 16)".

[i.27] ETSI TS 131 102 (V18.4.0): "Universal Mobile Telecommunications System (UMTS); LTE; 5G; Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102 version 18.4.0 Release 18)".

[i.28] ETSI TS 131 111 (V16.1.0): "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) (3GPP TS 31.111 version 16.1.0 Release 16)".

[i.29] Santha, M., & Vazirani, U. V. (1986): "Generating quasi-random sequences from semi-random sources", Journal of computer and system sciences, 33(1), 75-87.

[i.30] Van Griensven, Rosas, Pecen: "Quantum Proofing the Economy", Applied Quantum Technologies Institute (AQT) publications, 2025.

[i.31] Matthias Peter, Werner Schindler: "A Proposal for Functionality Classes for Random Number Generators", Version 3.0, 2024.

[i.32] ETSI TS 133 110 (V18.0.0): "Universal Mobile Telecommunications System (UMTS); LTE; Key establishment between a Universal Integrated Circuit Card (UICC) and a terminal (3GPP TS 33.110 version 18.0.0 Release 18)".

[i.33] GSMA™ SGP.25: "eUICC for Consumer and IoT Devices Protection Profile",Version 2.0, 19 December 2023.

[i.34] GSMA™ SGP.22: "RSP Technical Specification", Version 3.1 Final, 01 December 2023.

[i.35] FIPS Pub 140-3: "Security Requirements for Cryptographic Modules", 22 March 2019.

[i.36] BSI 20/31: "A Proposal for Functionality Classes for Random Number Generators", 10 September 2024.

[i.37] ISO/IEC 19790:2025: "Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules", February2025.

[i.38] ISO/IEC 24759:2025: "Information technology — Security techniques — Test requirements for cryptographic modules", Fourth edition 2025.

[i.39] ISO/IEC 20543:2019: "Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408", First edition 2019-10.

[i.40] ISO/IEC 15408-1:2022: "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security", Fourth edition, 2022-08.

[i.41] ETSI GS QKD 014 (V1.1.1): "Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API".

[i.42] Recommendation ITU-T X.1702 (11/2019): "Quantum noise random number generator architecture".

[i.43] IETF RFC 4086: "Randomness requirements for security", June 2005.

[i.44] NIST SP 800-160v1r1: "Engineering Trustworthy Secure Systems".

[i.45] ITU-T Y.3800 series: "Quantum key distribution networks – Role in end-to-end cryptographic services with non-quantum cryptography", November 2023.

[i.46] ISO/IEC 17025:2017: "General requirements for the competence of testing and calibration laboratories", Third edition, 2017-11.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

ACL	Access Control List
ADC	Analog-to-Digital Convertor
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AIS	Additional Information Sequence
ANSSI	Agence nationale de la sécurité des systèmes d'information (French National Agency for the Security of Information Systems)
API	Application Programming Interface
AXI	Advanced eXtensible Interface
BF	Bloom Filter

BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CCCS	Canadian Centre for Cyber Security
CCN	Centro Criptológico Nacional
CPU	Central Processing Unit
DMA	Direct Memory Access
DRBG	Deterministic Random Bit Generator
DRNG	Deterministic Random Number Generator
DSP	Digital Signal Processing
EBF	Element-based sliding Bloom Filter
ECC	Elliptic Curve Cryptography
EMI	Electromagnetic Interference
ENT	Enterprise Network and Telecommunications
EU	European Union
eUICC	Embedded UICC
EZT	Entropy Zero Trust
FIPS	Federal Information Processing Standards (United States)
FPGA	Field-Programmable Gate Array
FPR	Floating Point Register
FRM	Fast Resource Management
FRMs	Faraday Rotator Mirrors
GS	Ground Station
GSMA	GSM Association
HSM	Hardware Security Module
HWRoT	Hardware Root of Trust
ID	Identity
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IID	Independent and Identically Distributed
IoT	Internet of Things
ISO	International Organization for Standardization
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
LED	Light Emitting Diode
LFSR	Linear Feedback Shift Register
LO	Local Oscillator
ML-DSA	Module-Lattice-based Digital Signature standard
ML-KEM	Module-Lattice-based Key-Encapsulation Mechanism standard
NIST	National Institute of Standards and Technology
OS	Operating System
PBF	Partitioned sliding Bloom Filter
PCB	Printed Circuit Board
PCIe	Peripheral Component Interface express
PIN	Personal Identity Number
POVM	Positive Operator-Valued Measure
PPM	Prediction by Partial Matching
PQC	Post-Quantum Cryptography
PQU	Post Quantum Unit
PRNG	Pseudo-Random Number Generator
PSA	Protocol Service Availability
PTRNG	Physical True Random Number Generator
QES	Quantum Entropy Source
QKD	Quantum Key Distribution
QRNG	Quantum Random Number Generator
RBG	Random Bit Generator
RF	Radio Frequency
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman

NOTE: A public-key encryption algorithm.

SLH-DSA	Stateless Hash-Based - Digital Signature Standard

SoC	System on Chip
SP	Special Purpose
SWaP	Size, Weight and Power
TCG	Trusted Computing Group
TPM	Trusted Platform Module
TRNG	True Random Number Generator
UICC	Universal Integrated Circuit Card
UK	United Kingdom
URL	Universal Record Locator
USB	Universal Serial Bus
USB-C	Universal Serial Bus Type-C
VPN	Virtual Private Network

4 Theory of quantum random number generation

4.0 Introduction

The purpose of this clause is to show a theoretical basis for random number generation and what this might mean in practical implementations.

4.1 The definition of randomness

QRNGs are devices that use quantum mechanics' inherent unpredictability to produce *true random numbers*, i.e. numbers that are ϵ-close to being uniformly random and independent of all prior information [i.1] to [i.10].

Definition 1. A QRNG's outcome K is ϵ-*secure* (or ϵ-truly-random) if:

$$D\left(\rho_{KE}, \frac{I}{|K|} \otimes \rho_E\right) \leq \epsilon, \tag{1}$$

where:

1) $\rho_{KE} = \sum p(k)|k\rangle\langle k| \otimes \rho_E^k$ is the classical-quantum state describing the correlations between the classical random variable K and the (in general, quantum) state ρ_E of a potential eavesdropper's system E, where E is considered to be *side-information*.

2) $I/|K|$ is a uniform distribution over strings of length $|K|$ (usually, 2^n for some bit string length n).

3) $D(\sigma, \tau) \coloneqq \frac{1}{2}\|\sigma - \tau\|_1$ is the trace-distance between states σ and τ.

The role of system E, the side-information, in the definition of ϵ-security is to model all degrees of freedom that are, although relevant to the QRNG's operation, outside of the manufacturer (and, hence, of the honest user) control. In other words, these are untrusted sources of stochasticity (or, noise) which influence the QRNG's outcomes. The implicit quantification over all (the continuously) many states ρ_E might seem, at first, to turn this definition impractical. However, as shown next, the *physical modelling* of the device directly provides a way to compute the distance in Eq. (1) for the worst-case ρ_E.

Before moving on, there are two central aspects worth highlighting about the definition of randomness:

1) It is information-theoretical, i.e. without any computational assumption about the eavesdropper's power.

2) By being based on the trace distance, it satisfies the property of *universal composability* [i.11]. In short, this means that any cryptographic protocol (be it classical or quantum) which is ϵ'-secure when taking "ideal" random inputs remains $(\epsilon + \epsilon')$-secure when receiving "real" ϵ-secure inputs.