Technical Reference Standard for Entanglement-Based Quantum Random Number Generator (EQRNG) Protocols

Definitions, Theoretical Concepts, Protocols, Processes, Architectures, Functional Requirements, Technical Implementations, Devices, Operative Principles, Security Models, Conformance Assessments, Use Cases, Randomness Certification, Statistical Randomness Testing, Device Independence and Public Verification Schemes for Entanglement-Based QRNGs

RS-EITCI-QSG-EQRNG-PROTOCOL-STD-VER-2.5

Witold A. Jacak*[1,2], Janusz E. Jacak[1,2], Piotr Jóźwiak[2], Wojciech A. Donderowicz[1], and Lucjan Jacak[1,2]

[1]EITCI Institute, Quantum Standards Group, Belgium
[2]Wrocław University of Science and Technology, Poland

October 31, 2025

Abstract

This Technical Reference Standard specifies terminology, theoretical foundations, protocol families, architectures and functional requirements, technical implementations of devices and their operative principles, security models, conformance assessments, use cases, as well as randomness certification, statistical randomness testing, device independence and public verification schemes for entanglement-based quantum random number generators (EQRNGs), with particular emphasis on protocols enabling *public verification of randomness* without disclosure of underlying secret random bits. The document also consolidates and generalizes the entanglement QRNG with public randomness certification (verification) protocol originally disclosed by Jacak *et al.* in a 2017 WIPO patent application (PV-EQRNG), where multipartite entangled states with random correlation/anticorrelation patterns were proposed to support outsourced statistical testing under preserved secrecy. [1–5] It incorporates subsequent theoretical developments on quantum generators of random numbers and quantum sources of entropy, [6–10] as well as experimental implementations of publicly verifiable QRNGs and certified entanglement-based QRNGs on photonic platforms. [11–14] The scope complements generic random-bit, QRNG and QKD standards such as ISO/IEC 18031, the NIST SP 800-90 series, NIST SP 800-22, ETSI GS QKD 014 (contextual interoperability scope) and ITU–T X.1702, [15–19] by focusing on protocols in which multipartite entanglement is an explicit resource and central to functionality, including device-dependent, semi-device-independent and device-independent realizations. In this reference standard an extended introduction and a detailed clause structure with technically oriented synopses are provided as the basis for a normative referencing of entanglement-based QRNGs and their conformance assessments. In addition, the standard introduces and formalizes the notion of entanglement-level-based reduction of computational complexity in secrecy-preserving statistical randomness verification, showing that increasing the multipartite entanglement degree can effectively collapse the per-bit testing overhead while maintaining the quantitative security guarantees expressed by the standard, aligning with an insight that the multi-qubit entanglement is a key resource underlying computational speed-ups. [20–22]

*Corresponding author: witold.jacak@eitci.org

Contents

Introduction

Background and motivation

Random numbers are a critical primitive in modern information and communication technologies. They underpin cryptographic keys and nonces, authentication tokens, secure communication protocols, privacy-preserving algorithms, randomized algorithms and simulations, distributed consensus mechanisms and many other functions.

Classical pseudo-random number generators (PRNGs) are deterministic algorithms whose outputs appear statistically random when the internal state remains secret and the underlying computational hardness assumptions hold. Their unpredictability is therefore *computational* and can fail if an adversary obtains sufficient side information or if algorithmic weaknesses are found.

True random number generators (TRNGs) based on physical noise sources aim at *information-theoretic* unpredictability. Conventional TRNGs use classical thermal or electronic noise or chaotic analog dynamics, with the random bit generation modelled as a stochastic process whose parameters must be estimated, monitored and periodically revalidated. [8, 9] Their security is limited by how accurately the physical model captures the device behaviour and by the possibility of subtle side channels.

Quantum random number generators (QRNGs) exploit the intrinsic indeterminism of quantum measurement. In a textbook example, a qubit prepared in a superposition

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) \tag{1}$$

and measured in the computational basis produces outcomes 0 and 1 with probabilities $p(0) = p(1) = \frac{1}{2}$. For an ideal implementation, these probabilities are irreducible given the validity of quantum mechanics and no-signalling. Practical QRNGs must, however, contend with imperfect state preparation, detector inefficiencies, classical noise contamination and implementation side channels. [7, 23] Modern analyses therefore quantify the extractable randomness using entropy measures such as min-entropy $H_\infty(X)$ and conditional min-entropy $H_\infty(X|E)$, where E models classical or quantum side information held by an adversary. [7, 24]

Over the last decade, a rich family of QRNG architectures has emerged based on single-photon detection, vacuum fluctuations, phase noise and other microscopic entropy sources. [7–10] In parallel, a hierarchy of trust models has been developed: device-dependent (trusted hardware and model), semi-device-independent (partial trust, constrained by observed statistics) and fully device-independent (DI) QRNGs, where randomness is certified from Bell inequality violations with minimal assumptions. [24–27]

Most deployed QRNGs today are single-system and device-dependent. They can deliver high throughput and good security in well-controlled environments but do not, by themselves, address two important requirements:

- the need for *public assurance* that the random numbers used in critical infrastructures are genuinely random, without revealing the random strings themselves;

- the desire to systematically use *entanglement* not only as a source of entropy but as a structural resource enabling new protocol-level properties.

Historical development and the role of the Jacak entanglement QRNG concept

Entanglement-based QRNGs (EQRNGs) form a subclass of QRNGs in which multipartite entangled states provide the entropy and non-classical correlations that underpin the protocol. The idea that entanglement can be used not only to certify but also to structure randomness was developed in a series of works by Jacak and co-workers.

A key milestone is the 2017 WIPO patent application "Entanglement Quantum Random Number Generator with Public Randomness Certification", [1] which introduced a class of protocols in which measurements on entangled multi-qubit states generate several classical bit strings with rigorously linked statistical properties. One of these strings can be publicly disclosed and subjected to intensive statistical testing, while other strings remain secret but inherit the same randomness profile by construction. This was complemented by a preprint and later by the Scientific Reports article on entangled quantum random numbers generation and certification, [2] and formalized in the first EITCI EQRNG reference standards. [3–5]

The archetypal construction uses a three-qubit generalized Bell state

$$|\Psi_{XAB}\rangle = \frac{1}{2}\big(|000\rangle_{XAB} + |011\rangle_{XAB} + |101\rangle_{XAB} + |110\rangle_{XAB}\big), \tag{2}$$

topologically represented as a three-linked chain. Measuring the auxiliary qubit X in the computational basis collapses the remaining pair (A, B) into either a correlated Bell state $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ or an anticorrelated Bell state $|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, each with probability $\frac{1}{2}$. Repeating this process generates:

- a control string $\boldsymbol{A} = (A_i)$ recording if the pair at position i is correlated or anticorrelated;
- two output strings $\boldsymbol{B} = (B_i)$ and $\boldsymbol{C} = (C_i)$ obtained by measuring the A and B qubits in the computational basis.

In the ideal case the relation

$$C_i = \begin{cases} B_i & \text{if } A_i = 0 \text{ (correlation)}, \\ B_i \oplus 1 & \text{if } A_i = 1 \text{ (anti-correlation)}, \end{cases} \tag{3}$$

holds for every position i, so that $\boldsymbol{B}$ and $\boldsymbol{C}$ are individually uniformly random and statistically indistinguishable, while $\boldsymbol{A}$ encodes a secret pattern of correlations. A user can keep, say, $\boldsymbol{B}$ secret while disclosing $\boldsymbol{C}$ to one or more *Verification Centres* (VCs) that run arbitrarily strong statistical tests (NIST SP 800-22, TestU01 and others). [2, 17, 28] Successful tests on $\boldsymbol{C}$ then imply high entropy for $\boldsymbol{B}$, without revealing its contents.

This *public randomness verification under secrecy* was, to the best of current knowledge, the first explicit proposal for a QRNG protocol in which multipartite entanglement is engineered to provide a public proof of private randomness at the bit-string level. The Jacak works also analyzed alternative quantum mechanisms for randomness generation (e.g. quantum transitions governed by Fermi's golden rule) and introduced a broader framework of "quantum generators of random numbers" combining entangled and non-entangled sources. [6]

The EITCI Quantum Standards Group subsequently published three reference standards: one on theoretical concepts and use cases, one on protocols, processes and operative principles for EQRNG with public randomness certification and one on testing and verification schemes including sustaining secrecy. [3–5] These documents detailed topological models of entanglement, generalized Bell-chain states, XOR relations among generated strings, and workflow diagrams for public randomness testing of EQRNG.

Later experimental work by Islam *et al.* and Kolangatt *et al.* realized publicly verifiable EQRNGs on photonic platforms. [11,12] Their implementations closely follow the Jacak protocol structure, using polarization-entangled photon pairs, multi-qubit encodings and measurement patterns that generate a secret random string and an associated public test string. Independent lines of work have demonstrated certified QRNGs based on single-particle entanglement and semi-device-independent (SDI) analyses. [13, 14]

In parallel, DI QRNG schemes based on loophole-free Bell tests have improved in performance and practicality. [24–27, 29, 30] While DI QRNGs typically focus on certifying public randomness or expanding a private seed, they share with EQRNGs the central role of entanglement and nonlocal correlations. The Jacak public-verification concept can therefore be seen as an application-layer complement to DI security: it provides a protocol interface for using entanglement (and also DI guarantees) to certify randomness of secret strings in deployed systems.

Standardization context and objectives

General random bit and QRNG standards, such as ISO/IEC 18031, the NIST SP 800-90 series, NIST SP 800-22, ETSI GS QKD 014 and ITU–T X.1702, [15–19] define models and requirements for entropy sources, conditioning components, health tests, statistical testing and interfaces. They cover classical and quantum entropy sources and provide a common basis for certification of cryptographic modules and QRNG devices.

These documents, however, largely focus on single-system or noise-based QRNGs and do not yet systematically address protocol structures whose functionality critically relies on multipartite entanglement, such as public-verification EQRNGs, multi-party entanglement-assisted QRNGs or entanglement-based DI QRNGs. The earlier EITCI reference standards addressed this gap for one particular family of EQRNG protocols. [3–5] Building on them and on subsequent research, there is now a need for a more general, technology-agnostic technical reference standard for entanglement-based QRNG protocols.

This document is intended to fulfil that role, with a focus on:

- clear **definitions** of EQRNG-related terms and symbols;
- a **taxonomy** of QRNGs that highlights the distinctive features of entanglement-based protocols;
- concise but rigorous **quantum-theoretical foundations** relevant to EQRNGs, including entanglement measures, entropy measures and nonlocality;
- the core **principles and protocol patterns** of entanglement-based QRNGs, with emphasis on public randomness verification;
- **security models** and threat analyses tailored to EQRNGs and their relationship to DI and SDI QRNG frameworks;
- high-level **implementation profiles** and **use cases**, while leaving platform-specific parameters and hardware requirements to complementary documents.

Structure of this document

The remainder of this Technical Reference Standard is organized as numbered clauses. The introduction is intentionally unnumbered, so that Clause 1 follows the convention of standards documents in designating the scope. Brief synopses are provided for each clause; detailed normative requirements and parameter ranges are developed on top of this structure.

- Clause 1 defines the scope and field of application.

- Clause 2 lists normative references.
- Clause 3 specifies terms, definitions and abbreviations.
- Clause 4 fixes mathematical symbols and notation.
- Clause 5 reviews QRNG architectures, introduces a taxonomy and recalls generic QRNG requirements.
- Clause 6 develops quantum-theoretical foundations relevant to EQRNGs.
- Clause 7 specifies generalized multi-qubit parity-entangled states and XOR structures for PV-EQRNG protocols.
- Clause 8 presents core entanglement-based QRNG principles and reference protocol families, including public-verification schemes.
- Clause 9 formulates functional requirements for EQRNG protocols.
- Clause 10 specifies security models, threat analyses and public randomness verification conditions.
- Clause 11 outlines implementation profiles and physical realizations at an abstract level.
- Clause 12 addresses randomness extraction, post-processing and statistical testing.
- Clause 13 maps EQRNG profiles to use cases and deployment patterns.
- Clause 14 sketches conformance assessment and profile definitions.
- Clause 15 summarizes future work items and possible extensions.

Throughout the document, the term "clause" is used for numbered sections (Clauses 1 and above). When the key words "*shall*", "*shall not*", "*should*", "*may*" and "*can*" appear in subsequent normative versions of this text, they are to be interpreted as requirement, prohibition, recommendation, permission and possibility, respectively.

1 Scope and field of application

1.1 General

This Technical Reference Standard specifies concepts, terminology, mathematical models and protocol-level requirements for *entanglement-based quantum random number generators* (EQRNGs). It is concerned with the design and analysis of *protocols* and *functional behaviours*, rather than with detailed hardware implementation parameters.

The document focuses on entanglement-based QRNG protocols in which multipartite quantum entanglement is an explicit resource and in which at least one key functionality—such as public verification of randomness under secrecy, multi-party sharing of correlated random strings or device-independent certification—*depends essentially* on the entanglement structure of the underlying quantum state. [2–5]

This standard is intended to be used in conjunction with generic random bit generation and QRNG standards such as ISO/IEC 18031, ISO/IEC 20543, NIST SP 800-90B, NIST SP 800-22 and ITU–T X.1702. [15–17, 19, 31] It does not replace those documents; rather, it provides a specialized framework for entanglement-based protocols that can be mapped onto the entropy-source and random-bit-generator abstraction used in those standards.

1.2 In-scope protocol classes

This standard applies to quantum random number generation protocols that satisfy all of the following conditions:

(a) The primary entropy source is a quantum state ρ_S of a composite system $S = S_1 S_2 \dots S_m$ that is entangled across at least one non-trivial partition of subsystems. [7, 8]

(b) Random bits generated by local quantum measurements on one or more subsystems of S.

(c) The protocol's security or functional guarantees (for example, public randomness verification, multi-party correlation patterns or device-independent entropy certification) *explicitly rely* on the entanglement properties of ρ_S.

(d) The unpredictability of the resulting bit strings is justified using quantum information-theoretic arguments (e.g. bounds on min-entropy or conditional min-entropy) as opposed to purely classical or empirical arguments. [7, 24]

Within this scope the following EQRNG protocol classes are defined:

EQRNG-1 (device-dependent EQRNG).
Protocols in which the source and measurement devices are modelled and trusted at the level of their relevant quantum degrees of freedom. Security and entropy bounds are derived from a device-level physical model and parameter estimation. The Jacak generalized Bell-chain EQRNG with public randomness certification [2, 4, 6] is a canonical example.

EQRNG-2 (semi-device-independent EQRNG).
Protocols in which some components (for example, the source or the measurement apparatus) are treated as untrusted black boxes but are constrained by partial assumptions such as dimension bounds or observed statistics (Bell or contextuality inequalities). Examples include source-device-independent and other semi-DI QRNGs based on entanglement. [13, 14, 30, 32]

EQRNG-3 (device-independent EQRNG).
Protocols in which randomness is certified solely from observed non-local correlations (typically Bell inequality violations) under minimal assumptions such as no-signalling and secure laboratories. Entanglement is used to produce the non-local correlations and to bound an adversary's information about the outputs. [24–27]

An EQRNG implementation *SHALL* declare the EQRNG class or classes to which it claims conformance.

1.3 Public randomness verification use case

A principal focus of this standard is on EQRNG protocols that enable *public verification of randomness under secrecy*. In such protocols:

- the device generates one or more *secret* random bit strings to be consumed by the user (for example, as cryptographic keys);
- the device simultaneously generates one or more *public* test strings whose statistical properties are provably linked, via the entanglement structure of the underlying quantum state, to those of the secret strings;

- public test strings are disclosed to one or more Verification Centres (VCs) which apply prescribed statistical and/or physical tests; the results of these tests allow the VCs and relying parties to assess the randomness quality of the secret strings without learning their values. [2, 4, 11]

Protocols of this type are typically of class EQRNG-1 or EQRNG-2. General requirements for public verification workflows are given in later clauses.

1.4 Out-of-scope items

The following items are out of scope of this Technical Reference Standard:

- classical pseudo-random number generators (PRNGs) and physical true RNGs whose entropy sources are purely classical (thermal noise, chaotic oscillators, etc.) without quantum modelling;
- QRNG protocols based solely on single-system quantum effects (superposition, vacuum fluctuations) that do not use entanglement as an explicit resource, unless such protocols are combined with entanglement-based mechanisms in a hybrid architecture;
- complete cryptographic protocols (for example QKD, secret sharing, authentication schemes) except insofar as they define requirements for the EQRNG component or rely on its outputs;
- detailed electrical, optical or mechanical design parameters of hardware implementations; these are expected to be covered by hardware-specific standards and by implementation guides aligned with ITU–T X.1702, ISO/IEC 18031 and related documents. [15, 19]

1.5 Conformance profiles

A *conformance profile* under this standard is identified by the quadruple

{EQRNG class, protocol family, entropy model, verification model},

where:

- the EQRNG class is EQRNG-1, EQRNG-2 or EQRNG-3 as defined above;
- the protocol family identifies the high-level construction, such as Bell-pair EQRNG, Jacak generalized Bell-chain EQRNG, GHZ-based multiparty EQRNG, or DI Bell-test-based EQRNG;
- the entropy model specifies how min-entropy or conditional min-entropy is bounded from observed data and physical assumptions;
- the verification model specifies whether and how public or internal tests are used (e.g. purely internal health tests, public-release statistical tests, or Bell-test-based certification).

An EQRNG implementation claiming conformance to this standard *SHALL* declare at least one conformance profile and *SHALL* satisfy all requirements associated with that profile in the relevant clauses of this document.

2 Normative references

The following referenced documents are indispensable for the application of this Technical Reference Standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

2.1 General RNG and QRNG standards

- ISO/IEC 18031, *Information technology – Security techniques – Random bit generation.* [15]
- ISO/IEC 20543, *Information technology – Security techniques – Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408.* [31]
- NIST Special Publication 800-90B, *Recommendation for the Entropy Sources Used for Random Bit Generation.* [16]
- NIST Special Publication 800-22 Revision 1a, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.* [17]
- ITU–T Recommendation X.1702, *Quantum noise random number generator architecture*, specifying architectural and security requirements for quantum entropy sources. [19]
- Telecommunication Engineering Centre GR/QS-91020, *Quantum Random Number Generator (QRNG) – Generic Requirements*, specifying generic requirements for QRNG components in Indian telecommunications infrastructure. [33]

These documents define the general framework for entropy sources, random bit generators, conditioning components, statistical testing and conformance, within which EQRNG implementations *SHALL* be analysed.

2.2 Existing EQRNG reference standards and patents

- RS–EITCI–QSG–EQRNG–THEORY–STD-VER-1.0, *Reference Standard for the Entangled Quantum Random Number Generator with the Public Randomness Certification – Theoretical Concepts (Definitions, True Randomness, Use Cases).* [3]
- RS–EITCI–QSG–EQRNG–PROTOCOLS–STD-VER-1.0, *Reference Standard for the Entangled Quantum Random Number Generator with the Public Randomness Certification – Protocols, Processes, Devices and Operative Principles.* [4]
- RS–EITCI–QSG–EQRNG–TESTING–STD-VER-1.0, *Reference Standard for the Entangled Quantum Random Number Generator with the Public Randomness Certification – Testing and Verification Schemes including Sustaining Secrecy.* [5]
- WIPO Patent WO2019132679, *Entanglement Quantum Random Number Generator with Public Randomness Certification.* [1]

These documents define the original Jacak entanglement-based QRNG with public randomness certification and are normative for the definition of the Jacak generalized Bell-chain protocol family in this standard.

2.3 Core entanglement-based QRNG scientific references

- Jacak *et al.*, *Entangled quantum random numbers generation and certification.* [2]
- Jóźwiak *et al.*, *New concepts and construction of quantum random number generators.* [10]
- Jacak *et al.*, *Quantum generators of random numbers.* [6]
- Islam *et al.*, *A privacy-preserving publicly verifiable quantum random number generator.* [11]
- Kolangatt *et al.*, *Publicly verifiable quantum random-number generator with a four-qubit photonic system.* [12]

- Mazzucchi *et al.*, *Entropy certification of a realistic quantum random-number generator based on single-particle entanglement.* [13]
- Leone *et al.*, *Certified quantum random-number generator based on single-photon entanglement.* [14]

These references are normative for the physical and information-theoretic definitions of the EQRNG protocol families and entropy models used in this document.

2.4 QRNG review and framework literature

- Ma *et al.*, *Quantum random number generation.* [7]
- Herrero-Collantes and Garcia-Escartín, *Quantum random number generators.* [8]
- Mannalatha *et al.*, *A comprehensive review of quantum random number generators.* [9]
- Jacak *et al.*, *New concepts and construction of quantum random number generators.* [10]

These documents provide the general conceptual background and taxonomy for QRNGs and are referenced for classification and terminology.

2.5 Device-independent and semi-device-independent QRNG

- Pironio *et al.*, *Random numbers certified by Bell's theorem.* [24]
- Liu *et al.*, *Device-independent quantum random-number generation.* [25]
- Marangon *et al.*, *Source-device-independent quantum random number generation.* [32]
- Shalm *et al.*, *Device-independent randomness expansion with entangled photons.* [26]
- Zhang *et al.*, *A simple low-latency real-time certifiable quantum random number generator.* [29]
- Avesani *et al.*, *Source-device-independent heterodyne-based quantum random number generator at 17 Gbps.* [30]
- Kavuri *et al.*, *Traceable random numbers from a non-local quantum advantage.* [27]

These references are normative for the device-independent and semi-device-independent security models used in this standard.

3 Terms, definitions and abbreviations

3.1 Verbal forms for requirements

The key words *"SHALL"*, *"SHALL NOT"*, *"SHOULD"*, *"SHOULD NOT"*, *"MAY"* and *"NEED NOT"* in this document are to be interpreted in accordance with common technical-standard practice:

- *SHALL* indicates a requirement strictly to be followed in order to conform to the standard.
- *SHALL NOT* indicates a prohibition.
- *SHOULD* indicates a recommended course of action; there may exist valid reasons in particular circumstances to ignore a *SHOULD* recommendation, but the full implications must be understood and carefully weighed.

- *MAY* indicates a permitted course of action.
- *NEED NOT* indicates something that is truly optional.

3.2 Terms

Unless otherwise stated, terms defined in ISO/IEC 18031, ISO/IEC 20543, NIST SP 800-90B and NIST SP 800-22 apply. [15–17,31] The following terms are specific to this standard or refine existing definitions.

3.2.1 Random bit generator (RBG)

A *random bit generator* is a system, algorithm or device that outputs sequences of bits intended to be statistically indistinguishable from ideal random sequences. In this standard the term is used in the sense of ISO/IEC 18031 and NIST SP 800-90B. [15,16]

3.2.2 Quantum random number generator (QRNG)

A *quantum random number generator (QRNG)* is an RBG whose entropy source is a quantum physical process and whose unpredictability is justified using a quantum-theoretical model of that process. [7,8]

3.2.3 Entanglement-based quantum random number generator (EQRNG)

An *entanglement-based quantum random number generator (EQRNG)* is a QRNG that satisfies all of the following:

(a) the primary entropy source is the measurement of multipartite entangled quantum states;

(b) the protocol's security or functionality relies on entanglement properties such as non-classical correlations, monogamy of entanglement or Bell inequality violations;

(c) the role of entanglement is explicitly specified in the description of the protocol and its security model. [2,3]

3.2.4 Public randomness verification

Public randomness verification is a process in which an entity called a *Verification Centre* (VC) receives one or more bit strings generated by an EQRNG and performs specified statistical and/or physical tests to assess their randomness, while at least one other bit string generated by the same protocol instance remains secret. The EQRNG protocol ensures that successful tests on the public string(s) imply lower bounds on the entropy of the secret string(s) without revealing their specific values. [2,4,11]

3.2.5 Device-dependent, semi-device-independent and device-independent EQRNG

Device-dependent EQRNG.
An EQRNG in which the internal components (sources, channels, detectors) are modelled and trusted; security analysis is carried out within this device model. [7,9]

Semi-device-independent EQRNG.
An EQRNG in which some components are treated as black boxes but constrained by partial assumptions (for example, bounded dimension or bounded energy). Security bounds are derived from these constraints and measured statistics. [13,30,32]

Device-independent EQRNG.
An EQRNG in which randomness is certified solely from observed non-local correlations (e.g. Bell inequality violations) under minimal assumptions such as no-signalling and secure measurement settings. [24–26]

3.2.6 Raw random string

A *raw random string* is a bit string obtained directly from the digitized output of the quantum measurement processes of an EQRNG, prior to any classical post-processing such as debiasing, compression or privacy amplification.

3.2.7 Extracted random string

An *extracted random string* is a bit string obtained from one or more raw random strings by a randomness extractor or conditioning component, with the aim of producing bits that are close to uniformly distributed and independent of any side information. [7, 16]

3.2.8 Min-entropy and conditional min-entropy

For a discrete random variable X with distribution $p_X(x)$, the *min-entropy* is

$$H_\infty(X) = -\log_2 \max_x p_X(x).$$

For a classical-quantum state ρ_{XE} describing side information E held by an adversary, the *conditional min-entropy* $H_\infty(X|E)$ quantifies the adversary's optimal guessing probability of X and is the primary entropy measure used in this standard for security statements. [7, 24]

3.2.9 Verification Centre (VC)

A *Verification Centre (VC)* is a logical entity—which may be a laboratory, regulatory body, audit organisation or distributed protocol— that performs public randomness verification by applying specified tests to public output strings and reporting the results. A VC is not assumed to be trusted with respect to the secrecy of private bit strings but is assumed to follow the prescribed test procedures honestly.

3.3 Abbreviations

The following abbreviations are used:

DI	device-independent
EQRNG	entanglement-based quantum random number generator
QRNG	quantum random number generator
PRNG	pseudo-random number generator
RBG	random bit generator
SDI	semi-device-independent (including source-device-independent)
VC	Verification Centre
GHZ	Greenberger–Horne–Zeilinger (state)
POVM	positive-operator valued measure
QKD	quantum key distribution

4 Symbols and notation

This clause defines the mathematical symbols and quantum-information notation used throughout the standard. All EQRNG protocol descriptions and security claims in this document *SHALL* be interpretable within this notation.

4.1 Quantum states and operators

- $\mathcal{H}$ denotes a finite-dimensional complex Hilbert space. Qubit systems correspond to $\mathcal{H} \cong \mathbb{C}^2$.
- $|\psi\rangle \in \mathcal{H}$ denotes a (column) unit vector representing a pure state. The corresponding bra is $\langle\psi| = |\psi\rangle^\dagger$.
- $|\psi\rangle\langle\psi|$ denotes the rank-one projector $|\psi\rangle\langle\psi|$.
- For subsystems $A, B, \ldots$, the composite Hilbert space is $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. States on multiple subsystems are denoted, for example, by $|\psi\rangle_{AB}$ or ρ_{AB}.
- A *density operator* (or density matrix) ρ is a positive semidefinite operator on $\mathcal{H}$ with $\mathrm{Tr}(\rho) = 1$. Mixed states and statistical ensembles are represented by density operators.
- For a bipartite state ρ_{AB}, the reduced state on subsystem A is $\rho_A = \mathrm{Tr}_B \rho_{AB}$, where Tr_B denotes the partial trace over B.
- I_d denotes the $d \times d$ identity operator; I denotes the identity when the dimension is clear.

4.2 Standard entangled states

The following standard entangled states are used:

- Two-qubit Bell states:

$$\left|\Phi^{\pm}_{AB}\right\rangle = \tfrac{1}{\sqrt{2}}\left(|00\rangle_{AB} \pm |11\rangle_{AB}\right), \tag{4}$$

$$\left|\Psi^{\pm}_{AB}\right\rangle = \tfrac{1}{\sqrt{2}}\left(|01\rangle_{AB} \pm |10\rangle_{AB}\right). \tag{5}$$

- n-qubit GHZ state:

$$|\Psi_{\mathrm{GHZ}}\rangle = \tfrac{1}{\sqrt{2}}\left(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\right).$$

- n-qubit W state:

$$|W_n\rangle = \tfrac{1}{\sqrt{n}} \sum_{j=1}^{n} |0\rangle^{\otimes(j-1)} |1\rangle |0\rangle^{\otimes(n-j)}.$$

- Three-qubit "three-link chain" state used in the Jacak EQRNG:

$$|\Psi_{XAB}\rangle = \tfrac{1}{2}(|000\rangle_{XAB} + |011\rangle_{XAB} + |101\rangle_{XAB} + |110\rangle_{XAB}),$$

  where X is an auxiliary qubit and A, B are output qubits. [2,3]

- Generalized state used for EQRNG, for an arbitrary number of qubits n, can be expressed in the following simplified forms [10]

$$\left|\Psi_n^{\alpha_1 \ldots \alpha_{n'}}\right\rangle = \frac{1}{\sqrt{n'+1}} \sum_{x=0}^{n'} e^{i\alpha_{x_{10}}} |x_2\rangle_{n-1} \otimes \left|\oplus_{i=1}^{n-1} x_{2,i}\right\rangle, \tag{6}$$

$$\left|\Psi_n^{\beta_1 \ldots \beta_{n'}}\right\rangle = \frac{1}{\sqrt{n'+1}} \sum_{x=0}^{n'} e^{i\beta_{x_{10}}} |x_2\rangle_{n-1} \otimes \left|\oplus_{i=1}^{n-1} x_{2,i} \oplus 1\right\rangle, \tag{7}$$

  where x_2 is the binary and x_{10} is the decimal representation of x, $x_{2,i}$ is the i-th bit of x_2, $|x_2\rangle_{n-1} = |x_{2,1}\rangle \otimes \ldots \otimes |x_{2,n-1}\rangle$, and $n' = 2^{n-1} - 1$, $\oplus_{i=1}^{n-1} x_{2,i}$ and $\oplus_{i=1}^{n-1} x_{2,i} \oplus 1$ calculates bitwise parity and the negation of bitwise parity of x_2 accordingly. The phases α_0 and β_0 can be chosen as zero due to the global phase invariance of the quantum wavefunction.

Where relevant, topological interpretations of multipartite entanglement (Borromean rings, linked chains) follow the conventions in the EITCI EQRNG theory standard and in Jacak *et al.* [2,3]

4.3 Measurements

- A projective measurement is specified by a family of orthogonal projectors $\{P_x\}$ satisfying $\sum_x P_x = \mathrm{I}$. Measuring ρ with $\{P_x\}$ yields outcome x with probability $p(x) = \mathrm{Tr}(\rho P_x)$.
- A general quantum measurement (POVM) is specified by positive operators $\{M_x\}$ with $\sum_x M_x = \mathrm{I}$. The outcome probabilities are $p(x) = \mathrm{Tr}(\rho M_x)$.
- Classical outcomes of measurements are denoted by capital letters $X, A, B, C, \ldots$ when treating them as random variables, and by lowercase $x, a, b, c, \ldots$ for particular realisations.

4.4 Entropy and information measures

- For a discrete random variable X with distribution $p_X(x)$, the Shannon entropy is $H(X) = -\sum_x p_X(x) \log_2 p_X(x)$.
- The min-entropy is $H_\infty(X) = -\log_2 \max_x p_X(x)$.
- For a density operator ρ, the von Neumann entropy is $S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$.
- For a classical-quantum state ρ_{XE} modelling side information E, the conditional min-entropy $H_\infty(X|E)$ is defined as in standard quantum information theory and is used to quantify secure randomness against an adversary with system E. [7, 24]

4.5 Random variables, bit strings and operations

- Random variables are denoted by uppercase letters $(X, A, B, C, \ldots)$; specific outcomes are denoted by lowercase letters $(x, a, b, c, \ldots)$.
- Bit strings of length n are denoted by bold symbols $\boldsymbol{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$.
- The bitwise XOR (exclusive OR) operation is denoted by $\oplus$. For bits $u, v \in \{0,1\}$, $u \oplus v$ is 1 if $u \neq v$ and 0 otherwise. XOR on bit strings is applied component-wise.
- The index i is typically used to label successive uses (rounds) of a protocol. For example, A_i denotes the i-th value in a control sequence, and B_i the corresponding bit in an output sequence. The total number of rounds is denoted N.

5 QRNG architectures, taxonomy and general requirements

This clause provides an overview of quantum random number generator architectures and a taxonomy of QRNG types, and states general requirements that *all* QRNGs, including entanglement-based QRNGs, *SHALL* satisfy. It situates entanglement-based approaches within the broader QRNG landscape and links the present standard to existing RNG and QRNG standards. [7–10]

5.1 Overview of physical QRNG architectures

5.1.1 Discrete-variable (DV) QRNGs

DV QRNGs employ individual quantum events that produce discrete outcomes, typically detected by single-photon or single-particle detectors. Examples include:

- beam-splitter QRNGs where a single photon randomly exits one of two output ports;
- time-of-arrival QRNGs where detection times are discretised into bins;

- path or polarization encoding QRNGs based on single qubits in balanced superposition states. [7, 8]

Such QRNGs usually operate in a device-dependent model, with entropy analysis based on models of the photon source, optical losses and detector imperfections.

5.1.2 Continuous-variable (CV) QRNGs

CV QRNGs measure continuous observables, typically:

- vacuum fluctuations or phase noise of an optical field measured by homodyne or heterodyne detection;
- amplified spontaneous emission noise;
- electronic quantum shot noise in suitably designed circuits. [7, 8]

The raw outcome is a real-valued random variable, which is digitised and processed by a conditioning component. ITU–T X.1702 [19] and NIST SP 800-90B [16] provide architectural and statistical requirements for such QRNGs.

5.1.3 Entanglement-based QRNGs

Entanglement-based QRNGs use multipartite entangled states as the entropy source. Key examples include:

- Bell-pair QRNGs in which a source emits Bell states and one or both qubits are measured to generate random bits; [8]
- GHZ-based schemes in which multiple parties share an n-qubit GHZ state and obtain correlated random bits by local measurements; [2]
- Jacak-type generalized Bell-chain schemes in which an $(n+1)$-qubit entangled state yields one or more control strings and several output strings with linked correlation/anticorrelation patterns, enabling public randomness verification; [2–5]
- DI and SDI QRNGs in which entanglement is used to produce Bell-inequality violations or other non-classical correlations, from which certified randomness is derived. [24–27, 30, 32]

Entanglement-based architectures are central to this standard.

5.2 Taxonomy by trust model and functionality

Following Ma *et al.*, Herrero-Collantes *et al.*, Mannalatha *et al.* and Jacak *et al.*, [7–10] QRNGs can be classified along the following axes.

5.2.1 Trust model

Device-dependent (trusted device).
The internal components of the QRNG are modelled and trusted. Entropy estimation uses detailed physical models and calibration measurements.

Semi-device-independent.
Only partial trust is assumed. For example, in source-device-independent QRNGs the detectors are trusted but the source is uncharacterised; in other variants the dimension of the Hilbert space is bounded while details remain unknown. [13, 30, 32]

Device-independent.
Randomness is certified solely from observed correlations, usually via loophole-free Bell tests. No detailed model of the devices is needed beyond basic assumptions (secure laboratories and random, independent measurement choices). [24–26]

EQRNG protocols may belong to any of these categories; the Jacak Bell-chain schemes, for example, are naturally device-dependent but can be combined with DI tests. [2, 11, 27]

5.2.2 Functional properties

QRNGs can also be classified by their functional role:

- *secret randomness generators* producing internal keys;
- *public randomness beacons* publishing random values for external use;
- *public-verification QRNGs* supporting public testing of randomness quality while keeping certain strings secret;
- *multi-party EQRNGs* distributing correlated or identical random strings across several parties. [2, 6, 11]

This standard primarily targets the latter three categories when entanglement is the enabling resource.

5.3 Relationship to existing standards

Generic RNG and QRNG standards, such as ISO/IEC 18031, ISO/IEC 20543, NIST SP 800-90B, NIST SP 800-22, ITU–T X.1702 and TEC GR/QS-91020, define requirements for entropy sources, statistical models, health tests, interfaces and environmental robustness. [15–17, 19, 31, 33]

- ISO/IEC 18031 and ISO/IEC 20543 define general concepts of entropy sources and random bit generators, and specify test and analysis methods that apply equally to classical and quantum sources. [15, 31]
- NIST SP 800-90B specifies how entropy sources are to be modelled and validated, including start-up and online health tests, estimator design and documentation. [16]
- NIST SP 800-22 and TestU01 [28] provide baseline statistical test suites for assessing randomness quality empirically. [17]
- ITU–T X.1702 focuses on quantum-noise-based QRNG architectures (especially optical vacuum-noise QRNGs), specifying component-level requirements for such devices. [19]
- TEC GR/QS-91020 specifies generic requirements for QRNG components in Indian telecommunications networks, including interface, reliability and security requirements. [33]

5.4 QKD and key delivery interface specifications

- ETSI GS QKD 014, *Quantum Key Distribution (QKD); Protocol and Data Format of REST-Based Key Delivery API.* [18]

EQRNG implementations intended for deployment in contexts where any of the above standards apply *SHALL* be designed so that the entanglement-based entropy source and protocol can be mapped onto the entropy-source and random-bit-generator abstractions used in those standards, and *SHALL* meet the applicable requirements of those standards in addition to the conceptual and protocol-level requirements in this document.

In the broader quantum communication ecosystem, ETSI GS QKD 014 specifies a REST-based key delivery API between QKD key management entities and consuming applications. [18] That document does not define QRNG requirements or architectures; instead it assumes that cryptographic keys delivered over the API originate from secure key generation mechanisms (which MAY include QKD, EQRNGs or other compliant entropy sources). Implementers of EQRNG devices intended for integration with QKD infrastructures SHOULD ensure that their output key formats and metadata can be conveyed over interfaces compatible with ETSI GS QKD 014, but conformance to that specification is not a prerequisite for conformance to the present EQRNG Technical Reference Standard.

5.5 General QRNG requirements

The following high-level requirements apply to all QRNGs covered by this standard, including EQRNGs. More detailed requirements may be specified in application-specific standards.

5.4.1 Entropy and unpredictability

- A QRNG *SHALL* be accompanied by a documented entropy model that specifies, with clearly stated assumptions, a lower bound on the min-entropy per output bit (or per output symbol) of the raw source. [7, 16]
- For QRNGs intended for cryptographic applications, the manufacturer or designer *SHALL* state a target conditional min-entropy per output bit h_{target} (typically close to one bit per output bit) and *SHALL* justify this target via analysis and empirical evidence.
- Any randomness extraction or conditioning component *SHALL* be designed so that the extracted output can be proven, under the entropy model, to be close to uniformly distributed and independent of an adversary's side information. [7, 16]

5.4.2 Health tests and monitoring

- A QRNG *SHALL* implement start-up and continuous health tests suitable for detecting catastrophic failures and significant deviations from the assumed source model, in line with ISO/IEC 20543 and NIST SP 800-90B. [16, 31]
- Health tests *SHOULD* include simple statistical checks (such as monobit and run-length tests) on short blocks and, where appropriate, tests tailored to the specific physical implementation (for example, monitoring count rates or visibility of interference fringes).
- On detection of a failure or out-of-range parameter, the QRNG *SHALL* enter a defined safe state (for example, halting output or signalling an alarm) until the condition is cleared.

5.4.3 Documentation

A QRNG conforming to this standard *SHALL* provide documentation including at least:

- a description of the physical entropy source and, for EQRNGs, of the entanglement structure and measurement scheme;
- the entropy model, including assumptions on adversaries and side information;

- a description of randomness extraction and post-processing;
- the list of internal health tests and their parameters;
- guidance on intended applications and relevant conformance profiles.

5.6 Additional requirements specific to entanglement-based QRNGs

In addition to the general QRNG requirements above, EQRNGs *SHALL* satisfy the following:

- The entanglement resource (e.g. Bell pairs, GHZ states, Jacak generalized Bell-chain states) *SHALL* be specified, including the ideal target state and relevant observables for characterising entanglement. [2, 3]
- The implementation *SHALL* include methods for quantifying the degree of entanglement or non-classical correlation, such as visibility measurements, entanglement witnesses or, where feasible, Bell inequality tests. [13, 14, 24]
- For protocols with public randomness verification, the mapping between secret and public output strings and any auxiliary control strings *SHALL* be explicitly specified, and the conditions under which successful tests on public strings imply bounds on the entropy of secret strings *SHALL* be documented. [2, 4, 11]
- If an EQRNG claims device-independent or semi-device-independent security, the relevant assumptions (e.g. dimensionality, trusted randomness of measurement choices, isolation of laboratories) *SHALL* be stated, and the entropy analysis *SHALL* be consistent with the DI/SDI references cited in Clause 2. [24–26, 30, 32]

These requirements ensure that entanglement-based QRNGs are treated as proper entropy sources in the sense of general RNG standards, while preserving the specific advantages and use cases of entanglement-based protocols.

6 Quantum-theoretical foundations for entanglement-based QRNGs

This clause specifies the quantum-theoretical framework that SHALL be used throughout this Technical Reference Standard to model, analyse and specify entanglement-based quantum random number generator (EQRNG) protocols. The notation and concepts introduced here are consistent with standard quantum information theory [34, 35] and with state-of-the-art QRNG reviews [7–10], and they SHALL be used by subsequent clauses when formulating functional and security requirements.

6.1 Quantum systems, states and measurements

6.1.1 Finite-dimensional systems

Unless explicitly stated otherwise, systems considered in this standard are finite-dimensional. A single qubit is described by a two-dimensional Hilbert space $\mathcal{H} \cong \mathbb{C}^2$ with computational basis $\{|0\rangle, |1\rangle\}$. An n-qubit register is described by $\mathcal{H}^{\otimes n}$ with basis $\{|x_1\rangle \otimes \cdots \otimes |x_n\rangle : x_i \in \{0, 1\}\}$.

- A *pure state* is represented by a unit vector $|\psi\rangle \in \mathcal{H}$, identified up to a global phase.
- A *mixed state* is described by a density operator $\rho \in \mathcal{B}(\mathcal{H})$ satisfying $\rho \geq 0$ and $\operatorname{Tr} \rho = 1$.

For composite systems AB, the joint state space is $\mathcal{H}_A \otimes \mathcal{H}_B$ with density operator ρ_{AB}. The reduced state on subsystem A is $\rho_A = \operatorname{Tr}_B \rho_{AB}$, where Tr_B denotes the partial trace.

An EQRNG protocol MAY use qudits (systems with local dimension $d > 2$) rather than qubits. In such cases, the above definitions generalise with $\mathcal{H} \cong \mathbb{C}^d$ and computational basis $\{|0\rangle, \ldots, |d-1\rangle\}$.

6.1.2 Measurements and instruments

A general quantum measurement on a system with state ρ is modelled by a positive operator valued measure (POVM) $\{M_x\}_x$ with $M_x \geq 0$ and $\sum_x M_x = I$. When outcome x is observed, the probability of obtaining x and the post-measurement state are

$$p(x) = \mathrm{Tr}(\rho M_x), \qquad \rho'_x = \frac{\sqrt{M_x}\,\rho\,\sqrt{M_x}}{p(x)}. \tag{8}$$

In this standard, unless otherwise specified, measurements SHALL be assumed projective (PVM) in a fixed orthonormal basis. For qubits, the computational basis measurement is defined by projectors $P_0 = |0\rangle\langle 0|$, $P_1 = |1\rangle\langle 1|$. For an n-qubit register, the measurement in the computational basis is the tensor product of the single-qubit measurements, with classical output bit string $\boldsymbol{x} \in \{0,1\}^n$.

The association of quantum measurement outcomes with classical random variables is as follows.

- Each measurement outcome x is identified with a value of a discrete random variable X distributed according to $p(x)$.
- A sequence of N measurements, possibly on correlated or entangled states, gives rise to a random vector $\boldsymbol{X} = (X_1, \ldots, X_N)$ whose joint distribution MAY exhibit correlations.

The randomness extracted by an EQRNG SHALL be analysed in this classical probabilistic representation, taking into account that the underlying state and measurement structure is quantum.

6.2 Entanglement and reduced mixedness

6.2.1 Definition of entanglement

A bipartite state ρ_{AB} is called *separable* if it can be written as a convex combination of product states,

$$\rho_{AB} = \sum_j p_j\, \rho_A^{(j)} \otimes \rho_B^{(j)}, \qquad p_j \geq 0,\ \sum_j p_j = 1. \tag{9}$$

Otherwise, ρ_{AB} is *entangled* [35]. For multipartite systems, entanglement is defined with respect to partitions of the subsystems; various notions of *genuine multipartite entanglement* are distinguished in the literature.

Pure two-qubit entangled states of central relevance to EQRNGs include the Bell states

$$\left|\Phi^{\pm}_{AB}\right\rangle = \tfrac{1}{\sqrt{2}}\big(|00\rangle_{AB} \pm |11\rangle_{AB}\big), \tag{10}$$

$$\left|\Psi^{\pm}_{AB}\right\rangle = \tfrac{1}{\sqrt{2}}\big(|01\rangle_{AB} \pm |10\rangle_{AB}\big), \tag{11}$$

and three-qubit GHZ- and W-type states,

$$|\mathrm{GHZ}_3\rangle = \tfrac{1}{\sqrt{2}}\big(|000\rangle + |111\rangle\big), \tag{12}$$

$$|W_3\rangle = \tfrac{1}{\sqrt{3}}\big(|001\rangle + |010\rangle + |100\rangle\big). \tag{13}$$

6.2.2 Maximal mixedness of reduced states

For a pure bipartite entangled state $|\Psi_{AB}\rangle$, the reduced state on subsystem A is

$$\rho_A = \mathrm{Tr}_B\, |\Psi_{AB}\rangle\langle\Psi_{AB}|\,. \tag{14}$$

If $|\Psi_{AB}\rangle$ is maximally entangled, then ρ_A and ρ_B are maximally mixed:

$$\rho_A = \rho_B = \frac{1}{d} I_d, \tag{15}$$

where d is the local Hilbert space dimension. For Bell states one has $d = 2$, so $\rho_A = \rho_B = \frac{1}{2} I_2$ and the von Neumann entropies $S(\rho_A) = S(\rho_B) = 1$ bit. Consequently, projective measurements in any basis produce *locally* uniform random outcomes.

EQRNG protocols SHALL leverage this property: randomness is generated by measurement of subsystems whose reduced states are (ideally) close to maximally mixed as a result of entanglement. Where applicable, implementations SHALL provide evidence (e.g. via tomography, entanglement witnesses or Bell tests) that reduced states of output subsystems are close to maximally mixed, within specified tolerances.

6.2.3 Multipartite entanglement patterns relevant to EQRNGs

Following Jacak *et al.* and the EITCI standards, three canonical multipartite entanglement patterns are distinguished for three qubits A, B, C [2,3,6]:

- **GHZ-type entanglement**, represented by $|\mathrm{GHZ}_3\rangle$, where measurement of any one qubit projects the remaining pair into a product state. This pattern is suited to multi-party key agreement, but less suited to generating pairs of unrelated random strings.
- **W-type entanglement**, represented by $|W_3\rangle$, which is more robust under particle loss but whose measurement statistics are biased and asymmetric. W-type states are therefore generally unsuitable as primary entropy sources for high-quality QRNGs without additional processing.
- **Three-link-chain entanglement**, represented by the state

  $$|\Psi_{XAB}\rangle = \frac{1}{2}\big(|000\rangle_{XAB} + |011\rangle_{XAB} + |101\rangle_{XAB} + |110\rangle_{XAB}\big), \tag{16}$$

  in which measurement of the auxiliary qubit X in the computational basis projects the remaining pair (A, B) into one of two maximally entangled Bell states:

  $$|0\rangle_X \Rightarrow \left|\Phi^+_{AB}\right\rangle, \qquad |1\rangle_X \Rightarrow \left|\Psi^+_{AB}\right\rangle. \tag{17}$$

  This pattern underlies the Jacak EQRNG random correlation generator and SHALL be considered a reference entanglement structure for EQRNGs with public randomness verification.

The Jacak Scientific Reports paper and the associated patent further generalise Eq. (16) to $(n+1)$-qubit chain-like entangled states in which one or more auxiliary qubits randomly select between families of correlation/anticorrelation patterns on n output qubits. These patterns are realised by sequences of Hadamard and controlled-NOT (CNOT) gates, and are topologically represented by linked rings and braid diagrams in the EITCI standards [1–4].

6.3 Randomness, entropy and adversarial side information

6.3.1 Classical and quantum entropies

For a classical discrete random variable X with distribution $p(x)$, Shannon entropy and min-entropy are defined as

$$H(X) = -\sum_x p(x) \log_2 p(x), \tag{18}$$

$$H_\infty(X) = -\log_2 \max_x p(x). \tag{19}$$

Quantum mechanically, a state's uncertainty is quantified by the von Neumann entropy

$$S(\rho) = -\operatorname{Tr}(\rho \log_2 \rho). \tag{20}$$

For a bipartite pure state $|\Psi_{AB}\rangle$, the entanglement entropy $S(\operatorname{Tr}_B |\Psi_{AB}\rangle\langle\Psi_{AB}|)$ equals the entropy of either subsystem and measures the degree of entanglement [35].

In the presence of an adversary holding side information E, the relevant measure of extractable randomness is the *conditional min-entropy* $H_\infty(X|E)$, defined operationally via the adversary's guessing probability [36, 37]. For a classical-quantum state

$$\rho_{XE} = \sum_x p(x) \, |x\rangle\langle x| \otimes \rho_E^{(x)}, \tag{21}$$

the guessing probability and conditional min-entropy satisfy

$$P_{\text{guess}}(X|E) = \sup_{\{M_x\}} \sum_x p(x) \operatorname{Tr}(M_x \rho_E^{(x)}), \qquad H_\infty(X|E) = -\log_2 P_{\text{guess}}(X|E), \tag{22}$$

where the supremum is over all POVMs $\{M_x\}$ on E.

6.3.2 Entropy accumulation and finite-size effects

EQRNGs produce sequences of bits by repeating a quantum process N times. The entropy per round MAY vary due to source drifts, detector memory effects or other imperfections [13]. In security analyses one SHALL take into account finite-size effects and possible correlations between rounds. Modern DI and SDI QRNG proofs use entropy accumulation theorems to derive min-entropy bounds of the form

$$H_\infty(\boldsymbol{X}|E) \geq N \, h_{\min} - \Delta(N, \varepsilon), \tag{23}$$

where $h_{\min}$ is a per-round bound, Δ is a finite-size correction and ε is a failure probability parameter [24, 36, 37].

Implementers of EQRNG protocols SHOULD, where appropriate, provide entropy estimation procedures consistent with these finite-size frameworks, especially in DI and SDI profiles.

6.4 Bell nonlocality and device-(in)dependence

Device-independent (DI) and semi-device-independent (SDI) QRNGs certify randomness using observed nonlocal correlations, without relying on detailed internal device models [24–27, 30, 32].

6.4.1 CHSH inequality and Bell parameter

In a CHSH scenario, two parties A and B choose measurement settings $a, b \in \{0, 1\}$ and obtain binary outcomes $x, y \in \{\pm 1\}$, leading to a Bell parameter

$$S = E_{00} + E_{01} + E_{10} - E_{11}, \tag{24}$$

where $E_{ab} = \langle xy \rangle_{ab}$. Local hidden-variable models satisfy $|S| \leq 2$. Quantum mechanics allows $|S| \leq 2\sqrt{2}$, achieved by measuring a maximally entangled Bell state in appropriately chosen bases.

For DI QRNGs, observed violation $S > 2$ provides a lower bound on the conditional min-entropy $H_\infty(X|E)$ of one party's output [24, 37]. EQRNG protocols in Class EQRNG-3 (DI profiles) SHALL specify which Bell inequality and parameter mapping are used to derive their entropy bounds.

6.4.2 Relation to entanglement-based QRNGs with public verification

The entanglement used in DI QRNGs is typically bipartite, and outputs are public or become public after extraction. EQRNGs with public verification as considered in this standard occupy an intermediate position:

- They rely on entanglement to link secret and public strings at the protocol level (see Clause 8).
- They MAY, additionally, use Bell tests or entanglement witnesses to upper bound adversarial information about the internal entangled state, thereby tightening entropy estimates for the secret string.

Designers of EQRNG protocols SHOULD consider whether a DI or SDI analysis can be combined with the structural properties of the entanglement-based scheme to obtain stronger guarantees, especially in high-assurance applications.

6.5 Topological viewpoint (informative)

Jacak group considers an illustrative topological discussion of entanglement in which multidimensional rotations of qubits topologically entangle them, which can be intuitively represented by non-trivial linkings of loops [2–4]. In this simplified topological illustrative model:

- Each qubit is associated with a closed loop (topological circle).
- Unentangled product states correspond to collections of disjoint, unlinked loops.
- Entangling multi-qubit unitary transformations correspond, at an abstract level, to braidings and linkings of these loops.

The model is used as an intuitive tool for visualising which entanglement patterns are suitable for QRNG purposes, particularly in the Jacak EQRNG construction, and SHALL be regarded as informative rather than normative.

6.5.1 Link diagrams and entanglement classes

In the EITCI standards, basic entanglement classes for three-qubit states are illustrated as link diagrams:

- A Bell pair tensored with a separable qubit is pictured as two linked loops plus one disjoint loop.
- GHZ-type entanglement is associated with Borromean rings, where all three loops are mutually linked but any two become unlinked if the third is removed. This reflects the property that tracing out any qubit destroys bipartite entanglement [38].
- Three-link-chain entanglement is represented as a chain of three loops, each linked to its neighbours, capturing the property that measuring one qubit (the auxiliary link) leaves the remaining two in a Bell state.

Figure 1 illustrates these basic entanglement classes using linked closed loops. In this standard the figure SHALL be interpreted as an informative representation of how separable, GHZ-type and chain-type three-qubit states correspond to topologically inequivalent linkings, while preserving the closed-loop character of world-lines.

These correspondences are compatible with other work relating quantum entanglement to topological links and braids, for example Kauffman and Lomonaco's mapping of simple link diagrams to multi-qubit entangled states [39].

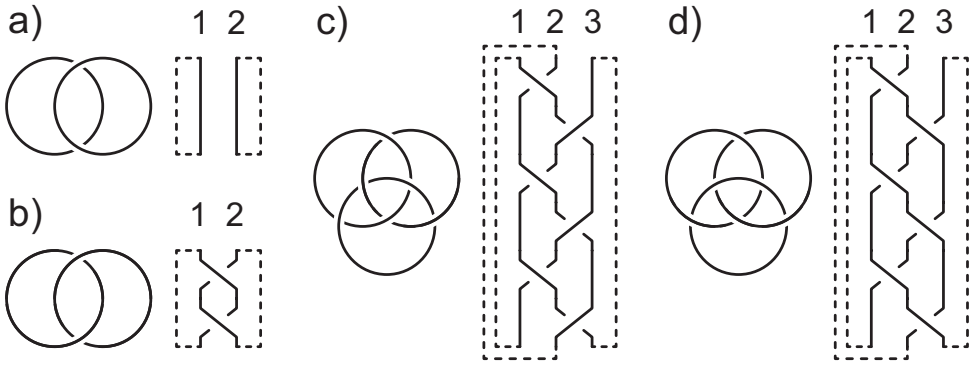

Figure 1: Informative topological representation of inequivalent entanglement classes for qubit systems. Each qubit is depicted as a closed loop; unlinked loops represent separable states, pairwise linked loops represent bipartite entanglement, and Borromean- or chain-like linkings represent GHZ- and chain-type multipartite entanglement. Gaps in the drawn lines do not break the loop topology and are used only to improve visual clarity.

6.5.2 Relation to multi-qubit rotations in high-dimensional Hilbert spaces

Formally, an n-qubit pure state is a vector in a 2^n-dimensional complex Hilbert space, and entangling gates are special unitary transformations $U \in \mathrm{SU}(2^n)$. Any such U can be implemented as a sequence of elementary one- and two-qubit gates, each corresponding to a rotation in an appropriate subspace of the full Hilbert space [34].

The topological model used by Jacak *et al.* provides an intuitive projection of these high-dimensional rotations into planar braid diagrams:

- Each world-line in the circuit diagram (qubit line) is associated with a strand in a braid.
- Controlled-NOT (CNOT) operations correspond to crossings between strands, whose pattern determines whether the resulting state is of GHZ, W or chain type.
- Closing the braid into loops yields link diagrams that classify entanglement patterns up to local unitary transformations (LU-equivalence) within the restricted family of circuits considered.

This approach is compatible with broader research that relates quantum circuits to braid group representations and topological quantum computation. In particular, certain families of quantum gates generate braid group actions whose closures correspond to link invariants and knot polynomials, and entangled states can be associated with nontrivial link types [39–41].

Figure 2 provides an illustrative set of basic quantum circuits that generate topologically inequivalent entanglement patterns discussed above. The gapped regions indicate successive evaluation steps of the multi-qubit gate sequence and SHALL be read as a logical, rather than physical, segmentation of the circuit.

For the purposes of this standard:

- The topological model MAY be used informally to reason about which gate patterns yield desirable entanglement structures for QRNGs, such as the three-link chain states used in Jacak's protocols.
- Implementers are NOT REQUIRED to adopt any particular topological formalism; however, when EQRNG protocols are specified using link diagrams or braid representations, these SHALL be accompanied by explicit circuit-level descriptions (gate sequences) that unambiguously define the underlying quantum operations.

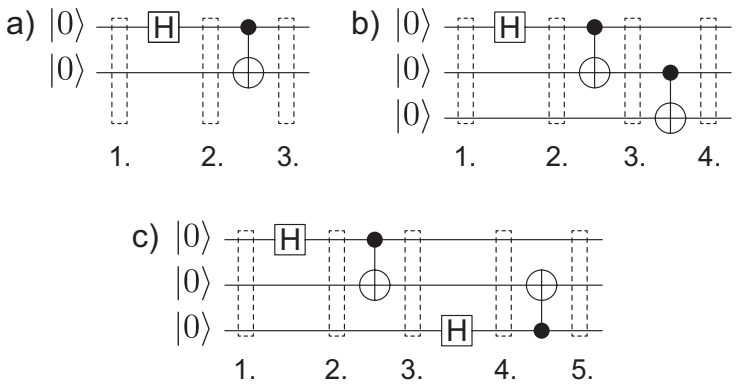

Figure 2: Exemplary quantum circuits realising topologically inequivalent entanglement structures for qubits. Each subfigure corresponds to a distinct sequence of Hadamard gates and CNOT gates that generates a) Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, b) $|\Psi\rangle_{\mathrm{GHZ}} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ GHZ-type, or chain-type entangled states $\frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$. Gapped regions denote consecutive logical stages of the circuit evaluation and are used to highlight how different gate orderings lead to different entanglement classes.

6.5.3 Connection to topological entanglement entropy (informative)

In many-body physics, *topological entanglement entropy* has been proposed as a marker of topological order in ground states of strongly correlated systems [40, 41]. Although the systems considered there (e.g. lattice models with anyonic excitations) differ from the few-qubit EQRNG setting, both perspectives highlight that entanglement possesses structural features that are not reducible to pairwise correlations.

This standard does not require the use of topological entanglement entropy. Nevertheless, designers of advanced EQRNG protocols MAY draw inspiration from these concepts when analysing multipartite entanglement resources, especially for future extensions to higher-dimensional or many-body implementations.

7 Generalized multi-qubit parity-entangled states for PV-EQRNG

This clause specifies, in an abstract Hilbert-space description, the family of multi-qubit parity-entangled states that SHALL be used by public-verification entanglement-based QRNG (PV-EQRNG) protocols conforming to this standard. These states generalise the Jacak three-qubit construction and its multi-qubit extensions introduced in [2, 10] and implemented experimentally in [42, 43].

The defining structural features are:

- all computational-basis components appearing in the superposition have the same parity (even or odd) with respect to the Pauli-Z basis;
- all such components occur with equal probability when measured in the computational basis (equal modulus of amplitudes).

PV-EQRNG implementations that claim conformance to the profiles in Clause 11 and rely on this construction SHALL base their protocol on states that are locally equivalent (up to single-qubit unitaries and global phases) to those specified in this clause.

7.1 Parity and basic two-qubit examples

For an n-qubit computational-basis ket $|q_1 q_2 \dots q_n\rangle$, with $q_i \in \{0,1\}$ and $|q_1 q_2 \dots q_n\rangle \equiv |q_1\rangle \otimes |q_2\rangle \otimes \dots \otimes |q_n\rangle$, the *parity* is defined as

$$\text{parity}(q_1, \dots, q_n) = \sum_{i=1}^{n} q_i \bmod 2 = q_1 \oplus q_2 \oplus \dots \oplus q_n, \tag{25}$$

where $\oplus$ denotes bitwise XOR with $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$.

The two-qubit Bell basis provides the simplest example of parity-structured entangled states:

$$\begin{aligned} |\Phi^+\rangle &= \tfrac{1}{\sqrt{2}} \left(|00\rangle + |11\rangle\right), \\ |\Phi^-\rangle &= \tfrac{1}{\sqrt{2}} \left(|00\rangle - |11\rangle\right), \\ |\Psi^+\rangle &= \tfrac{1}{\sqrt{2}} \left(|01\rangle + |10\rangle\right), \\ |\Psi^-\rangle &= \tfrac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle\right). \end{aligned} \tag{26}$$

In the first two states, $|\Phi^\pm\rangle$, the components $|00\rangle$ and $|11\rangle$ both have parity 0 and occur with equal probability 1/2. In the last two states, $|\Psi^\pm\rangle$, the components $|01\rangle$ and $|10\rangle$ have parity 1, again with equal probability 1/2.

More general two-qubit parity-entangled states with these properties are

$$|\Phi^\alpha\rangle = \tfrac{1}{\sqrt{2}}\big(|00\rangle + e^{i\alpha}\,|11\rangle\big), \qquad \left|\Psi^\beta\right\rangle = \tfrac{1}{\sqrt{2}}\big(|01\rangle + e^{i\beta}\,|10\rangle\big), \tag{27}$$

for real phases $\alpha, \beta \in \mathbb{R}$. These states SHALL be regarded as canonical two-qubit building blocks for parity-based multi-qubit constructions.

7.2 Three-qubit parity-entangled states and EQRNG operation

7.2.1 Definition of the three-qubit parity families

The simplest PV-EQRNG realisation based on this construction uses $n = 3$ qubits. An orthonormal basis of three-qubit parity-entangled states with equal-probability components in the computational basis is given by

$$\begin{aligned} \left|\Phi_3^{+++}\right\rangle &= \tfrac{1}{2} \left(|000\rangle + |011\rangle + |101\rangle + |110\rangle\right), \\ \left|\Phi_3^{--+}\right\rangle &= \tfrac{1}{2} \left(|000\rangle - |011\rangle - |101\rangle + |110\rangle\right), \\ \left|\Phi_3^{-+-}\right\rangle &= \tfrac{1}{2} \left(|000\rangle - |011\rangle + |101\rangle - |110\rangle\right), \\ \left|\Phi_3^{+--}\right\rangle &= \tfrac{1}{2} \left(|000\rangle + |011\rangle - |101\rangle - |110\rangle\right), \\ \left|\Psi_3^{+++}\right\rangle &= \tfrac{1}{2} \left(|001\rangle + |010\rangle + |100\rangle + |111\rangle\right), \\ \left|\Psi_3^{--+}\right\rangle &= \tfrac{1}{2} \left(|001\rangle - |010\rangle - |100\rangle + |111\rangle\right), \\ \left|\Psi_3^{-+-}\right\rangle &= \tfrac{1}{2} \left(|001\rangle - |010\rangle + |100\rangle - |111\rangle\right), \\ \left|\Psi_3^{+--}\right\rangle &= \tfrac{1}{2} \left(|001\rangle + |010\rangle - |100\rangle - |111\rangle\right). \end{aligned} \tag{28}$$

In the first four states, all computational-basis kets in the sum have parity 0 and are equiprobable; in the last four states, all components have parity 1 and are equiprobable.

More generally, three-qubit states suitable for PV-EQRNG SHALL satisfy:

- all basis components appearing in the superposition have same parity (all-even or all-odd);
- all these components have amplitudes of equal modulus (and therefore equal measurement probabilities in the computational basis).

The corresponding general forms are

$$|\Theta_3^{\alpha_1\alpha_2\alpha_3}\rangle = \tfrac{1}{2} \left(|000\rangle + e^{i\alpha_1}\,|011\rangle + e^{i\alpha_2}\,|101\rangle + e^{i\alpha_3}\,|110\rangle\right), \tag{29}$$

for parity 0, and

$$\left|\Theta_3^{\prime\beta_1\beta_2\beta_3}\right\rangle = \tfrac{1}{2}\left(|001\rangle + e^{i\beta_1}|010\rangle + e^{i\beta_2}|100\rangle + e^{i\beta_3}|111\rangle\right), \tag{30}$$

for parity 1, with $\alpha_i, \beta_i \in \mathbb{R}$. Local unitaries MAY be used to transform between different members of these families without changing their role in the protocol.

7.2.2 Canonical three-qubit PV-EQRNG state and XOR structure

A canonical choice for PV-EQRNG with $n = 3$ is the state

$$\left|\Phi_3^{+++}\right\rangle = \tfrac{1}{2}\left(|000\rangle + |011\rangle + |101\rangle + |110\rangle\right). \tag{31}$$

This state can be equivalently written as

$$\left|\Phi_3^{+++}\right\rangle = \tfrac{1}{\sqrt{2}}|0\rangle \otimes \left(\tfrac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)\right) + \tfrac{1}{\sqrt{2}}|1\rangle \otimes \left(\tfrac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)\right), \tag{32}$$

illustrating that a measurement of one qubit in the computational basis projects the remaining two qubits into either a correlated Bell state $|\Phi^+\rangle$ or an anticorrelated Bell state $|\Psi^+\rangle$.

In the canonical three-qubit PV-EQRNG protocol:

3P.1 The device prepares the state $\left|\Phi_3^{+++}\right\rangle$ (or an equivalent state in the same family) for each protocol round. Preparation MAY use a known sequence of Hadamard and CNOT gates, and repeated preparation of this known state SHALL be treated as state re-preparation rather than cloning in the no-cloning sense [44].

3P.2 All single-qubit measurements are performed in the Pauli-Z basis $\{|0\rangle, |1\rangle\}$, corresponding to the observable $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

3P.3 In each round i, the three outcomes are denoted $q_i^{(1)}, q_i^{(2)}, q_i^{(3)} \in \{0, 1\}$, collected into three raw sequences $\mathbf{Q}^{(j)} = (q_i^{(j)})_{i=1}^N$.

3P.4 Due to the parity structure of $\left|\Phi_3^{+++}\right\rangle$, each single measurement outcome is unbiased, and the three sequences are individually balanced (in the limit of large N) and unconditionally random under the ideal model.

3P.5 For every round i, the three bits satisfy the XOR constraint

$$q_i^{(1)} \oplus q_i^{(2)} = q_i^{(3)}, \tag{33}$$

up to an empirically measurable error rate caused by imperfections. By commutativity and associativity of XOR, equivalent relations hold for permuted indices.

Under the ideal model, the three sequences are:

- individually random and balanced;
- pairwise (binary) uncorrelated in the usual sense of empirical correlation tests;
- jointly (ternary) correlated through the XOR constraint.

This *statistical entanglement* at the sequence level SHALL be treated as a structural property of the protocol. Any PV-EQRNG implementation based on three-qubit states of the form (31) **SHALL**:

- monitor the frequency of XOR violations as an error indicator;
- designate at most one of the three sequences as a public verification string;
- designate at most one of the remaining two sequences as a cryptographic output; and
- keep the third sequence private and never disclose it, in order to preserve secrecy given the ternary XOR correlations.

7.3 Scaling to four qubits and beyond

7.3.1 Four-qubit parity-entangled states

For $n = 4$ qubits, parity-entangled states suitable for PV-EQRNG SHALL satisfy the same two conditions: identical parity for all basis components and equal measurement probabilities. A canonical four-qubit example can be obtained recursively from $\left|\Phi_3^{+++}\right\rangle$ and $\left|\Psi_3^{+++}\right\rangle$:

$$\begin{aligned}\left|\Phi_3^{+++}\right\rangle &= \tfrac{1}{2}\left(|000\rangle + |011\rangle + |101\rangle + |110\rangle\right),\\ \left|\Psi_3^{+++}\right\rangle &= \tfrac{1}{2}\left(|001\rangle + |010\rangle + |100\rangle + |111\rangle\right),\end{aligned} \tag{34}$$

leading to

$$\begin{aligned}\left|\Phi_4^{+++++++}\right\rangle &= \tfrac{1}{\sqrt{2}}|0\rangle \otimes \left|\Phi_3^{+++}\right\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \otimes \left|\Psi_3^{+++}\right\rangle\\ &= \tfrac{1}{2\sqrt{2}}\big(|0000\rangle + |0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle\big).\end{aligned} \tag{35}$$

More general four-qubit states with the required properties are

$$\begin{aligned}|\Theta_4^{\alpha_1\ldots\alpha_7}\rangle =& \tfrac{1}{2\sqrt{2}}\big(|0000\rangle + e^{i\alpha_1}|0011\rangle + e^{i\alpha_2}|0101\rangle + e^{i\alpha_3}|0110\rangle\\ &+ e^{i\alpha_4}|1001\rangle + e^{i\alpha_5}|1010\rangle + e^{i\alpha_6}|1100\rangle + e^{i\alpha_7}|1111\rangle\big),\end{aligned} \tag{36}$$

for parity 0, and

$$\begin{aligned}\left|\Theta_4^{'\beta_1\ldots\beta_7}\right\rangle =& \tfrac{1}{2\sqrt{2}}\big(|0001\rangle + e^{i\beta_1}|0010\rangle + e^{i\beta_2}|0100\rangle + e^{i\beta_3}|0111\rangle\\ &+ e^{i\beta_4}|1000\rangle + e^{i\beta_5}|1011\rangle + e^{i\beta_6}|1101\rangle + e^{i\beta_7}|1110\rangle\big),\end{aligned} \tag{37}$$

for parity 1, with $\alpha_i, \beta_i \in \mathbb{R}$. Setting all phases to zero yields the illustrative forms

$$\begin{aligned}&\left|\Phi_4^{+++++++}\right\rangle\\ &= \tfrac{1}{2\sqrt{2}}\big(|0000\rangle + |0011\rangle + |0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle + |1100\rangle + |1111\rangle\big),\end{aligned} \tag{38}$$

and

$$\begin{aligned}&\left|\Psi_4^{+++++++}\right\rangle\\ &= \tfrac{1}{2\sqrt{2}}\big(|0001\rangle + |0010\rangle + |0100\rangle + |0111\rangle + |1000\rangle + |1011\rangle + |1101\rangle + |1110\rangle\big).\end{aligned} \tag{39}$$

The state $\left|\Phi_4^{+++++++}\right\rangle$ can be rewritten as

$$\begin{aligned}\left|\Phi_4^{+++++++}\right\rangle = \;& \tfrac{1}{\sqrt{2}}|0\rangle \otimes \tfrac{1}{2}\big(|000\rangle + |011\rangle + |101\rangle + |110\rangle\big)\\ &+ \tfrac{1}{\sqrt{2}}|1\rangle \otimes \tfrac{1}{2}\big(|001\rangle + |010\rangle + |100\rangle + |111\rangle\big),\end{aligned} \tag{40}$$

showing that measurement of any single qubit projects the remaining three into a state of the three-qubit families defined above.

In a four-qubit PV-EQRNG protocol based on such a state, the four bit sequences $\mathbf{Q}^{(j)} = (q_i^{(j)})_{i=1}^N$ obtained from Pauli-Z measurements satisfy the XOR relation

$$q_i^{(1)} \oplus q_i^{(2)} \oplus q_i^{(3)} = q_i^{(4)}, \tag{41}$$

for each round i, up to an observed error rate. By permutation symmetry of XOR, this relation holds for all permutations of the indices.

The XOR structure implies that:

- knowledge of any two sequences does not determine the other two;
- knowledge of any three sequences determines the remaining fourth one.

Therefore, in four-qubit PV-EQRNG implementations:

- at most one sequence SHALL be disclosed for public verification;
- at least one further sequence SHALL remain permanently undisclosed;
- at most two sequences (i.e. $n-2$ for $n=4$) MAY be used as cryptographic outputs.

7.3.2 General n-qubit parity-entangled states

For general $n \geq 3$, the families of parity-entangled states used in the protocol can be written as

$$\left|\Theta_n^{\alpha_1 \ldots \alpha_{n'}}\right\rangle = \frac{1}{2^{\frac{n-1}{2}}} \sum_{q_1=0}^{1} \sum_{q_2=0}^{1} \cdots \sum_{q_{n-1}=0}^{1} \left(e^{i\alpha_{f(q_1,\ldots,q_{n-1})}} \prod_{k=1}^{n-1}{}^{(\otimes)} |q_k\rangle \otimes |q_1 \oplus q_2 \oplus \ldots \oplus q_{n-1}\rangle \right), \quad (42)$$

and

$$\left|\Theta_n^{'\beta_1 \ldots \beta_{n'}}\right\rangle = \frac{1}{2^{\frac{n-1}{2}}} \sum_{q_1=0}^{1} \sum_{q_2=0}^{1} \cdots \sum_{q_{n-1}=0}^{1} \left(e^{i\beta_{f(q_1,\ldots,q_{n-1})}} \prod_{k=1}^{n-1}{}^{(\otimes)} |q_k\rangle \otimes |q_1 \oplus q_2 \oplus \ldots \oplus q_{n-1} \oplus 1\rangle \right), \quad (43)$$

where $n' = 2^{n-1} - 1$, $f(q_1, \ldots, q_{n-1}) = \sum_{i=1}^{n-1} 2^{n-1-i} q_i$, $\alpha_i, \beta_i \in \mathbb{R}$, and $\prod^{(\otimes)}$ denotes the tensor product over $k = 1, \ldots, n-1$. The states $|\Theta_n^{\alpha_1 \cdots}\rangle$ and $\left|\Theta_n^{'\beta_1 \cdots}\right\rangle$ have parity 0 and 1, respectively. Global phases (e.g. α_0, β_0) MAY be fixed to zero.

For each n, a PV-EQRNG protocol based on these states generates n raw sequences $\mathbf{Q}^{(j)}$, one per qubit. The XOR structure generalises the three- and four-qubit cases: suitable linear XOR relations exist among the n bits in each round and SHALL be documented for any declared implementation profile. In particular:

- at most one sequence SHALL be designated as the public verification sequence;
- at least one further sequence SHALL remain permanently undisclosed;
- at most $n-2$ sequences MAY be used as cryptographic outputs.

7.4 Alternative representation and implemented examples

A convenient alternative representation of the n-qubit parity-entangled families is

$$\left|\Psi_n^{\alpha_1 \ldots \alpha_{n'}}\right\rangle = \frac{1}{\sqrt{n'+1}} \sum_{x=0}^{n'} e^{i\alpha_{x_{10}}} |x_2\rangle_{n-1} \otimes \left|\oplus_{i=1}^{n-1} x_{2,i}\right\rangle, \quad (44)$$

$$\left|\Psi_n^{\beta_1 \ldots \beta_{n'}}\right\rangle = \frac{1}{\sqrt{n'+1}} \sum_{x=0}^{n'} e^{i\beta_{x_{10}}} |x_2\rangle_{n-1} \otimes \left|\oplus_{i=1}^{n-1} x_{2,i} \oplus 1\right\rangle, \quad (45)$$

where x_2 is the $(n-1)$-bit binary representation of x, x_{10} is the decimal representation, $x_{2,i}$ denotes the i-th bit of x_2, $|x_2\rangle_{n-1} = |x_{2,1}\rangle \otimes \ldots \otimes |x_{2,n-1}\rangle$ and $n' = 2^{n-1} - 1$. The expressions $\oplus_{i=1}^{n-1} x_{2,i}$ and $\oplus_{i=1}^{n-1} x_{2,i} \oplus 1$ compute the parity and its negation, respectively. Phases α_0 and β_0 MAY be set to zero.

Independent experimental implementations have used states in these families for $n = 3$ and $n = 4$ demonstrating PV-QRNG/PV-EQRNG operation [10, 42, 43]. For $n = 3$ one has

$$|\Psi_3^{\alpha_1\alpha_2\alpha_3}\rangle = \frac{1}{2}\left(|00\rangle \otimes |0\rangle + e^{i\alpha_1}|01\rangle \otimes |1\rangle + e^{i\alpha_2}|10\rangle \otimes |1\rangle + e^{i\alpha_3}|11\rangle \otimes |0\rangle\right), \tag{46}$$

with, for example, $\alpha_0 = 0$, $\alpha_1 = \pi$, $\alpha_2 = 0$, $\alpha_3 = \pi$, giving

$$\left|\Psi_3^{-+-}\right\rangle = \tfrac{1}{2}\left(|000\rangle - |011\rangle + |101\rangle - |110\rangle\right)$$

as used in [42]. For $n = 4$ one has

$$\begin{aligned}|\Psi_4^{\alpha_1\ldots\alpha_7}\rangle = \frac{1}{2\sqrt{2}}\Big(&|000\rangle \otimes |0\rangle + e^{i\alpha_1}|001\rangle \otimes |1\rangle + e^{i\alpha_2}|010\rangle \otimes |1\rangle + e^{i\alpha_3}|011\rangle \otimes |0\rangle \\ &+ e^{i\alpha_4}|100\rangle \otimes |1\rangle + e^{i\alpha_5}|101\rangle \otimes |0\rangle + e^{i\alpha_6}|110\rangle \otimes |0\rangle + e^{i\alpha_7}|111\rangle \otimes |1\rangle\Big),\end{aligned} \tag{47}$$

and the choice $\alpha_0 = 0$, $\alpha_1 = \pi$, $\alpha_2 = 0$, $\alpha_3 = 0$, $\alpha_4 = \pi$, $\alpha_5 = \pi$, $\alpha_6 = 0$, $\alpha_7 = \pi$ yields

$$\left|\Psi_4^{-++--+-}\right\rangle = \tfrac{1}{2\sqrt{2}}\big(|0000\rangle - |0011\rangle + |0101\rangle + |0110\rangle - |1001\rangle - |1010\rangle + |1100\rangle - |1111\rangle\big),$$

as implemented in [43].

Implementations *MAY* adopt these specific phase patterns or any locally equivalent choice, provided the two structural properties (fixed parity and equal probabilities over all appearing basis states) are preserved and the XOR relations between output sequences are maintained as required by this clause.

7.5 Relation to GHZ states and implementation considerations

The parity-entangled states in this clause are closely related to GHZ states under local basis changes. For example, the three-qubit GHZ state [45, 46]

$$|\Psi_{\mathrm{GHZ}}\rangle = \tfrac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \tag{48}$$

can be mapped into a parity-entangled state of the above family by applying Hadamard gates $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ to all three qubits. In the Hadamard basis $\{|+\rangle, |-\rangle\}$, with $|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ and $|-\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$, one obtains

$$\begin{aligned}H^{\otimes 3}|\Psi_{\mathrm{GHZ}}\rangle &= H^{\otimes 3}\tfrac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right) \\ &= \tfrac{1}{2}\left(|+++\rangle + |+--\rangle + |-+-\rangle + |--+\rangle\right),\end{aligned} \tag{49}$$

which is a member of the three-qubit parity-entangled family expressed in a rotated basis.

Consequently:

- experimental platforms capable of preparing three-qubit GHZ states [45, 46] MAY be used as a starting point for implementing the $n = 3$ PV-EQRNG protocol by appropriate local basis changes;
- analogous constructions MAY be derived for larger n where suitable multi-qubit GHZ or graph states are available;
- when GHZ-based preparations are used, implementations SHALL document the local unitaries applied to map into the parity-entangled forms of this clause and SHALL verify the resulting parity and XOR constraints empirically.

PV-EQRNGs based on these generalized multi-qubit parity-entangled states introduce a class of QRNGs in which:

- multiple raw sequences of identical randomness quality are generated simultaneously;
- one sequence can be fully disclosed for arbitrarily intensive public randomness testing (free from local computational constraints);
- the test results, together with the structural XOR relations, support entropy guarantees for the remaining secret sequences as formalised in Clauses 10 and 12;
- at most $n-2$ sequences per block are usable as cryptographic outputs, in order to preserve secrecy under the multi-sequence XOR structure.

These capabilities directly address the need for publicly verifiable randomness testing in the presence of imperfect, realistic quantum devices, while preserving the secrecy of the random strings intended for cryptographic and other high-assurance applications.

8 Core entanglement-based QRNG principles and reference protocol families

This clause specifies the core design principles of entanglement-based quantum random number generators and defines reference protocol families. The principles generalise and formalise the constructions introduced by Jacak and co-workers in the original EQRNG patent, the Scientific Reports paper on entangled quantum random numbers generation and certification, the EITCI reference standards, and subsequent theoretical and experimental work on EQRNGs and publicly verifiable QRNGs [1–4, 6, 10–12].

8.1 General design principles

An EQRNG protocol SHALL satisfy the following general design principles:

G.1 **Entanglement as primary entropy source.** Randomness SHALL be generated primarily from measurements on entangled quantum states whose reduced subsystems are (close to) maximally mixed, as described in Clause 6. Auxiliary classical randomness MAY be used (for example for basis selection or sampling) but SHALL NOT be the dominant entropy source.

G.2 **Structural use of correlations.** The protocol SHALL exploit entanglement-induced correlations in a structural way. In particular, there SHALL exist explicit relations between subsets of output strings (e.g. XOR relations, parity constraints) that are enforced by the entangled state and gate pattern, not only by classical post-processing.

G.3 **Decoupling of secrecy and verifiability.** For profiles that support public randomness verification, at least one output string SHALL remain secret while one or more other strings are made public exclusively for testing and verification. The protocol SHALL be designed such that public data enable assessment of randomness quality but do not reveal the values of secret bits (beyond what is implied by their randomness).

G.4 **Platform independence.** The protocol definition SHALL be expressible at the level of abstract quantum states and operations (Hilbert space models and circuit descriptions). Physical realisations MAY vary across platforms (photonic, superconducting, trapped ions, etc.), provided they implement an equivalent state preparation and measurement scheme.

8.2 Reference family A: two-qubit Bell-pair EQRNGs

Reference family A comprises EQRNG protocols in which the basic resource is a stream of two-qubit maximally entangled states $\left|\Phi^+_{AB}\right\rangle$ or related Bell states generated by a source and distributed to one or two parties.

8.2.1 Basic operation

In each round i:

A.1 The source prepares a Bell state, for instance $\left|\Phi^+_{AB}\right\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$.

A.2 Subsystem A is measured in a fixed basis (e.g. computational basis), producing bit B_i.

A.3 Subsystem B MAY be measured in the same or a different basis, producing bit C_i.

The resulting bit strings $\boldsymbol{B}$ and $\boldsymbol{C}$ are individually random and perfectly correlated (or anti-correlated) in the ideal case. Reference family A MAY be used for:

- local randomness generation (ignoring $\boldsymbol{C}$);
- simple distributed randomness where two parties share identical bits;
- DI or SDI QRNGs based on Bell inequality tests when measurement bases are appropriately chosen [24–26, 29].

Family A DOES NOT by itself implement public randomness verification with secrecy; it serves as a baseline entanglement-based QRNG architecture and as a building block for more advanced families.

Figure 3 shows a representative gate-level realisation of a two-qubit random-correlation generator compatible with Reference family A. In particular, it illustrates how an auxiliary qubit and classical control lines can be used to select between different Bell-state preparations prior to measurement.

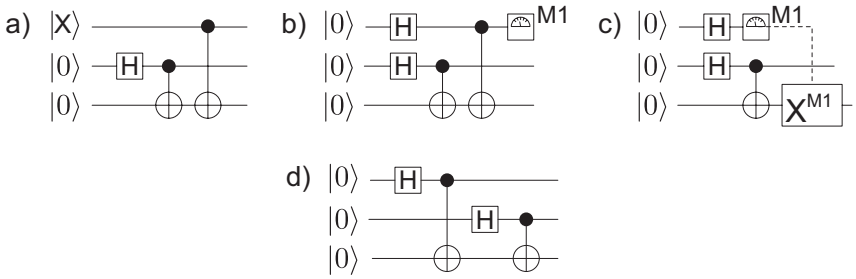

Figure 3: Quantum gate scheme of a random-correlation generator based on a two-qubit entangled state and one auxiliary qubit X. Subfigure (a) depicts a fixed Bell-state preparation, while subfigures (b) and (c) include a random selection mechanism for the Bell state type. Double lines indicate classical control paths carrying measurement results that condition subsequent quantum operations. This structure SHALL be regarded as a normative example of a device-dependent EQRNG in Family A.

8.3 Reference family B: Jacak random correlation EQRNG with public verification

Reference family B formalises the Jacak EQRNG concept with public randomness certification introduced in [1, 2] and codified in the EITCI standards [3, 4]. It forms the primary reference for EQRNGs with public verification under this standard.

Figure 4 summarises the main functional elements of a Jacak-type EQRNG with public proof of randomness. It SHALL be interpreted as a reference architecture for Family B implementations.

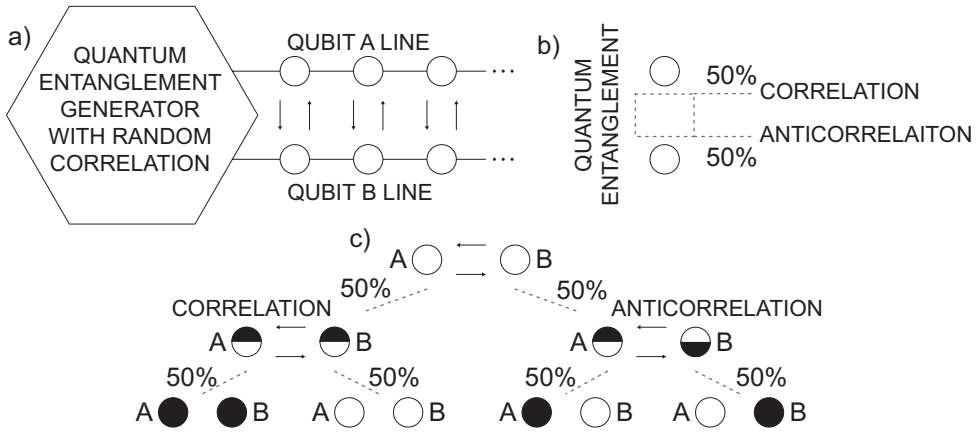

Figure 4: Schematic elements of a protocol for an entanglement-based quantum random number generator with public proof of randomness. Panel (a) shows the generation of random correlations via multi-qubit entanglement; panel (b) indicates the distinct correlation/anticorrelation types available in the protocol; panel (c) lists the possible measurement outcomes and their assignment to secret output strings, public verification strings and internal control data. The diagram SHALL be used as a normative reference for the logical decomposition of Family B protocols.

8.3.1 Three-qubit base protocol (B1)

The minimal B1 protocol uses the three-qubit state $|\Psi_{XAB}\rangle$ of Eq. (16).

Protocol steps. In each round i:

B1.1 **State preparation.** The device prepares $|\Psi_{XAB}\rangle$ using a fixed quantum circuit consisting of a Hadamard gate on an initial $|0\rangle$ qubit, followed by a sequence of CNOT gates coupling the auxiliary and data qubits, as specified in the EITCI protocols standard.

B1.2 **Control measurement.** The auxiliary qubit X is measured in the computational basis, yielding a classical control bit A_i. The measurement projects qubits (A, B) into $|\Phi^+\rangle$ if $A_i = 0$ or $|\Psi^+\rangle$ if $A_i = 1$.

B1.3 **Data measurements.** Qubits A and B are measured in the computational basis, yielding bits B_i and C_i.

B1.4 **String assignment.** Over N rounds, three raw strings are obtained:

$$\boldsymbol{A} = (A_1, \ldots, A_N), \quad \boldsymbol{B} = (B_1, \ldots, B_N), \quad \boldsymbol{C} = (C_1, \ldots, C_N), \tag{50}$$

with the deterministic relation $C_i = B_i \oplus A_i$ in the ideal case.

Secret and public strings. The EQRNG owner SHALL designate at least one string as secret (typically $\boldsymbol{B}$) and one string as public for verification (typically $\boldsymbol{C}$). The control string $\boldsymbol{A}$ SHALL remain internal to the device and SHALL NOT be disclosed to any external party.

Due to the entanglement structure, $\boldsymbol{B}$ and $\boldsymbol{C}$ are individually unbiased and exhibit the same statistical properties when considered as sequences of bits, even though they are algebraically related via $\boldsymbol{A}$. Under ideal conditions and in the absence of side information, the joint distribution $(\boldsymbol{B}, \boldsymbol{C})$ is symmetric in the sense that $I(\boldsymbol{B}; \boldsymbol{C}) = 0$ while $H(\boldsymbol{B}) = H(\boldsymbol{C}) = N$ bits and $H(\boldsymbol{B}, \boldsymbol{C}) = 2N$.

Public verification workflow. The public-verification workflow SHALL include the following:

B1V.1 The EQRNG device outputs $\boldsymbol{B}$ to the user over a secure interface.

B1V.2 It outputs $\boldsymbol{C}$, together with metadata (block length, time stamps, protocol parameters), to one or more Verification Centres (VCs) over an authenticated channel.

B1V.3 Each VC applies a prescribed battery of statistical tests (see Clause 12) and returns an accept/reject verdict and detailed test statistics.

B1V.4 The user accepts $\boldsymbol{B}$ as a high-quality random string only if all designated VCs accept $\boldsymbol{C}$ according to the configured policy.

Implementations SHALL ensure that:

- Test outcomes on $\boldsymbol{C}$ cannot be manipulated by the device in a way that invalidates conclusions about $\boldsymbol{B}$ (e.g. by selectively disclosing "good" blocks). Appropriate sampling and logging arrangements SHOULD be used.
- Failed tests lead to discard or quarantine of the corresponding portions of $\boldsymbol{B}$, and MAY trigger additional diagnostics.

8.3.2 Multi-qubit generalisations (B2)

The Jacak patent and subsequent work generalise B1 to $(k+1)$-qubit chain states with k auxiliary qubits and multiple output registers. These schemes, denoted B2, support:

- simultaneous generation of several secret random strings $\boldsymbol{S}^{(1)}, \ldots, \boldsymbol{S}^{(m)}$;
- generation of one or more public strings $\boldsymbol{P}^{(j)}$ used for verifying all secret strings;
- higher "multiple consent" security levels in which correct operation requires agreement between several control qubits.

Figure 5 gives a normative example of a three-qubit entanglement generator with two auxiliary qubits, illustrating how multiple entangled-state types can be randomly selected in a B2 construction to realise higher "multiple-consent" security levels.

In a typical four-qubit variant, three auxiliary qubits X, Y, Z and one output qubit are arranged so that measurement outcomes on (X, Y, Z) select one of four Bell states on two output qubits or one of several GHZ-type states on three output qubits [1,4]. The corresponding gate-level circuits are illustrated by the figures supplied with this standard, where double lines represent classical control by measurement outcomes.

For B2 protocols, the following SHALL hold:

B2.1 The mapping from auxiliary measurement outcomes to correlation patterns on output qubits SHALL be explicitly specified (e.g. in terms of parity equations between output bits).

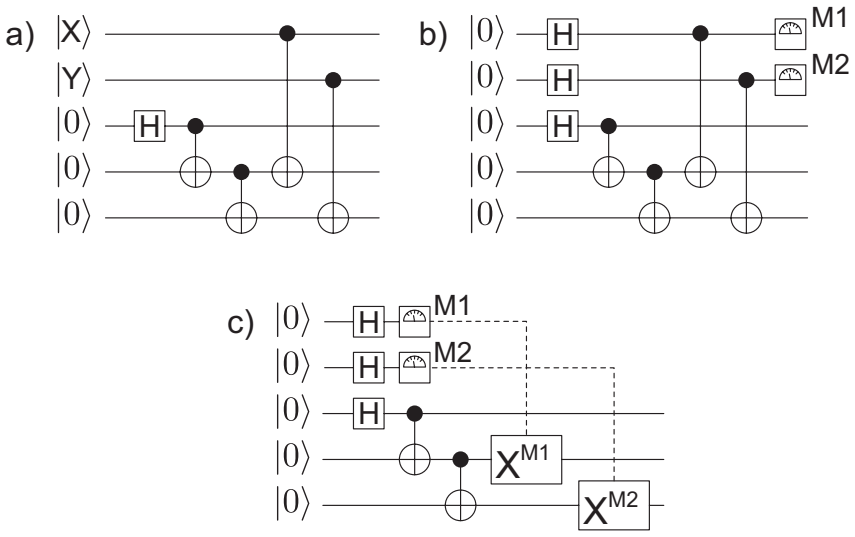

Figure 5: Quantum circuit scheme of a random-correlation entanglement generator with a three-qubit entangled state and two auxiliary qubits X and Y. Case (a) shows a fixed preparation of a given three-qubit entangled state, while cases (b) and (c) incorporate a random selection among different three-qubit entangled-state types. Double lines denote classical control paths carrying measurement results of auxiliary qubits. This scheme SHALL be regarded as a reference pattern for multi-auxiliary Jacak-type EQRNGs in Profile B2.

B2.2 At least one output string SHALL be designated as public and used for randomness tests; it SHALL be guaranteed by design to have the same randomness profile as the secret strings, up to explicitly stated bounds.

B2.3 The algebraic relations linking public and secret strings SHALL be such that knowledge of all public strings and all protocol parameters does not permit an adversary to predict secret bits with probability significantly larger than 2^{-1} per bit, except as bounded by the entropy analysis in Clause 10.

8.4 Reference family C: GHZ-based multi-party EQRNG and secret sharing

Reference family C comprises protocols in which n-party GHZ states are used to generate correlated random strings shared among multiple parties. In the simplest case, n parties share $|\Psi_{\mathrm{GHZ}}\rangle$ and each measures in the computational basis, yielding identical random bits in the ideal case [2,6,9].

- Family C MAY be used to implement quantum-enhanced secret sharing, in which reconstruction of a secret key requires cooperation of at least a threshold number of parties.
- Public verification MAY be integrated by designating one party's string as public while others remain secret, but care SHALL be taken because GHZ-type correlations are fully symmetric and may leak more structure than the chain-type correlations in family B.

Detailed requirements on secret-sharing applications are outside the primary scope of this standard but SHALL conform to the general EQRNG requirements in Clause 9.

8.5 Reference family D: DI and SDI entanglement-based QRNGs

Reference family D covers EQRNG protocols where entanglement is used together with DI or SDI security proofs to certify randomness:

- **Family D1 (DI EQRNGs).** Two or more untrusted devices share entangled states and perform measurements with randomly chosen settings. Observed Bell violation is converted into a min-entropy bound on outputs, as in [24–27]. Public verification MAY be added by disclosing a subset of outputs for statistical tests.
- **Family D2 (SDI EQRNGs).** One part of the device (source or measurement) is modelled as untrusted but bounded in some way (e.g. by dimension), and entangled states (possibly single-particle entanglement) are used to certify randomness [13, 14, 30, 32].

When an EQRNG implementation claims conformance to a D-class profile, it SHALL specify:

- which DI/SDI security proof is used;
- which observed parameters (e.g. Bell parameter, visibility) are measured and how often;
- how these parameters are converted into entropy bounds for the secret and any public output strings.

8.6 Experimental realisations and reference implementations

Recent experimental work has demonstrated that reference families B and D can be implemented in realistic photonic platforms:

- Islam *et al.* realised a B1-type protocol using entangled photon pairs, path-polarisation encoding and a three-qubit effective configuration, demonstrating privacy-preserving publicly verifiable QRNG with NIST SP 800-22 testing on the public string [11].
- Kolangatt *et al.* implemented a four-qubit photonic EQRNG that simultaneously produces public and private random strings and demonstrated publicly verifiable operation at the protocol level, including classical control lines implementing the Jacak-style XOR relations [12].
- Jozwiak *et al.* developed an extended conceptual framework for QRNG architectures, including entanglement-based generators, emphasising layered views of randomness sources and interactions between physical, device and protocol layers [10]. This framework SHALL be considered informative for future extensions of this standard.

Implementers seeking high interoperability SHOULD align their designs with one of the reference families A–D and SHOULD document any deviations explicitly.

9 Functional requirements for EQRNG protocols

This Clause specifies functional requirements that SHALL be satisfied by entanglement-based quantum random number generator (EQRNG) protocols covered by this standard. Requirements are stated at the protocol and interface level and are independent of physical implementation details. Security-specific requirements are further elaborated in Clause 10, and implementation and testing requirements in Clauses 11 and 12.

The requirements in this Clause apply to all EQRNG protocol families defined in Clause 8, including publicly verifiable EQRNGs (PV-EQRNGs) based on multi-qubit parity-entangled states as proposed in [2–4, 10] and photonic implementations as in [11, 12].

9.1 Entropy source and randomness generation

9.1.1 Use of entangled states

Requirement E1 (Entropy-source specification). An EQRNG protocol SHALL specify the family of entangled quantum states used as the primary entropy source, including at least:

- the number of subsystems n (qubits or qudits) in each entangled state;
- the computational basis and Hilbert-space structure for these subsystems;
- the ideal target state (e.g. Bell states, GHZ states, chain states or Jacak-type multi-qubit parity-entangled states such as $\left|\Phi^{+}_{AB}\right\rangle$, $|\Psi_{XAB}\rangle$ of Eq. (16), $|\Psi_{\mathrm{GHZ}}\rangle$ or a specified $(k+1)$-qubit chain state);
- the entanglement pattern or graph (e.g. star, chain, cluster, or multi-parity structures of the form described in [2, 10]);
- the state preparation procedure at the circuit level (sequence of single- and two-qubit gates, or an equivalent physical process such as SPDC-based photonic sources, multi-photon graph-state generation, or integrated photonic circuits).

The protocol SHALL describe how imperfections (mixedness, decoherence, loss, mode mismatch) are modelled at the state level, e.g. via noise channels (depolarising, dephasing, amplitude damping) acting on the ideal state. Where appropriate, the protocol SHOULD define entanglement metrics (e.g. fidelity to the target state, CHSH parameter S, visibility, entropy-based witnesses) that are used for monitoring the entropy source [2, 12, 35].

Requirement E2 (Measurement configuration). The protocol SHALL define, for each protocol round i:

- which subsystems are measured to obtain random outputs (e.g. which of the n qubits contribute to each logical sequence);
- the measurement basis for each subsystem (e.g. Pauli-Z, Pauli-X, rotated bases), including any adaptive or time-varying structure;
- whether basis choices are fixed or randomised and, if randomised, how basis randomness is generated and at what security level.

Any auxiliary randomness used for basis choices or configuration control SHALL be generated from a source whose security level is at least as strong as the intended security level of the EQRNG outputs, and SHALL NOT introduce deterministic dependencies between basis settings and outcomes.

9.1.2 Random variables and output strings

Requirement E3 (Random variables and data organisation). For each protocol round i, the protocol SHALL define random variables representing measurement outcomes (e.g. $A_i, B_i, C_i, \dots$) and SHALL specify which bit strings are considered:

- secret output strings $\mathbf{R}^{(j)}_{\mathrm{sec}}$ intended for cryptographic or other high-assurance use;
- public output or test strings $\mathbf{R}^{(k)}_{\mathrm{pub}}$ intended for public verification and statistical testing (e.g. PV-EQRNG schemes where one or more strings are disclosed as in [2, 11, 12]);

- internal control strings (e.g. **A**, **B**) not exposed externally but used for monitoring, calibration or internal testing.

The protocol SHALL:

- indicate algebraic relations between these strings (e.g. XOR relations or parity constraints) implied by the entangled state and measurement pattern, such as $C_i = A_i \oplus B_i$ for Jacak-type three-qubit schemes or $A_i \oplus B_i \oplus C_i \oplus D_i = 0$ for four-qubit PVQRNG schemes [2,12];
- specify the block structure (block length, ordering, indexing of rounds) for each string;
- specify which strings or subsequences are subject to extraction and which are retained only as metadata or for verification.

9.2 Randomness quality and entropy targets

Requirement E4 (Entropy targets). Each EQRNG protocol SHALL specify, for each secret string $\mathbf{R}_{\text{sec}}^{(j)}$, a target min-entropy per raw output bit, $h_{\text{target}}^{(j)}$, before extraction. Typical high-security targets are $h_{\text{target}}^{(j)} \approx 1$ bit per bit, allowing for small deviations due to imperfections.

The protocol SHALL also specify:

- the model used to estimate or bound $H_\infty(\mathbf{R}_{\text{sec}}^{(j)} \mid E)$, where E represents adversarial side information (classical or quantum);
- whether the bound is device-dependent, source-device-independent (SDI) or device-independent (DI) in nature, in line with the classifications in [7,8,37];
- the statistical confidence level (failure probability) ε associated with the entropy estimate, as required by finite-size analyses [36];
- the operating region (e.g. permitted ranges of visibility, QBER, loss) for which the entropy bound is claimed to hold.

Requirement E5 (Online entropy estimation). Where practical, the protocol SHOULD provide an *online* entropy estimation method that updates bounds on the effective min-entropy of recent outputs based on measured parameters (e.g. visibility, parity-violation rate, error rates, Bell parameters, test statistics), in line with methodologies from NIST SP 800-90B and DI/SDI QRNG analyses [11–14,16,37].

The online estimator MAY be conservative with respect to the offline security analysis but SHALL NOT be more optimistic. Any discrepancy between online and offline estimates SHALL be documented.

9.3 Public verification and linkage between public and secret strings

9.3.1 Mapping between secret and public data

Requirement V1 (Structural mapping). For protocols supporting public randomness verification, the mapping between secret and public strings SHALL be specified by explicit algebraic relations derived from the entangled state structure (e.g. $C_i = B_i \oplus A_i$ in family B1, or higher-order parity constraints for $n > 3$).

Figure 6 gives an explicit flow for a three-qubit PV-EQRNG instance, including generation of raw sequences, enforcement of the XOR rule and classification of correct versus incorrect measurement outcomes. Implementations claiming conformance to Family B SHALL exhibit equivalent logical behaviour.

The protocol SHALL ensure that:

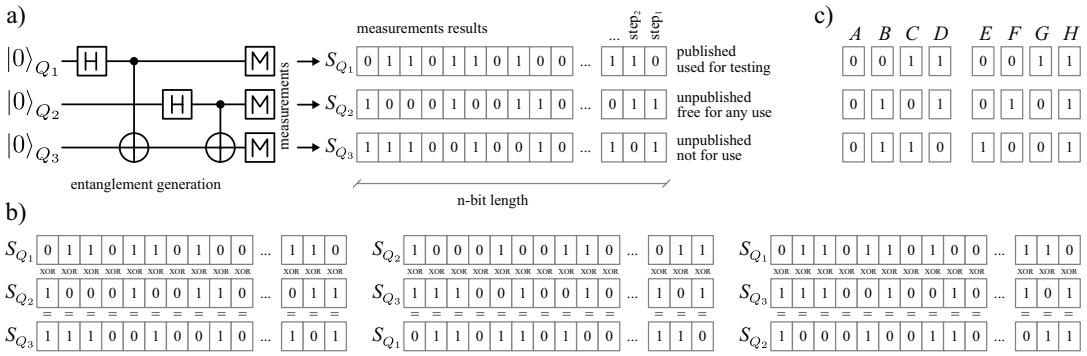

Figure 6: Exemplary flow of a three-qubit entanglement-based QRNG protocol. Panel (a) shows the generation and measurement of entangled states and the resulting sequences S_{Q_i} associated with each measured qubit. Panel (b) illustrates the XOR rule whereby, for every protocol round, the bitwise XOR of any two sequences deterministically yields the third, providing a structural correlation constraint. Panel (c) enumerates the logically allowed ("correct") outcome triplets (A, B, C) and highlights "incorrect" triplets, whose occurrence is interpreted as evidence of bias or device malfunction. The protocol SHALL monitor the frequency of such incorrect outcomes as an error indicator for parity-based PV-EQRNGs.

- the marginal distributions of secret and public strings are equal (or within specified tolerances) under the ideal state and noise model;
- the joint distribution satisfies symmetry properties that preclude significant information leakage from public to secret strings beyond what is accounted for in the entropy analysis;
- for parity-entangled constructions, the number of secret sequences used cryptographically is at most $n - 2$, with at least one sequence reserved for public verification and at least one sequence never disclosed, as in [2, 10].

Requirement V2 (Public verification interface). The protocol SHALL define a public verification interface through which $\mathbf{R}_{\text{pub}}^{(k)}$ and associated metadata (block identifiers, lengths, timestamps, protocol and hardware configuration parameters, test configuration identifiers) are made available to one or more Verification Centres (VCs). The interface SHALL support:

- authentication and integrity protection (e.g. digital signatures, MACs) to prevent tampering with public data;
- replay protection and unique block identifiers;
- clear indication of which sequences are verification strings and which are not to be disclosed.

The interface MAY follow patterns similar to API-based key delivery in [18] but SHALL clearly distinguish between public randomness data and any cryptographic key material.

9.3.2 Entropy guarantees conditioned on public tests

Requirement V3 (Public test family). The protocol SHALL specify a family of statistical and/or physical tests $\mathcal{T}$ to be applied to public strings by VCs (e.g. NIST SP 800-22 tests, TestU01 batteries, additional QRNG-oriented tests), along with:

- test parameters (sequence lengths, block sizes, significance levels);

- acceptance criteria (e.g. minimum fraction of tests passed, combined p-value thresholds, treatment of multiple comparisons);
- procedures for aggregating results from multiple test batteries and multiple VCs;
- handling of inconclusive or borderline results (e.g. re-testing, extended sampling).

Requirement V4 (Linking public tests to secret entropy). The protocol SHALL provide, or reference, an analysis that connects successful public tests on $\mathbf{R}_{\text{pub}}^{(k)}$ to a lower bound on the conditional min-entropy of each secret string $\mathbf{R}_{\text{sec}}^{(j)}$:

$$H_\infty\left(\mathbf{R}_{\text{sec}}^{(j)}\middle|\mathbf{R}_{\text{pub}}^{(1)},\ldots,\mathbf{R}_{\text{pub}}^{(K)},E\right)\geq h_{\min}^{(j)}, \tag{51}$$

for an explicit $h_{\min}^{(j)}$ and failure probability ε. The analysis MAY rely on the structural relations defined by the entangled state and on statistical modelling of imperfections, as in the Jacak EQRNG analysis and its extensions [2, 6, 10–12].

The analysis SHALL be documented sufficiently for independent review, and assumptions about stationarity, independence between blocks, and adversarial capabilities SHALL be explicitly stated.

9.4 Interfaces and data formats

Requirement I1 (Random-output interface). Each EQRNG protocol SHALL specify a logical interface for random output generation, including:

- commands or API calls to request random bit strings of specified length(s) and, where applicable, of specified type (secret or public);
- indications of whether outputs are raw, entropy-estimated, or fully extracted (post-processed) outputs;
- identifiers linking each output block to the corresponding public test blocks (if applicable) and to the relevant configuration of the entropy source.

Requirement I2 (Logging and auditability). For public-verification protocols, the device SHALL provide a logging interface that records, for each block:

- block identifier and timestamps;
- length and partitioning into secret and public segments;
- summary of internal health-test results and entanglement-quality indicators (e.g. visibility, error rates);
- references to external VC test reports (e.g. hashes or signatures);
- indication of whether the block was accepted or rejected for cryptographic use.

This information MAY be used by auditors and certification bodies to verify that public verification is being carried out as specified.

9.5 Robustness, health tests and abort conditions

Requirement R1 (Internal health tests). EQRNG protocols SHALL include internal health tests and sanity checks on raw measurement data, analogous to those recommended in ITU–T X.1702, ETSI QRNG-related documents and NIST SP 800-90B [16, 19]. Typical health tests include:

- monitoring of detector count rates, dark counts and coincidence rates;
- checks for stuck-at faults (e.g. strings of identical bits, frozen detectors);
- simple frequency and run-length tests on short windows of raw data;
- monitoring of entanglement indicators (e.g. visibility, parity violation rates) for drift beyond calibrated tolerances.

Requirement R2 (Abort and fallback conditions). The protocol SHALL define abort conditions under which output is considered invalid and MUST NOT be used. Abort conditions SHALL include at least:

- failure of internal health tests beyond acceptable limits;
- failure of public randomness verification tests on recent blocks, according to the criteria defined under Requirement V3;
- detection of anomalies in entanglement quality indicators (e.g. low visibility, parity-error rate above threshold, Bell parameter below threshold) where such indicators are monitored;
- loss of synchronisation or timing faults that invalidate the assumed mapping between quantum events and classical bits.

Where possible, the protocol SHOULD define safe fallback modes (e.g. reduced throughput, higher thresholds, or complete shutdown) and associated alerts.

9.6 Conformance profiles

For the purposes of this standard, an EQRNG protocol SHALL declare at least one conformance profile of the form

$$\text{Profile} = (\text{Family},\ \text{Class},\ \text{Verification}),$$

where:

- **Family** is one of A–D as defined in Clause 8, or an explicitly specified extension;
- **Class** indicates device-dependence level (EQRNG-1, -2 or -3 as defined in Clause 1);
- **Verification** indicates whether public verification is supported and, if so, according to which requirements in this Clause and Clause 10.

Requirement C1 (Profile documentation). A protocol claiming conformance SHALL document:

- its declared profile(s);
- associated entropy targets $h^{(j)}_{\text{target}}$ and bounds $h^{(j)}_{\min}$;
- the test suites and parameters used both internally and for public verification;

- any assumptions on trusted components, physical isolation and adversarial capabilities (M1–M3 as defined in Clause 10).

This information SHALL be made available to evaluators, certification bodies and, where appropriate, end users, to enable informed risk assessment and interoperability across implementations.

10 Security models, threat analyses and public randomness verification

This Clause defines security objectives, adversarial models, threat categories and public randomness verification conditions for Entanglement Quantum Random Number Generator (EQRNG) protocols and their implementations.

Security considerations SHALL be interpreted in the context of the quantum foundations introduced in Clause 6 and the entanglement-based protocol families in Clause 8, with specific emphasis on publicly verifiable entanglement QRNGs with secret random outputs as developed in [1, 2, 10–12]. The more general QRNG security classifications in [7, 8, 37] are also taken into account.

10.1 Security objectives

An EQRNG protocol and its implementation SHALL specify which of the following security objectives are claimed:

1. **Unpredictability of secret outputs.** The bit strings designated as secret random outputs SHALL be information-theoretically unpredictable (up to a claimed security parameter) for any adversary allowed by the declared security model, including a quantum adversary with side information and unlimited classical computing power consistent with quantum mechanics [36, 37]. Formally, the conditional min-entropy $H_\infty(\mathbf{R}_{\text{sec}} \mid E)$ SHALL exceed a specified bound used in the extraction stage (Clause 12).

2. **Statistical quality of randomness.** The output bit strings SHALL exhibit empirical statistical properties consistent with i.i.d. Bernoulli(1/2) bits within the limits of the chosen test suites and acceptance criteria, as detailed in Clause 12 and informed by [2, 11, 17, 28].

3. **Privacy of secret sequences.** Secret random sequences SHALL remain information-theoretically private (up to the claimed security parameter) against adversaries with side information that is classically or quantumly correlated with the EQRNG device, in line with extractor-based privacy guarantees [36, 37]. Any information disclosed in public verification (verification strings, test outcomes) SHALL be taken into account in the entropy and privacy analysis.

4. **Integrity of public verification.** Publicly verifiable EQRNG protocols SHALL guarantee that a dishonest verifier or man-in-the-middle cannot increase the probability of accepting a non-random or biased device beyond a negligible amount, given the declared threat model and test configuration [2, 11, 12].

5. **Side-channel robustness.** EQRNG devices SHALL be designed to minimise exploitable side channels (including optical leakage, timing, RF emissions, unintended correlations with auxiliary degrees of freedom) and SHALL document residual channels and mitigations [1, 15, 16]. Side-channel considerations SHALL explicitly include the possibility of unintended entanglement with the environment (mixed-state entanglement).

10.2 Adversarial models

An EQRNG protocol SHALL explicitly declare which adversarial model(s) it addresses. The following reference models are defined:

M0: Honest-but-faulty device, no external adversary. Only unintentional imperfections, noise and drift are present. This model is intended for internal engineering validation and SHALL NOT be used as the sole basis for security claims in cryptographic use.

M1: Classical external adversary. The adversary controls all classical communication channels, can inject classical signals and observe public outputs, but has no direct control of the internal quantum hardware and no entangled quantum side information beyond what leaks through classical interfaces. This corresponds to the baseline cryptographic attacker in ISO/IEC 18031 [7, 15].

M2: Quantum side-information adversary. The adversary may hold a quantum system entangled with the EQRNG device or its environment, and may perform arbitrary joint measurements at any time. Security is expressed in terms of min-entropy conditioned on quantum side information, as formalised in [36, 37].

M3: Malicious manufacturer or partially compromised device. The adversary controls the device design and implementation, subject only to the external interface specifications and observable behaviour. This model subsumes the traditional "black-box" perspective of DI and SDI QRNGs [24,25,32]. Claims in this model SHALL specify which components, if any, are trusted (e.g. measurement stations, extraction hardware).

A protocol or implementation claiming compliance with this standard SHALL state which of M1–M3 it targets and SHALL NOT implicitly assume M0 in cryptographic applications.

10.3 Threat categories for EQRNGs

EQRNG implementations SHALL analyse, at minimum, the following high-level threat categories:

1. **Source manipulation and entanglement degradation.** This includes intentional or unintentional reduction of entanglement visibility, introduction of classical correlations, or control of pump power, phase or mode structure in photonic sources (e.g. SPDC, integrated waveguides), or analogous manipulations in non-photonic platforms [2, 6, 11, 12]. Implementations SHALL specify acceptable ranges of entanglement metrics (e.g. CHSH violation, parity-violation rate, fidelity) below which random outputs are rejected or heavily down-rated in entropy.

2. **Measurement and detector attacks.** Threats such as detector blinding, basis control, time-shift attacks and manipulation of thresholds or dead-time SHALL be considered, by analogy with known attacks on quantum optical systems, and mitigated by protective design and monitoring [7, 8, 11]. Where relevant, calibration procedures and monitoring of detector statistics SHALL be documented.

3. **Classical interface and control attacks.** Manipulation of control signals (e.g. basis-choice settings, trigger gating), leakage of raw data over external buses, or modification of extraction parameters are in scope. Implementations SHALL define access control and integrity mechanisms for such interfaces, including authenticated firmware updates and configuration management.

4. **Side-channel leakage and unintended entanglement.** The ideal entangled states employed in EQRNG protocols are, by construction, maximally entangled within a well-defined multi-qubit Hilbert space, which excludes additional entanglement with external degrees of freedom [2, 10]. In practice, decoherence and imperfect isolation can produce mixed states entangled with an environment. Implementations SHALL describe shielding, isolation, filtering, and monitoring strategies, and SHALL specify how entanglement metrics, parity-error rates and other observables map to entropy estimates under such imperfections [11, 12, 16].

5. **Compromised or malicious public verifier.** In public-verification protocols the verifier (or verification centre, VC) may attempt to deviate from the protocol, falsify test results, or correlate auxiliary observations with secret sequences [1, 2, 11]. Protocols SHALL be defined such that a malicious verifier cannot gain additional information about secret sequences beyond what is implied by published acceptance/rejection decisions and declared parameters. Use of multiple, independent VCs SHOULD be considered in high-assurance settings.

6. **Entropy overestimation and model errors.** Incorrect or over-optimistic entropy models (e.g. ignoring certain correlations or side channels) pose a systemic threat. Protocols SHALL document the modelling assumptions used to derive entropy bounds and SHALL include conservative margins for unmodelled effects.

10.4 Security of public randomness verification

EQRNG protocols with public randomness verification employ multi-qubit entangled states whose measurement outcomes define several bit strings with identical or near-identical statistical quality but constrained by parity or XOR relations [2, 4, 10–12].

For such protocols the following conditions SHALL hold:

1. **Indistinguishability of sequences.** All bit strings derived from measurements on subsystems (e.g. X_A, X_B, X_C, X_D) that are claimed to share randomness quality SHALL be generated from identically distributed quantum states, up to explicitly modelled noise and correlation errors. Their empirical statistics SHALL be indistinguishable within specified confidence bounds.

2. **Public–secret separation.** At least one bit string SHALL remain undisclosed and SHALL never be used in any public verification or debugging process. For a three-qubit EQRNG with XOR relation $X^{(1)} \oplus X^{(2)} = X^{(3)}$ only one of the remaining pair of sequences MAY be used cryptographically when one sequence is disclosed for verification [2, 10]. For n entangled qubits, at most $n - 2$ sequences MAY be used as cryptographic outputs.

3. **Verifier's information bound.** The public verifier SHALL only receive one (or a fixed limited number) of sequences designated as verification strings, together with declared protocol parameters such as error-rate estimates and test configuration. The protocol SHALL be designed so that, under the adopted adversarial model, the verifier's accessible information about any secret sequence is bounded by a negligible function of the security parameter after randomness extraction (Clause 12).

4. **Error indicators and thresholds.** In PV-EQRNG protocols based on parity constraints (e.g. XOR conditions among three or four strings [2, 11, 12]) the fraction of parity violations (often referred to as a QBER-type parameter) SHALL be used as an input to entropy estimation and to the decision whether to accept or reject a data block. Acceptance thresholds SHALL be specified and justified based on a conservative security analysis.

5. **Public test suites and transparency.** The statistical tests, parameters, and pass/fail criteria used by the public verifier SHALL be publicly specified and SHALL be reproducible by any external party using the published data, in line with the public randomness certification paradigm [2, 11, 17, 28].

10.5 Relation to DI and SDI security notions

EQRNG protocols considered here share conceptual similarities with DI and source-device-independent (SDI) QRNGs [24–26, 29, 32] but differ in that the central certification mechanism is based on entangled multi-qubit parity structures and statistical "entanglement" among multiple classical sequences, rather than directly on Bell inequality violation.

Implementations MAY additionally embed Bell tests or entanglement witnesses [35] to strengthen quantumness certification; if so, the mapping from observed Bell parameters or witnesses to min-entropy SHALL be documented, referencing appropriate security proofs.

10.5.1 Device-dependence profiles of PV-EQRNG

The PV-EQRNG protocols based on multi-qubit parity-entangled states and XOR constraints, as specified in Clauses 7, 8 and 11, are naturally formulated in a device-dependent (EQRNG-1) security model. The source, measurement devices and control electronics are modelled and trusted at the level of their relevant quantum degrees of freedom, and entropy bounds are derived from this model, from observed parity-violation rates and from standard detector parameters. [2, 10–12]

In principle, PV-EQRNG architectures can also support semi-device-independent or device-independent profiles by adding an explicit *entanglement verification phase* based on Bell or Bell-like inequalities:

- In an SDI realisation, some components (e.g. the source) may be treated as untrusted black boxes with dimension or energy constraints, while others (e.g. detectors) remain modelled. A subset of qubits and measurement rounds is devoted to tests of suitable inequalities (CHSH-type for bipartite cuts, or multi-partite inequalities for larger n), with outcomes revealed and used to bound the entropy available in the remaining rounds.

- In a DI realisation, measurement settings and outputs on spatially separated subsystems of the entangled state are chosen and recorded in a standard DI QRNG configuration. [24–27] A random subset of rounds (including bits drawn from all sequences, possibly including those that are otherwise secret) is sacrificed and disclosed in order to estimate Bell parameters. The remaining rounds are then used within the PV-EQRNG structure: one or more sequences serve as public verification strings, and others remain secret but inherit both the DI entropy guarantees and the statistical linkage to the public strings provided by the multi-qubit parity structure.

When such an additional DI/SDI phase is present and analysed according to the references in Clause 2, an implementation may claim conformance to EQRNG-2 or EQRNG-3 *in addition* to EQRNG-1, and SHALL state clearly which subset of modes and outputs enjoy DI/SDI guarantees and which are analysed in a device-dependent model. The fundamental limitation that no finite DI or PV-EQRNG procedure can provide absolute, assumption-free certainty about the randomness of specific secret bit strings (see Clause 10.6.5) remains unaffected by the choice of profile; what changes is the set of assumptions under which quantitative entropy bounds are derived.

10.6 Limitations of device-independent randomness certification for public verification under secrecy

A large body of work on entanglement-based QRNGs is concerned with *device-independent* (DI) or semi-device-independent (SDI) *certification* of randomness. [13, 14, 24–27, 29, 30, 32] In these schemes, entanglement is demonstrated and quantified through observed non-local correlations (typically Bell inequality violations), and those correlations are converted into lower bounds on the conditional min-entropy of certain output bits. The resulting devices are often described as "certified entanglement-based QRNGs" or "certified DI/SDI QRNGs".

This Clause clarifies a distinction between such DI/SDI *certification of randomness* and the notion of *public randomness verification under secrecy* implemented by Jacak-type entanglement QRNGs with multi-string outputs and parity constraints. [1–5, 10–12] The two concepts are complementary but not equivalent.

10.6.1 What DI/SDI certification actually certifies

DI and SDI QRNGs start from an abstract black-box model in which spatially separated devices receive classical inputs (measurement settings) and produce classical outputs (measurement results), with the only assumptions being, for example, no-signalling, free and independent choice of settings, and bounded dimension or energy. [24, 25, 32, 37] From the observed correlations one estimates:

- a Bell parameter or other non-classicality witness (e.g. CHSH S, Mermin parameter, dimension witness);
- a lower bound on the min-entropy $H_\infty(X|E)$ of some output variable X conditioned on an adversary's side information E;
- a composable security parameter for the extracted randomness after privacy amplification / randomness extraction. [24, 26, 36]

This certification has two important features:

(a) It is *device-level*: the statement is about the behaviour of the black-box devices under certain statistical tests, not about any particular secret bit string that is subsequently produced.

(b) It is typically *one-sided* with respect to secrecy versus publicity: either the outputs are meant to be public (e.g. randomness beacons and expansion experiments), or they are meant to be secret keys, in which case the raw key strings are never disclosed for external testing.

In current DI/SDI experiments, only a fraction of the raw data is ever made public: some samples are sacrificed to estimate the Bell parameter and other figures of merit; the actual key or private randomness is kept secret and is only subject to internal statistical checks and entropy estimation within the laboratory or device. [13, 14, 24, 26, 29] A user or regulator can verify that a device *type* is capable of producing certified randomness, but cannot *independently test the particular secret strings* used in cryptographic applications, because revealing them would destroy their secrecy.

10.6.2 Why CHSH-based certification alone does not provide public verification of secret strings

Consider a DI or SDI QRNG intended to generate secret keys. The protocol might proceed as follows:

- in each round, measurement settings are chosen at random and outcomes recorded;

- a random subset of rounds (the "test" sample) is publicly revealed to estimate CHSH or related parameters and verify a Bell violation;
- the remaining rounds (the "generation" sample) are kept secret and are processed into a key by randomness extraction.

From the perspective of a third party (e.g. a regulator or remote relying party), the only publicly available data are:

- the declared protocol and security model;
- the reported statistics of the test sample (Bell violation, error rates);
- possibly some aggregate information (e.g. average min-entropy per bit, number of extracted bits).

What is *not* available is the ability to run strong classical randomness tests (e.g. NIST SP 800-22, TestU01) [17, 28] on the actual secret key strings: those strings are deliberately never disclosed. From a cryptographic point of view this is entirely appropriate; from the point of view of *public verifiability of the randomness of specific secret strings* it is a fundamental limitation:

(i) Public CHSH or Bell statistics certify that the device behaves, on average, in a way that implies a non-zero entropy rate for the secret outputs under the model assumptions. [24, 37]

(ii) They do *not* allow an external party to test the concrete secret key strings themselves; only the manufacturer or local operator can analyse those strings directly.

(iii) Any attempt to publish or share the exact secret strings for testing would by definition destroy their value as secret keys.

In other words, standard DI/SDI QRNGs provide strong *theoretical* and *device-level* guarantees, but they do not, by themselves, solve the problem: "How can a distant relying party be convinced that *these particular secret keys* are of high randomness quality, without ever seeing them?"

10.6.3 Jacak-type EQRNGs: structural linkage between secret and public strings

The Jacak entanglement-based QRNG protocols address precisely this gap by engineering multipartite entangled states whose measurement outcomes generate *several classical bit strings with enforced algebraic relations* between them. [1–4, 10]

In the simplest three-qubit construction (Family B1 in Clause 8), measurements on the entangled state $|\Psi_{XAB}\rangle$ produce, round by round, three bits (A_i, B_i, C_i) such that ideally

$$C_i = A_i \oplus B_i \tag{52}$$

for each position i. Over many rounds this yields three sequences $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$ that satisfy:

- individually, each of $\boldsymbol{B}$ and $\boldsymbol{C}$ is (ideally) a sequence of i.i.d. unbiased bits; [2, 3]
- structurally, $\boldsymbol{A}$ is a control sequence that determines whether the pair (B_i, C_i) is correlated or anti-correlated, and Eq. (52) holds bitwise;
- any local imperfection (e.g. bias, misalignment, decoherence) affecting the randomness of $\boldsymbol{B}$ necessarily affects $\boldsymbol{C}$ in the same way, because both arise from the same entangled state and the same physical pathway up to local relabelling. [2, 6]

The EQRNG owner keeps one sequence, say $\boldsymbol{B}$, as a secret random output and discloses another, say $\boldsymbol{C}$, as a *public verification string*. External Verification Centres (VCs) can then run arbitrarily strong classical test batteries on $\boldsymbol{C}$ (NIST SP 800-22, TestU01, bespoke tests), without ever seeing $\boldsymbol{B}$. [2, 4, 17, 28] Because of the enforced XOR structure and the symmetry between $\boldsymbol{B}$ and $\boldsymbol{C}$ at the state level, successful tests on $\boldsymbol{C}$ imply that, except with small failure probability, the unseen $\boldsymbol{B}$ has essentially the same randomness profile. [2, 10–12]

This mechanism generalises to multi-qubit parity-entangled states: for an n-qubit configuration one can design families of states in which n output sequences satisfy linear relations (e.g. XOR constraints), with at most $n-2$ sequences used as secret outputs and at least one sequence reserved for public testing. [2, 3, 10] The key point is that the linkage between secret and public strings is enforced *per bit and per block* by the entanglement structure, rather than only at the level of aggregate Bell parameters.

10.6.4 Implications for other entanglement-based QRNGs

The above reasoning does *not* imply that DI/SDI or other entanglement-based QRNGs are insecure or that their certification is invalid; on the contrary, they provide some of the strongest security guarantees currently available for QRNGs in adversarial settings. [13,14,24–27] However, it highlights a structural limitation:

- DI/SDI certification, as typically formulated, guarantees that a device produces high-entropy outputs under certain tests and assumptions, but it does not, by itself, give an external party a way to publicly *test the particular secret strings* used in a cryptographic deployment.
- To achieve *bit-string-level public verification under secrecy*, an entanglement-based QRNG must be designed so that each secret string is paired with one or more public verification strings that share its randomness properties by construction. The Jacak protocols and their photonic realisations provide explicit examples of such designs, based on multi-qubit parity-entangled states and XOR relations between output sequences. [2–5, 10–12]

In principle, other entanglement-based QRNG architectures *could* be extended to incorporate similar multi-string entanglement structures and thus obtain public verification under secrecy. At present, however, Jacak-type EQRNGs and their descendants appear to be the only explicitly analysed family of protocols that engineer this property at the protocol level, rather than relying solely on Bell-inequality-based certification of the device as a whole. Further research on combining DI/SDI techniques with multi-string entanglement-based public verification is identified as a future work item in Clause 15.

10.6.5 Fundamental limits of randomness certification and role of PV-EQRNG

It is important to emphasise that, regardless of the approach—whether device-independent QRNG (DI-QRNG) or publicly verifiable entanglement-based QRNG (PV-EQRNG)—one cannot, in a fully assumption-free sense, realise the scenario in which the QRNG owner performs some public test that convinces a third party *indisputably*, i.e. with mathematical certainty and without any modelling assumptions, that a specific secret random string was generated by a certified physical QRNG device.

In more detail:

- In DI-QRNG, Bell/CHSH inequality violations are not generic randomness tests in the algorithmic sense; rather, they quantify non-classical correlations which, under a clearly stated set of assumptions (validity of quantum mechanics, no-signalling, independence of settings, secure laboratories, correct implementation of the protocol, honest data handling, etc.), can be converted into rigorous lower bounds on the entropy of the outputs. [24–26,37]

Even if a device exhibits a strong Bell violation on some sample, there is no way—purely from physics and without auxiliary assumptions about the device and its operation—to prove in an *indisputable* way that all remaining *secret* outputs come from the same source and are generated in the same, well-characterised physical process. In particular, one can never rule out, with logical certainty, that the device behaves differently when not being tested, or that an adversary has stored or precomputed some of the outputs.

- In PV-EQRNG, the situation is conceptually similar. Public randomness tests on disclosed sequences can provide strong evidence (and, within a suitable model, quantitative security bounds) that the undisclosed sequences have the same statistical properties. The multi-qubit entanglement structure ensures that secret and public strings are generated from the same measurement pattern and obey the same parity/XOR relations (cf. Clauses 7 and 8). Nevertheless, these conclusions still rely on assumptions about the physical device, its stability over time, the validity of the entanglement model and the correctness of the implemented protocol. They cannot yield an absolute, assumption-free guarantee that the secret randomness has exactly the same properties as the tested public part.

The only fundamentally reasonable scenario is therefore that the physical owner/controller of a QRNG device, who has direct control over the hardware and its environment, wishes to verify its quality to a level that is sufficient for their application and threat model. Even in this scenario, however, several non-trivial issues arise:

- There is no general mathematical theorem stating that (even idealised) infinite statistical testing of measurement-result correlations —for example, confirming the existence and quality of quantum entanglement by estimating Bell/CHSH parameters or multi-partite correlation functions —is equivalent to applying a *universal* randomness test in the sense of algorithmic randomness theory. Universal tests of randomness (e.g. in the sense of Martin-Löf) do exist, but they are not computable and therefore cannot be implemented as practical iterative statistical tests on a physical device.

- Likewise, there is no mathematical proof that finite statistical testing of Bell/CHSH violation is equivalent to testing the randomness of a *finite* generated sequence by exhaustively checking the empirical frequencies of all patterns of length up to the sequence length against their ideal probabilities. Such an exhaustive pattern test scales exponentially with pattern length (there are 2^k different binary patterns of length k), and is therefore infeasible in practice beyond modest k. In contrast, Bell-type tests involve a fixed set of correlators whose number does not grow with the tested sequence length; longer sequences only improve the confidence with which those correlators are estimated.

- The experimental procedures used to certify entanglement and to test Bell/CHSH inequalities are themselves subject to various imperfections (e.g. detector inefficiencies, miscalibrations, time-tagging errors and other implementation loopholes) which can mask imperfections of the underlying entanglement. In other words, the observed violation may be limited not only by the quality of entanglement, but also by errors in the process of entanglement certification.

- The computational resources of the QRNG owner (or the system that integrates the QRNG, such as a terminal, server, or embedded controller) are always finite and, in realistic deployments, often quite modest. This places a practical ceiling on the complexity and depth of locally executed randomness tests and statistical analyses on secret outputs.

Even if one views Bell/CHSH-based certification and classical randomness testing as parts of a single, idealised randomness-certification workflow, one still faces the fundamental limitation that perfect "certainty" about randomness is unreachable: any physically realisable statistical

test or certification procedure can only bound the probability that the device's behaviour deviates from the ideal model; it cannot reduce that probability to zero. Approaching very high confidence levels typically leads to resource requirements that scale superlinearly (and, in many simple test families, exponentially) with the target confidence and with the length and structure of the tested sequences. Locally, those resources are always limited.

In this perspective, the PV-EQRNG protocol offers a qualitative advantage over purely DI-QRNG concepts with respect to *who* must provide the computational resources. While in both DI and PV-EQRNG architectures entanglement certification can (in principle) be carried out, PV-EQRNG protocols are explicitly designed so that arbitrarily complex statistical tests on one of the generated sequences can be safely outsourced and performed publicly by one or more third parties, without compromising the secrecy of the remaining sequences that will later be used cryptographically.

Any concept of randomness certification performed *on the secret strings themselves* by anyone other than the physical owner/controller of the QRNG is therefore inherently limited: a remote party cannot check a secret sequence without seeing it. In particular, QRNG-as-a-service architectures (for example, remote QRNG access over the network, or services based on small entanglement-capable quantum computers) always require a high degree of trust in the service provider. Security in such models ultimately reduces to the security of the classical mechanisms used to deliver and authenticate the random bits (e.g. asymmetric cryptography, secure channels and hardware security of the provider). From the end-user's perspective, the overall security level is then limited by the weakest link in this classical cryptographic and operational stack, rather than by the intrinsic quantum randomness alone.

10.7 Summary of mandatory security requirements

An EQRNG protocol that claims conformance with this Clause SHALL:

- declare its security objectives and adversarial model(s) (M1–M3);
- provide a threat analysis covering at least the categories in this Clause;
- specify how parity-error indicators, entanglement metrics and device parameters influence entropy estimates and acceptance criteria;
- define public-verification data flows such that disclosure of verification strings does not compromise the secrecy of cryptographic outputs, within the stated adversarial model;
- provide a mapping from observed statistics to a conservative lower bound on conditional min-entropy, used as input to the extraction stage (Clause 12).

11 Implementation profiles and physical realizations

This Clause defines abstract implementation profiles for EQRNG protocols and describes typical physical realizations, with emphasis on photonic multi-qubit entanglement as demonstrated in [2, 6, 10–12]. It operates at an architectural level; detailed device-level requirements and calibration procedures are specified in platform-specific implementation guidelines and conformance test suites.

The profiles described here are intended to capture key design patterns; an implementation MAY define additional profiles provided they remain compatible with the functional and security requirements of Clauses 9 and 10.

11.1 General implementation considerations

Any EQRNG implementation SHALL clearly separate:

1. the *quantum entropy source*, where entangled multi-qubit states are prepared, distributed and measured (e.g. photonic SPDC sources, multi-photon graph-state sources, or multi-qubit gates on trapped ions or superconducting qubits);
2. the *classical control and acquisition subsystem*, which configures quantum operations (gates, phase shifters, modulators), synchronises triggers, stores raw measurement outcomes and handles data flow to verifiers and users;
3. the *post-processing subsystem*, which performs entropy estimation, randomness extraction and statistical testing in accordance with Clause 12; and
4. the *public verification interface*, where applicable, used to deliver verification strings and receive test results from a public verifier or verification centre (VC) [1, 4, 11].

Interfaces between these subsystems SHALL be specified in a way that supports security analyses of Clause 10 and interoperability with external systems. In particular:

- quantum–classical boundaries (e.g. detector outputs, timing signals) SHALL be documented and protected against tampering;
- data formats for raw, intermediate and final outputs SHALL be specified, including bit ordering and metadata;
- control interfaces SHALL be access controlled, authenticated and auditable.

11.2 Reference implementation profiles

The following reference implementation profiles are defined. A concrete device MAY claim conformance to one or more profiles.

11.2.1 Profile P1: Three-qubit PV-EQRNG with public verification

Profile P1 corresponds to the minimal practical EQRNG realised with $n = 3$ entangled qubits in states of the form described in [2, 10, 11]. In this profile:

- The quantum source SHALL prepare three-qubit entangled states that are equal superpositions of computational basis states with fixed parity and equal probabilities (as in Eqs. (12)–(15) of [10]), realising the Jacak-type three-qubit parity-entangled states.
- Local projective measurements in the computational basis SHALL yield three classical bit strings X_A, X_B, X_C satisfying an XOR relation of the form $X_A \oplus X_B = X_C$ up to an observed rate of parity violations [2, 11].
- One string (e.g. X_A) SHALL be designated as the primary verification string; one string (e.g. X_B) SHALL be designated as a cryptographic output after extraction; the remaining string SHALL be reserved as never-disclosed auxiliary secret in accordance with [2, 10].
- The physical realization MAY use polarization qubits, time-bin qubits, path-encoded qubits, or other degrees of freedom, provided that the resulting state is equivalent (up to local unitaries) to the required three-qubit parity-entangled state.

The implementation SHALL specify:

- the method of entanglement generation (e.g. SPDC in nonlinear crystals, integrated photonic sources);
- the optical or physical path layout, including beam splitters, waveplates, fibre links and detectors;
- synchronisation and timing constraints (coincidence windows, jitter tolerance);
- calibration procedures for maintaining entanglement quality, referencing techniques such as quantum state tomography, Bell-inequality tests or entanglement witnesses [7, 8, 35];
- typical and maximum achievable bit rates and their dependence on pump power, entanglement visibility and detector performance, as in [2, 11].

11.2.2 Profile P2: Four-qubit photonic PV-EQRNG

Profile P2 covers four-qubit photonic implementations, such as those using photon pairs entangled in polarization and path degrees of freedom [12].

In this profile:

- The source SHALL produce two photons entangled in polarization (e.g. Bell state $\left|\Psi^+_{AB}\right\rangle$) which are then mapped through polarising and non-polarising beam splitters, half-wave plates and other linear optical elements into a four-qubit entangled state distributed across polarization and path modes A, B, C, D [12].
- The generated state SHALL be equivalent (up to local unitaries) to a four-qubit parity-entangled state in which computational basis states with a fixed parity occur with equal probability, enabling XOR constraints such as

$$X_A \oplus X_B \oplus X_C \oplus X_D = 0 \tag{53}$$

  or other specified linear relations.
- Measurement setups at the two spatially separated stations (e.g. Alice and Bob) SHALL allow independent local projective measurements on each subsystem and SHALL support multiple configurations for:
  1. PV-EQRNG operation (one or more sequences disclosed);
  2. entanglement verification (e.g. CHSH tests, visibility measurements);
  3. optional key-generation or additional randomness-generation modes, where applicable [12].
- The implementation SHALL include mechanisms to characterise and monitor entanglement visibility, CHSH parameter S, parity-error rates and noise processes, and SHALL map these to bit-generation rate, test performance (e.g. NIST tests) and entropy estimates in a way consistent with observed data [11, 12].

Figure 7 shows a gate-level realisation of a four-qubit random-correlation generator with three auxiliary qubits, aligned with the abstract description of Profile P2.

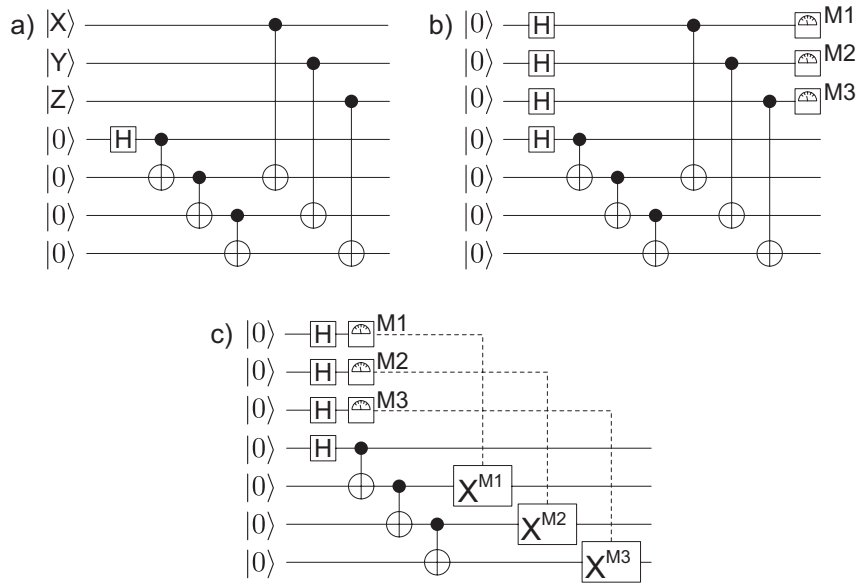

Figure 7: Quantum gate scheme of a random-correlation entanglement generator with a four-qubit entangled state and three auxiliary qubits X, Y and Z. Subfigure (a) corresponds to a fixed four-qubit entangled-state type, while subfigures (b) and (c) include a random selection among several such types. Double lines indicate classical control paths carrying measurement outcomes that influence subsequent gate operations. This figure SHALL serve as a reference pattern for four-qubit PV-EQRNGs in Profile P2.

11.2.3 Profile P3: Multi-qubit scalable EQRNG

Profile P3 generalises P1 and P2 to $n > 4$ entangled qubits, in line with the evolution described in [2, 4, 10].

In this profile:

- The implementation SHALL define a family of n-qubit entangled states that generalise the parity-based constructions, ensuring that measurement in the computational basis yields n bit strings with identical or near-identical statistical quality and specified XOR constraints, as in Eqs. (13)–(15) of [10].
- The number of usable secret sequences SHALL be at most $n-2$, with at least one sequence reserved for public verification and at least one sequence reserved as non-disclosed auxiliary secret, as per [2, 10].
- The architecture MAY be photonic (e.g. multi-mode integrated waveguides, multi-photon graph states [10]), trapped-ion, superconducting qubit, or other scalable platform, provided that it maintains the required entangled-state family and supports the public-verification workflow.
- The device SHALL support configuration of the block size, number of sequences used for verification, and the mapping of physical qubits to logical sequences, and SHALL document the effect of these choices on entropy, throughput and implementation complexity [4, 6].

Figure 8 illustrates gate-level constructions for three-qubit, four-qubit and generic $(k+1)$-qubit entanglement generators that are compatible with Profile P3. These schemes SHALL be interpreted as reference patterns for scalable Jacak-type EQRNG implementations.

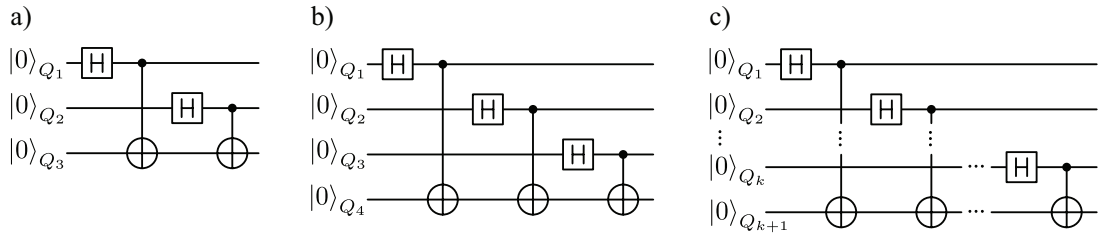

Figure 8: Representative quantum gate schemes for entanglement-based QRNGs. Panel (a) shows a circuit for a three-qubit protocol, panel (b) a four-qubit extension, and panel (c) a general $(k+1)$-qubit construction. Each circuit follows the Jacak-style pattern of applying single-qubit Hadamard gates and controlled operations to generate families of parity constrained entangled states. Double lines represent classical control wires associated with measurement results that condition later gates. Systems claiming conformance to Profile P3 SHALL implement gate patterns that are locally equivalent to one of these schemes.

11.3 Non-photonic implementations (informative)

Non-photonic EQRNGs MAY be built on trapped ions, neutral atoms, superconducting circuits, spin qubits, or hybrid platforms, following the same multi-qubit entanglement and parity principles. In such cases the general requirements of this Clause still apply, but the physical-layer details (e.g. cooling, trapping, microwave control, decoherence management) fall outside the scope of the present document and SHALL be specified in technology-specific implementation guides.

11.4 Integration with external systems

Where an EQRNG is integrated with cryptographic systems (e.g. QKD, secure key management services, hardware security modules), the implementation SHALL ensure that:

- the EQRNG entropy source is cryptographically independent of pseudorandom generators or other deterministic components used in the same system;
- interfaces to key-management systems and, where relevant, QKD key-delivery APIs (such as those specified in [18]) are clearly separated from public-verification interfaces;
- security analyses consider potential cross-coupling between EQRNG and other subsystems, in particular side channels that might link entangled states used in EQRNG and other quantum subsystems;
- the role of the EQRNG in the overall security architecture (e.g. seed generation for PRNGs, direct supply of keys) is documented and consistent with the assumptions in the cryptographic protocol specifications.

Figure 9 provides a high-level protocol diagram of a multi-qubit entanglement-based QRNG with public randomness verification, combining the quantum-entropy source, classical control, extraction and verification subsystems described in this Clause.

11.5 Implementation-profile conformance

An implementation claiming conformance with a profile defined in this Clause SHALL:

1. identify the profile(s) (P1, P2, P3, or additional profiles defined in future extensions) and the underlying protocol family as in Clause 8;

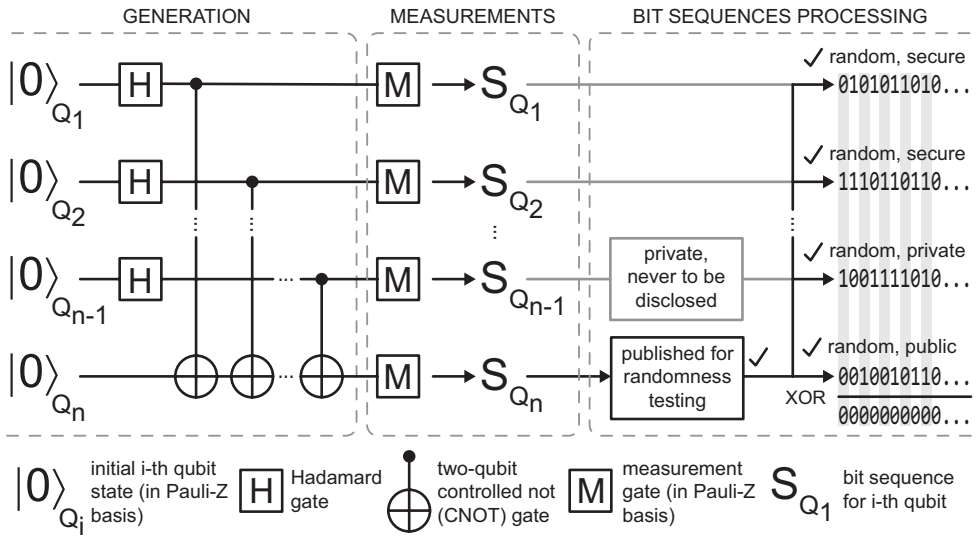

Figure 9: Protocol-level architecture of a multiqubit entanglement-based QRNG with public randomness verification. The diagram shows the preparation of multipartite entangled states, local measurements producing multiple bit sequences, classical control and synchronisation, the randomness extraction and post-processing module, and the interface to one or more Verification Centres (VCs) for public testing. Implementations claiming conformance to PV-EQRNG profiles SHALL provide an architecture that is functionally equivalent to this structure.

2. provide a high-level schematic of the quantum and classical subsystems, including entanglement generation, measurement, control and interfaces;

3. document calibration, monitoring and fault-handling strategies for maintaining entanglement quality and controlling parity-error rates;

4. demonstrate that the generated states and measurement outcomes satisfy the structural properties (parity, XOR relations, indistinguishability of sequences) used in the security and extraction analyses;

5. document the achieved bit rates, test results (e.g. NIST, TestU01) and observed entanglement metrics, including their stability over time [2, 11, 12].

12 Randomness extraction, post-processing and statistical testing

This Clause specifies requirements for transforming raw measurement outcomes from EQRNG implementations into final random outputs suitable for cryptographic and other high-assurance applications. It covers entropy estimation, randomness extraction, optional post-processing, and statistical testing, including publicly verifiable testing.

The requirements apply to all EQRNG classes and profiles, with specific attention to multiqubit parity-based schemes with public randomness verification as in [2, 4, 10–12].

12.1 Raw data and entropy estimation

Raw data are defined as the bit strings obtained directly from projective measurements on entangled quantum states, prior to any extractor or post-processing. For PV-EQRNGs this includes both verification strings and candidate secret strings (e.g. X_A, X_B, X_C, X_D) [2, 10–12].

1. Implementations SHALL record sufficient metadata (e.g. block size, time stamps, basis settings, entanglement metrics, parity-error rates, detector statistics) to support reproducible entropy estimation and post-hoc forensic analysis.

2. Entropy estimation SHALL provide a conservative lower bound on the conditional min-entropy of the raw secret strings given the adversary's side information, consistent with the declared adversarial model (M1–M3) and employing techniques such as those described in [2, 7, 11, 16, 36, 37].

3. For PV-EQRNGs, the structural relations between sequences (e.g. XOR constraints) and the observed rate of parity violations SHALL be explicitly included in the entropy model, following the analyses in [2, 10–12].

4. The entropy model SHALL state clearly the assumptions on independence between rounds, stationarity of the source, and possible memory effects; finite-size corrections SHALL be applied where appropriate.

12.2 Randomness extraction and entropy compression

Randomness extraction transforms raw data with imperfect entropy into nearly uniform random bits, typically using strong seeded extractors based on two-universal hashing or related constructions [36, 47–49].

12.2.1 Extractor requirements

1. The extraction function SHALL be a strong seeded randomness extractor (e.g. Toeplitz hashing, families of two-universal hash functions, Trevisan-type extractors) suitable for use against quantum side information, as required by [36, 37].

2. The seed used by the extractor SHALL be generated from a source independent of the raw EQRNG data or SHALL be derived from the same EQRNG under a composable security analysis that accounts for seed reuse. In all cases, seed generation and handling SHALL be documented, including seeding frequency and any re-keying policy.

3. The extraction parameters (output length, security parameter, seed length) SHALL be chosen such that the trace distance between the extractor output and the ideal uniform distribution is at most $2^{-\lambda}$ for a configurable security parameter λ. The choice of λ SHALL be documented and justified.

4. In PV-EQRNG scenarios where verification strings are disclosed to a public verifier, extraction SHALL be applied only to secret strings, and the entropy analysis SHALL condition on any information revealed by or to the verifier, including the verification string itself, parity error-rate estimates and any published statistics [2, 11, 12].

12.2.2 Entropy compression in the presence of errors and side information

Implementations **SHALL** treat any observed deviation from the ideal entanglement correlations or ideal device model as a reduction of the effective min-entropy of the raw output strings.

- For Jacak-type PV-EQRNG protocols and related multi-qubit parity schemes, the relevant observables include, but are not limited to:

  – the empirical frequency with which the correlation rule is violated (e.g. observed rate of positions where $C_i \neq A_i \oplus B_i$ or $A_i \oplus B_i \oplus C_i \oplus D_i \neq 0$);

  - entanglement visibility or deficits in Bell-type parameters (e.g. CHSH parameter S below its ideal value);
  - detector error rates, dark counts and other hardware-level error indicators [11, 12].

- The implementation **SHALL** incorporate these observables into its entropy-estimation model, yielding a conservative lower bound $H_\infty(R_{\text{raw}} \mid E)$ on the min-entropy of the raw output conditioned on potential side information E.

- A randomness extractor **SHALL** then compress R_{raw} to an extracted output R_{ext} of length

$$\ell \leq H_\infty(R_{\text{raw}} \mid E) - \Delta,$$

  where Δ is a security margin determined by the target trace-distance parameter and the finite-size analysis. The choice of extractor family and implementation (e.g. Toeplitz matrices, FFT-based hashing) **SHALL** be documented.

- If the estimated min-entropy per bit falls below a specified threshold $h_{\min}$ (e.g. due to excessive correlation errors or loss of entanglement quality), the implementation **SHALL** either abort the affected block or mark the corresponding output as not meeting the target security level and SHALL NOT label it as cryptographically secure.

In implementations that re-use hardware or analysis tools originally developed for QKD or DI QRNGs, it may be convenient to express error rates using QKD terminology (e.g. "quantum bit error rate", QBER) and to adopt privacy-amplification-style formulas for the output length. In this case:

- The use of QBER-based formulas **MAY** be adopted as an implementation choice, provided that the mapping from the measured error parameter(s) to $H_\infty(R_{\text{raw}} \mid E)$ is clearly specified, justified for the EQRNG setting and conservative.

- Any reuse of QKD finite-size or privacy-amplification analysis **SHOULD** be explicitly justified as applicable to the EQRNG threat model, and all assumptions (e.g. on independence of rounds, stationarity, and adversary capabilities) **SHALL** be stated.

The term "privacy amplification" **SHALL NOT** be used in this standard for the generic post-processing of EQRNG outputs; instead, the generic term "randomness extraction" **SHALL** be used. The expression "privacy amplification" **MAY** be used only in informative notes referring to QKD-derived analyses when an EQRNG protocol is tightly integrated with a QKD system and the assumptions can be clearly matched.

12.3 Optional post-processing

Beyond core extraction, implementations MAY apply additional post-processing steps, such as:

- format conversion (e.g. mapping bits to integers, floating-point variates, or other statistical distributions);

- buffering, framing and encoding for transport protocols and storage (e.g. framing random data into records, packets or messages);

- combination with pseudorandom generators to expand high-quality entropy into longer streams under well-defined assumptions [15, 16].

Such post-processing SHALL NOT be relied upon to increase entropy or repair systematic biases; its role SHALL be clearly distinguished from extraction. If post-processing includes deterministic expansion (e.g. PRNGs), the device documentation SHALL state clearly which portions of the output are information-theoretically random and which are computationally secure only under additional assumptions.

12.4 Statistical testing

Statistical testing complements, but does not replace, entropy-based security analysis. Testing SHALL be used for:

1. **Design-time validation.** Offline testing of large data sets from prototype devices, using established suites such as NIST SP 800-22, TestU01, and QRNG-specific tests [2, 7, 8, 11, 17, 28].
2. **Run-time health testing.** Online tests applied to shorter blocks to detect catastrophic failures, drifts or mode changes, as recommended in [15, 16, 19]. These tests SHALL be chosen to be lightweight enough not to compromise throughput while still detecting significant deviations.
3. **Public randomness verification.** Testing conducted by an external verifier or VC on disclosed verification strings in PV-EQRNG protocols [1, 2, 4, 11, 12].

12.4.1 Test selection and configuration

- Test suites SHALL include tests targeting monobit frequency, runs, serial correlation, spectral properties, linear complexity, pattern occurrences and other relevant aspects, chosen in light of known weaknesses of QRNG implementations [7, 8, 11, 17].
- The significance level(s), block sizes and total sample sizes SHALL be specified and justified. Multiple-comparison effects (e.g. p-value distributions across many tests) SHALL be taken into account when interpreting results.
- For PV-EQRNGs, the public verifier's test configuration SHALL be published and SHALL be reproducible by independent parties using the published verification strings [2, 11, 28].
- Where very large test batteries or long sequences are used (e.g. cloud or HPC-based VCs as envisaged in [2]), the computational assumptions (e.g. maximum testing delay) SHALL be documented.

12.4.2 Acceptance criteria and actions

1. Implementations SHALL define objective acceptance criteria (e.g. bounds on the fraction of tests that may fail, or p-value distribution tests) and SHALL specify the actions to be taken on failure (e.g. discard outputs, raise alarms, trigger recalibration).
2. For run-time health tests, transient failures MAY trigger temporary suspension of output or switching to a degraded mode; persistent failures SHALL result in output suppression until the root cause is addressed.
3. In PV-EQRNG protocols, if the verifier rejects the verification string, the corresponding secret strings SHALL NOT be used and SHALL be securely discarded, in accordance with [1, 2, 11, 12].

12.5 Conformance requirements for extraction and testing

An EQRNG protocol and implementation claiming conformance with this Clause SHALL:

- provide a documented entropy model and conservative min-entropy bounds for raw outputs under the declared adversarial model;
- implement a strong seeded extractor with specified security parameter and seed management, in line with [36, 37, 49];

- clearly separate extraction from non-entropic post-processing and document which outputs are information-theoretically random;
- specify design-time and run-time statistical test suites, parameters and acceptance criteria, and document how test results influence operational decisions (e.g. abort, degraded mode);
- in PV-EQRNG settings, define the interaction between public testing and private extraction, ensuring that disclosure of verification strings and test outcomes is properly accounted for in the entropy and security analysis, as in [2, 10–12].

13 Use cases and deployment profiles

This Clause maps the entanglement-based QRNG (EQRNG) profiles defined in Clauses 8, 9, 10 and 11 to application domains and deployment patterns.

Use cases are grouped by the required assurance level and by whether public randomness verification, multi-party functionality, or device-independence are required. The general QRNG application guidance of [7–9] and the EQRNG conceptual framework of [2, 6, 10] are taken into account.

13.1 General principles

- EQRNG outputs used for cryptographic or safety-critical applications SHALL be the *extracted* outputs defined in Clause 12, not raw detector data.
- For each deployment the required conformance profile (Family, Class and Implementation Profile) as defined in Clauses 8–11 SHALL be specified.
- Where regulatory or contractual frameworks impose additional requirements on entropy sources (e.g. ISO/IEC 18031, NIST SP 800-90B, ITU–T X.1702, TEC GR/QS-91020) [15, 16, 19, 33], the EQRNG deployment SHALL satisfy both those generic requirements and the EQRNG-specific requirements of this standard.
- Use of EQRNGs in roles beyond those listed in this Clause MAY be considered, provided the entropy and threat models are explicitly analysed and documented.

13.2 Cryptographic key and seed generation

13.2.1 High-assurance key generation

EQRNGs are natural candidates for generating secret keys and seeds for cryptographic mechanisms including, but not limited to, symmetric encryption, message authentication, public-key schemes and post-quantum cryptography [7, 8].

- Secret keys and seeds used directly in cryptographic modules (e.g. HSMs evaluated against FIPS 140-3 or ISO/IEC 19790) [50, 51] **SHALL** be generated by EQRNG profiles that:
  - meet or exceed the entropy and security requirements of Clauses 9–12;
  - declare at least adversarial model M1 (classical external adversary) and *SHOULD* declare at least M2 (quantum side-information adversary);
  - provide public or third-party verifiability of randomness (Profiles P1–P3 with public verification) when required by policy or regulation.
- For long-term or root keys, operators **SHOULD** favour profiles with public verification and multi-qubit entanglement (Families B or D; Classes EQRNG-1 or EQRNG-2; Implementation Profiles P1–P3) as these allow independent assessment of randomness quality without key disclosure [1, 2, 11, 12].

13.2.2 Seeding deterministic generators

Deterministic random bit generators (DRBGs) in cryptographic modules are often seeded from physical sources [15, 16].

- When an EQRNG is used to seed a DRBG, the entropy contributed by the EQRNG **SHALL** be sufficient on its own to meet the security goals for the DRBG, i.e. a seed of length s **SHALL** provide at least s bits of min-entropy under the relevant adversarial model.
- The seeding interface **SHALL** ensure that seed bits are not reused in a way that undermines the min-entropy guarantees, unless such reuse is covered by a composable security proof.
- Where public verification is available, EQRNG operators **SHOULD** provide evidence that verification strings obtained under the same operating conditions pass the specified test suites with the required confidence.

13.3 Public randomness services and beacons

Randomness beacons provide publicly accessible sequences of random values that can be used in lotteries, public decision-making, scientific experiments and cryptographic protocols [27]. Device-independent randomness expansion has been proposed and implemented for such services [24, 26, 27].

- EQRNG profiles with public verification **SHALL** be preferred for public randomness services where transparency and auditability are mandatory. The design **SHALL** allow any external party to re-run the randomness tests applied by the provider.
- Where the service simultaneously provides public randomness and secret randomness (e.g. Jacak-type PV-EQRNGs and related schemes) [1, 2, 10–12], the mapping between public and secret outputs **SHALL** be documented and analysed as in Clauses 10 and 12.
- For deployments that require traceable randomness (e.g. in metrology, standardisation trials or public audits) the service **SHALL** document:
  - the EQRNG profile and implementation profile used;
  - the test suites and parameters (NIST SP 800-22, TestU01, DI or SDI certification where applicable);
  - the archival strategy for raw and processed data and for public verification reports.

13.4 Multi-party and distributed applications

Multi-qubit EQRNG protocols naturally support multi-party use cases, including secret splitting and correlated randomness generation across distributed systems [2, 6, 10].

13.4.1 Secret splitting and threshold control

- EQRNG Families C and D (GHZ-type and chain-type multi-qubit entanglement) **MAY** be used to generate correlated bit strings shared among multiple parties. Protocols **SHALL** specify which coalitions of parties can reconstruct a given secret string and which cannot.
- In threshold-control applications (e.g. joint authorisation of high-value transactions, nuclear command-and-control or critical infrastructure operations), multi-party EQRNG schemes **SHALL** ensure that:

– the absence of one or more required parties provably prevents reconstruction of the secret randomness;
– any public testing conducted on one party's data is properly accounted for in the entropy analysis of the remaining parties' data.

13.4.2 Cloud and network-based EQRNG services

- When EQRNG functionality is provided as a network service, the API and security boundaries **SHALL** be explicitly defined. In particular, the entropy source and extraction logic **SHALL** be confined within a trusted execution boundary.
- For cloud-based deployments the provider **SHALL** document how entanglement is distributed across network links, what assumptions are made about intermediate nodes, and how end users can verify that they receive independent high-entropy outputs.
- Where EQRNG services are combined with QKD infrastructures, the interactions between the QRNG and QKD components (e.g. for basis selection or privacy amplification) **SHALL** be documented, and cross-dependencies **SHALL** be considered in the security analysis.

13.5 Scientific and calibration applications

- EQRNG devices **MAY** be used for scientific experiments requiring true randomness (e.g. Bell-test experiments, Monte Carlo simulations sensitive to bias, tests of fundamental physics), provided the limitations of the entropy model and statistical tests are documented.
- Entanglement-based structures (e.g. the XOR consistency rule in three-qubit Jacak schemes or multi-parity checks in multi-qubit schemes) **MAY** also be used as calibration and diagnostic tools for multi-qubit platforms, as deviations from the predicted parity relations provide sensitive indicators of decoherence and crosstalk [2, 6, 10, 12].

13.6 Applicability matrix

Annexes to this standard (informative) **MAY** provide matrices mapping:

- EQRNG Families (A–D), Classes (EQRNG-1–3) and Implementation Profiles (P1–P3),
- to use cases such as key generation, public beacons, multi-party control and calibration,

together with recommended minimum entropy targets, test suites and adversarial models for each combination.

14 Conformance assessment and profile definitions

This Clause defines how to assess conformance of EQRNG protocols and implementations to this standard and introduces conformance profiles that enable interoperable specification and evaluation.

Conformance assessment **SHALL** cover protocol specification, implementation design, statistical behaviour and security properties under the declared adversarial model.

14.1 Conformance items

The following items **SHALL** be assessed for any claimed EQRNG conformance:

1. **Protocol specification.** Completeness and consistency of the abstract protocol description, including entangled-state family, measurement pattern, mapping between quantum outcomes and classical sequences, and role of public verification.
2. **Entropy and security model.** Correctness and conservativeness of the entropy estimation model, including treatment of imperfections, QBER, and potential quantum side information, in line with [2, 7, 10, 11, 36, 37].
3. **Implementation architecture.** Separation of quantum, classical control, post-processing and verification subsystems as required by Clause 11.
4. **Statistical behaviour.** Empirical performance under test suites and health tests defined in Clause 12 (design-time and run-time).
5. **Documentation and traceability.** Availability of documentation and logs allowing independent verification of conformance claims, including test reports and calibration procedures.

14.2 Conformance profiles

To facilitate comparison and procurement, this standard introduces *EQRNG conformance profiles*. A profile is a tuple

$$\Pi = (\text{Family}, \text{Class}, \text{Implementation}, \text{Security}, \text{Verification}),$$

where:

- **Family** is one of the protocol families defined in Clause 8 (e.g. two-qubit Bell, Jacak three-qubit parity chain, GHZ multi-party, DI/SDI schemes).
- **Class** is EQRNG-1, EQRNG-2 or EQRNG-3 as defined in Clause 1, corresponding to device-dependent, SDI-like and DI-like security models, respectively.
- **Implementation** is one of the implementation profiles P1–P3 (or extensions) defined in Clause 11.
- **Security** specifies the adversarial model (M1–M3 from Clause 10), the target min-entropy per bit, and the security parameter (e.g. trace distance $2^{-\lambda}$).
- **Verification** specifies whether public verification is supported and, if so, which test suites and interfaces are used.

Profiles **SHALL** be denoted by profile identifiers, for example:

- `EQRNG-1/B/P1/M2/PV` for a device-dependent three-qubit Jacak EQRNG (Family B, Profile P1) secure against M2 with public verification.
- `EQRNG-3/A/P1/M3/DI` for a DI Bell-pair-based QRNG using observed Bell violation with no public verification of application strings.

14.3 Conformance assessment process

Conformance assessment **SHALL** be conducted according to a documented process that includes, at minimum:

1. **Document review.** Verification that the protocol and implementation documentation covers all items required by Clauses 9–12 and clearly specifies the claimed profile Π.
2. **Laboratory testing.** Execution of physical-layer and statistical tests using independent measurement equipment and toolchains where possible. For photonic implementations this **SHALL** include verification of entanglement visibility, Bell parameters or entanglement witnesses, as applicable [11, 12, 35].
3. **Security evaluation.** Analysis of the device under the claimed adversarial model, including inspection for obvious side channels and review of entropy estimation and extraction methods.
4. **Report generation.** Production of a conformance report summarising the tests performed, the results obtained and any deviations or conditions. The report **SHALL** indicate whether the device conforms to the claimed profile(s) and under what assumptions.

Conformance evaluation may be performed by internal teams, independent laboratories (e.g. accredited under ISO/IEC 17025) or certification bodies. Where results are used to support regulatory or high-assurance deployments, independent evaluation is strongly recommended.

14.4 Levels of conformance

The following qualitative levels of conformance are defined:

Base conformance. The implementation satisfies all mandatory requirements of Clauses 9–12 and declares at least one profile Π with documented test results.

Enhanced conformance. In addition to Base conformance, the implementation:

- undergoes independent laboratory testing;
- provides public access to representative verification data and test configurations;
- offers additional device-independent or SDI assurances where applicable (e.g. embedded Bell tests).

Certified conformance. The implementation has been evaluated by a recognised certification body according to a formal scheme that references this standard and possibly other standards (e.g. ISO/IEC 19790, FIPS 140-3). Certified conformance is outside the direct scope of this document but **MAY** be based on it.

14.5 Profile evolution

New profiles, families and implementation patterns **MAY** emerge as entanglement platforms and security analyses develop. Future revisions of this standard **SHALL** provide mechanisms for registering and documenting such profiles while maintaining backward compatibility with existing deployments.

15 Future work and extensions

This Clause summarises technical and standardisation topics that are expected to require further work. It is informative in nature but provides guidance for future revisions of this and related standards.

15.1 Public verifiability under secrecy versus device-independent certification

A large body of work on entanglement-based QRNGs is devoted to various forms of *certification* of randomness: device-dependent certification based on detailed physical models, [7–9] semi-device-independent (SDI) certification under dimension or source assumptions, [13, 14, 30, 32] and fully device-independent (DI) certification based on Bell inequality violations. [24–27, 29] In all of these schemes, entanglement plays a central role: it enables either a non-classical entropy source (Bell pairs, GHZ states, single-particle entanglement) or non-local correlations used to bound an adversary's information. The output bits are then said to be *certified* random in the sense that, under the assumptions of the relevant model, a lower bound on the conditional min-entropy of the output string is derived from observed statistics such as CHSH violation, visibility or error rates.

However, there is an important conceptual distinction between:

(a) *certifying that a device generates randomness according to a specified quantum model*, and

(b) *publicly verifying the randomness quality of specific bit strings that must remain secret for cryptographic use.*

Existing DI and SDI QRNGs primarily address (a). The Jacak entanglement QRNG concept and subsequent EQRNG standards, together with recent photonic implementations, [1–5, 10–12] explicitly target (b): *publicly verifiable randomness under secrecy.*

Device-independent certification: what is publicly visible?

In a canonical DI QRNG, an experimenter operates two or more nominally independent black-box devices supplied with random measurement settings; the devices share entangled states and produce classical outputs. From the observed input–output statistics, in particular a Bell inequality violation (e.g. CHSH parameter $S > 2$), one can derive a lower bound on the min-entropy of one party's output string conditioned on any quantum side information available to an adversary. [24–27, 37] Similar arguments apply for SDI schemes based on dimension witnesses or source assumptions. [13, 14, 30, 32]

The key point is that the DI/SDI *certification test* uses a subset of the raw input–output data:

- basis choices and corresponding outcomes in "test" rounds are used to estimate Bell parameters or other witnesses;
- the remaining rounds are used to form the raw random output to be extracted and consumed.

An external observer can in principle be shown the test data—for example a table of settings and outcomes from a designated subset of rounds—and can recompute the Bell violation or witness; this is the usual sense in which experimental demonstrations of DI or SDI QRNGs are "reproducible". [24–27, 29]

However, when the DI QRNG is used as a *secret key* source, the raw output string destined for cryptographic use cannot be fully disclosed to external verifiers without destroying its secrecy. What can be revealed is limited to:

- summary statistics (Bell parameters, estimated error rates, entropy bounds) computed by the device owner; and/or
- perhaps a small publicly disclosed sample of output bits, which then cannot be used as secret key bits.

In other words, DI certification makes the *entropy bound* publicly checkable from summary statistics, but the *actual cryptographic bit string* remains opaque to third parties. The same tension exists in device-dependent QRNGs: extensive internal statistical testing is recommended by NIST SP 800-90B, ITU–T X.1702 and related standards, [16,19,31] but external parties must either trust the manufacturer's test reports or sacrifice secrecy by accessing the raw keys being tested.

Secrecy versus statistical transparency

At the bit-string level there is a simple structural tension:

- To run arbitrarily strong statistical tests (e.g. the full NIST SP 800-22 battery, TestU01, application-specific tests) on a given string, one must have full access to that string.
- But a bit string intended as a cryptographic secret key cannot be published without losing its value as a secret.

Standard QRNG architectures resolve this by limiting external visibility: randomness tests are performed internally by the device or by a trusted laboratory, and external users obtain only the resulting entropy estimates and pass/fail flags. [7–9]

This leads to an inherently asymmetric situation:

(i) The *device owner* can, in principle, log and test all raw outputs, but must be trusted not to misreport results.

(ii) External stakeholders (regulators, auditors, relying parties in critical infrastructures) cannot themselves subject the *actual keys* to arbitrarily strong statistical scrutiny without destroying secrecy; they must rely on summary statistics or manufacturer claims.

Device-independent certification improves the situation at the level of abstract entropy bounds, but does not by itself remove this asymmetry for cryptographic secret keys.

Jacak-type EQRNGs: structuring entanglement to decouple secrecy from testing

The Jacak entanglement QRNG concept and the associated EITCI reference standards propose a different resolution of this tension: generate, from each use of the entangled state, *several* classical bit strings with rigorously linked statistical properties, so that at least one string can be published for intensive testing while other strings remain secret but inherit the same randomness profile by construction. [1–4, 10]

In the three-qubit Jacak scheme, measurements on a chain-type entangled state $|\Psi_{XAB}\rangle$ (cf. Eq. (16)) yield three raw bit strings $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}$ satisfying an XOR relation such as

$$C_i = A_i \oplus B_i$$

for each round i in the ideal case. [2, 3] All three strings are individually unbiased and, up to the modelled noise, statistically indistinguishable. The protocol designates:

- one string (say $\boldsymbol{B}$) as the *secret* output;
- one string (say $\boldsymbol{C}$) as the *public* verification string, to be disclosed in full to one or more Verification Centres (VCs);
- one string ($\boldsymbol{A}$) as an internal control string, never disclosed.

Because of the entanglement structure and symmetry of the construction, any statistical test applied to $\boldsymbol{C}$—no matter how complex—constrains the joint distribution of $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})$ and hence the distribution of $\boldsymbol{B}$. [2, 4] In effect, the protocol provides a *publicly testable surrogate* for the secret key: $\boldsymbol{C}$ is open to arbitrary testing; successful tests on $\boldsymbol{C}$ then imply the desired entropy bounds on $\boldsymbol{B}$, without revealing any of its bits.

Recent photonic implementations by Islam *et al.* and Kolangatt *et al.* realise this idea on multi-qubit photonic platforms: they generate multi-string outputs with parity constraints, designate some strings as public test strings and others as private outputs, and demonstrate that published strings pass standard QRNG test batteries while the corresponding secret strings remain inaccessible. [11, 12] These experiments provide concrete evidence that the Jacak-type entanglement structure can decouple secrecy from testability at the bit-string level.

Why generic certified QRNGs cannot trivially emulate public verifiability under secrecy

Conceptually, one might ask whether a *generic* certified QRNG (e.g. a DI QRNG based on a Bell test) could simply "publish some function" $f(K)$ of a secret key K to allow public testing without revealing K. In general, there is a trade-off:

- If $f(K)$ preserves enough structure of K to allow strong statistical tests (e.g. f is a large subset of the bits or a low-entropy invertible mapping), then $f(K)$ also leaks substantial information about K and undermines secrecy.
- If $f(K)$ is chosen to be information-theoretically hiding (e.g. a cryptographic hash with a secret salt), then $f(K)$ does not permit meaningful statistical tests on the underlying bit pattern of K.

Without additional structure, there is no generic way to make a single secret string simultaneously *fully* available for testing and *fully* secret.

The Jacak EQRNG approach uses multipartite entanglement to engineer additional degrees of freedom: instead of a single string K, the protocol generates a *tuple* of strings $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C}, \dots)$ with provably linked statistics. [2,3,5,10] Public testing can then be performed on one component (or a subset of components) while another component is kept secret. The security argument relies not on a clever choice of f, but on the entangled-state structure and parity constraints that enforce statistical equivalence among the strings.

From this perspective, existing DI and SDI QRNGs offer powerful *source certification*: they show that a given device, observed in a laboratory, must produce high-entropy bits under mild assumptions. But, in their usual form, they do not offer *bit-string-level public verifiability under secrecy*: there is no native mechanism that would allow an external VC to test application-level random strings in full without revealing them.

We do not claim a formal impossibility theorem: in principle, other protocols or architectures might be devised that achieve the same combination of properties as the Jacak EQRNG, it is likely however that these protocols would be reducible to the same type of protocol and would also need to be based on quantum entanglement. To the best of current knowledge, Jacak-type multipartite entanglement constructions and their photonic realisations are the first to systematically address and demonstrate the *public-verification-under-secrecy* property at the bit-string level. [1–4, 10–12]

This suggests several future-work directions:

- extending public-verification EQRNG designs to higher-dimensional and many-body entangled states;
- integrating DI or SDI entropy certification with Jacak-type multi-string architectures to combine device-independent guarantees with publicly verifiable secrecy at the bit-string level;

- formalising "public verifiability under secrecy" as a distinct cryptographic primitive and exploring its relations to other primitives such as verifiable random functions and randomness beacons.

These directions complement the more conventional refinement of DI/SDI security models and entropy analyses discussed in the following subsections.

15.2 Refinement of entropy and security models

- Existing entropy analyses for Jacak-type PV-EQRNGs and related multi-qubit schemes [2, 6, 10–12] assume particular noise and independence models. Future work **SHOULD** refine these models, including:
  - explicit Markovian or non-Markovian descriptions of temporal correlations, following techniques such as those in [13];
  - tighter finite-size bounds on min-entropy using advanced tools from smooth entropy theory [36];
  - security analyses incorporating realistic side channels and cross-couplings in integrated photonic or solid-state platforms.
- Device-independent and semi-device-independent approaches [24–27, 29, 32] **SHOULD** be further integrated with the EQRNG framework, including formal mappings from observed Bell parameters or dimension witnesses to entropy bounds for multi-qubit parity structures.

15.3 Continuous-variable and hybrid EQRNGs

- While this standard focuses on discrete-variable (qubit/qudit) entanglement, continuous-variable (CV) entanglement in squeezed and cluster states offers alternative platforms for high-rate EQRNGs. Future work **MAY** extend the concepts here to CV entanglement, leveraging the substantial literature on CV QRNGs and entanglement certification.
- Hybrid schemes combining CV and discrete-variable entanglement **MAY** provide advantageous trade-offs between rate, security and implementation complexity, and **SHOULD** be analysed once prototypes become available.

15.4 Scalability and network integration

- As multi-qubit entanglement generation scales up (e.g. using integrated photonics, trapped ions or neutral atoms), EQRNG protocols with larger n become feasible. Future work **SHOULD** explore:
  - scalable constructions of parity-entangled states for large n that preserve the public-verification and secrecy properties;
  - routing and distribution of entangled modes over quantum networks and repeaters;
  - integration of EQRNG services with emerging quantum internet architectures.
- Interactions between EQRNGs and QKD or other quantum communication systems **SHOULD** be investigated in more detail to ensure that joint deployments do not compromise security and that potential synergies (e.g. shared entanglement resources) are properly utilised.

15.5 Standardisation and certification frameworks

- This document provides a technical reference standard for EQRNG protocols and implementations. Future work **MAY** include:
  - developing profile-specific conformance test suites and protection profiles analogous to those in Common Criteria or FIPS 140-3;
  - aligning EQRNG-specific standards with broader cryptographic module standards (ISO/IEC 19790, FIPS 140-3, ETSI QKD series) and with national QRNG requirements [19, 33];
  - defining reference implementations and test vectors for interoperability testing.
- Coordination with international standardisation bodies (e.g. ITU–T, ETSI, ISO/IEC, NIST) **SHOULD** be pursued to ensure consistent treatment of entanglement-based QRNGs across standards and regulatory frameworks.

15.6 Topological and geometric perspectives

The illustrative topological models of entanglement discussed in Clauses 6 and 8, building on [2, 10, 38, 39], suggest deeper connections between the topology of multi-qubit rotations and entanglement classes.

- Future theoretical work **MAY** explore how braid-group and knot invariants, topological entanglement entropy [40, 41] and geometric structures on state manifolds can be systematically used to classify and design EQRNG states with desirable correlation properties.
- If such approaches lead to practically relevant constructions (e.g. topologically protected entanglement patterns with robustness to local noise), subsequent revisions of this standard **SHALL** consider incorporating them as new protocol families.

15.7 Scaling of PV-EQRNG and effective reduction of testing complexity

15.7.1 Classical randomness testing as exponential pattern search

In the EITCI theoretical reference standard for EQRNG it is emphasised that classical randomness testing of a bit sequence can be formalised as a pattern-finding procedure. [3–5] Let $x \in \{0,1\}^L$ be a finite binary string of length L. For each binary word $w \in \{0,1\}^k$ of length $k \le L$ one may define a *pattern-frequency test* that computes the empirical frequency $f_w(x)$ with which w occurs as a contiguous substring of x and compares $f_w(x)$ to the ideal Bernoulli(1/2) expectation. Deviation beyond a prescribed tolerance is interpreted as evidence against ideal randomness.

The space of binary patterns of length k has cardinality 2^k, and the total number of distinct patterns of length at most K is

$$N_{\mathrm{pat}}(K) \;=\; \sum_{k=1}^{K} 2^k \;=\; 2^{K+1} - 2, \tag{54}$$

which grows exponentially in K. Any attempt to implement an "exhaustive" pattern-frequency randomness test up to range K therefore faces an exponential blow-up in the number of test conditions. Even if each individual test can be implemented in (say) $O(L)$ time, a hypothetical complete test family would require time at least $O\big(L\,2^K\big)$, which becomes infeasible as K approaches L.

In practice, real-world test batteries—such as the NIST suite SP 800-22, DIEHARD and TestU01—select a small, finite subset of all possible tests, each of which runs in time polynomial

in L but jointly probe only a vanishingly small fraction of the space of potential deviations from ideal randomness. [17,28] The EITCI reference standard explicitly notes that because the family of conceivable tests is infinite, no finite set of classical tests can *prove* algorithmic or Martin-Löf randomness of a given finite sequence. [3–5] In this sense the underlying problem of "fully testing" randomness has an intrinsically exponential and ultimately unachievable character when approached purely classically via pattern search.

15.7.2 PV-EQRNG output structure and statistical conjugacy

Parity-based PV-EQRNG architectures exploit multipartite entanglement to change the structure of the certification problem. [2,10] In a simplified but representative model, each use of an n-qubit entangled state produces an n-component classical outcome vector $(A_1, \ldots, A_n) \in \{0,1\}^n$ upon measurement in a specified basis. If the source is used for T successive shots under identical control conditions, this yields n classical bit strings

$$S^{(j)} = \left(A_1^{(j)}, \ldots, A_T^{(j)}\right) \in \{0,1\}^T, \qquad j = 1, \ldots, n, \tag{55}$$

where $A_t^{(j)}$ denotes the outcome on subsystem j in shot t.

In a correctly implemented parity-entangled PV-EQRNG, Clause 7, the n-qubit resource state ρ_n and the measurement pattern are designed to satisfy three key properties (up to bounded noise):

1. *Symmetry.* The joint distribution of $(A_1, \ldots, A_n)$ is invariant under permutations of the n subsystems. Formally, if π is any permutation of $\{1, \ldots, n\}$ then

$$P(A_1 = a_1, \ldots, A_n = a_n) \;=\; P(A_{\pi(1)} = a_1, \ldots, A_{\pi(n)} = a_n). \tag{56}$$

2. *Locally unbiased marginals.* Each single-qubit marginal is ideally Bernoulli(1/2):

$$P(A_j = 0) = P(A_j = 1) = \tfrac{1}{2} \quad \text{for all} \quad j. \tag{57}$$

3. *Nonclassical parity correlations.* Certain multi-qubit parity combinations satisfy fixed relations (e.g. XOR constraints), and appropriate combinations of measurement settings give rise to violations of Bell inequalities. The joint statistics of $(A_1, \ldots, A_n)$ therefore cannot be reproduced by any local hidden variable model. [2,10]

Under these conditions, and assuming independence (or at least appropriate mixing) across successive shots t, the n output sequences $S^{(1)}, \ldots, S^{(n)}$ are *statistically conjugate*: in the ideal model they are identically distributed, and any systematic deviation from ideal randomness present in one sequence must be present in all, up to statistical fluctuations.

The PV-EQRNG protocol designates:

- at least one sequence as a *public certification string* P (obtained, for example, by fixing $j = 1$ across all shots),
- at least one sequence as an *auxiliary secret* to be used internally for additional cross-checks, and
- at most $n - 2$ sequences as *secret cryptographic outputs*.

The crucial structural property is that all these sequences arise from the same entangled state and measurement pattern and hence share the same underlying distribution. Classical randomness tests and quantum correlation tests applied to P and to a subset of runs are therefore informative not only about P but about *all* sequences generated by the device under the same control conditions.

15.7.3 Entanglement-enabled collapse of testing overhead: an operational theorem

The entanglement-enabled coupling between public and secret sequences allows one to trade quantum entanglement complexity against classical testing complexity. The following informal theorem makes this trade-off precise at the level of scaling.

Theorem (operational entanglement–testing trade-off). *Consider a PV-EQRNG architecture that, on each of T shots, produces n outcome bits $(A_1, \ldots, A_n)$ by measuring a symmetric n-qubit entangled state according to the protocol, and let $S^{(1)}, \ldots, S^{(n)} \in \{0,1\}^T$ be the corresponding output sequences. Let $\mathcal{T}$ be a fixed finite test battery consisting of*

1. *classical randomness tests applied to a designated public sequence $P := S^{(1)}$ of length T, and*
2. *quantum-correlation tests (parity checks, Bell tests) applied to a subset of shots, using all n outcomes per shot.*

Suppose that for given significance parameters (α, β) the outcome of $\mathcal{T}$ restricts the underlying device model to a family of quantum channels whose single-qubit output distribution on each subsystem is $\varepsilon(T, \alpha, \beta)$-close (e.g. in total-variation distance) to ideal Bernoulli$(1/2)$. Then:

- *this bound ε is independent of n;*
- *any post-processing of the remaining $n-1$ sequences (e.g. concatenation into a length-$N_{\mathrm{sec}} = (n-1)T$ secret string) yields secret outputs whose marginal statistics are ε-close to ideal, up to the same significance parameters (α, β);*
- *the classical computational cost $C(\mathcal{T})$ of running the test battery $\mathcal{T}$ depends only on T and on the structure of the tests, but not on n.*

In particular, for fixed T and fixed test battery, the classical testing cost per certified secret bit scales as

$$\frac{C(\mathcal{T})}{N_{\mathrm{sec}}} = \frac{C(\mathcal{T})}{(n-1)\,T} \xrightarrow[n\to\infty]{} 0. \tag{58}$$

In other words, within the promise class of outputs generated by a correct PV-EQRNG implementation, the total classical effort required to certify a *given quality* of randomness can be made essentially independent of the total number of secret bits produced. The resource that controls the scaling is the degree of multipartite entanglement n, not the total output length.

This scaling manifests sharply in the following thought experiment, which abstracts the intuition expressed in the EITCI reference standard and in parity-based PV-EQRNG proposals. [2–5, 10]

- Fix a block length T (for example $T \approx 10^3$ bits), and imagine that we apply an extremely heavy pattern test to P that is, in principle, exhaustive over all patterns up to range T. The conceptual cost of such a test scales like $O\big(T\,2^T\big)$ because of the 2^T possible patterns of length T.
- Suppose that this test, together with parity/Bell checks, yields a bound ε on the deviation of the device from the ideal PV-EQRNG model on each subsystem.
- Now let the entanglement degree n be extremely large (in principle $n \sim 10^{100}$). The same heavy test, run once on the length-T public string, applies (under the model assumptions) to the roughly $n-1 \sim 10^{100}$ other length-T sequences produced in the same shot ensemble.
- By concatenating these $(n-1)$ sequences we obtain a total secret string of length $(n-1)T$, which can be astronomically large, yet its statistical quality is certified by a *fixed* classical testing effort applied to P.

From the perspective of a purely classical randomness tester faced with the task of exhaustively checking a single binary string of length $N = (n-1)T$ for all patterns up to length N, the computational cost would be on the order of $O\big(N\,2^N\big)$ and therefore hopelessly intractable. The PV-EQRNG architecture, by leveraging multipartite entanglement and the symmetry of the quantum state, allows one to *circumvent* this exponential wall for this special family of sources: one instead performs an exponential-in-T analysis on a fixed-size probe string, then uses entanglement-induced statistical conjugacy to extend the certification to an arbitrarily large ensemble of secret bits.

In this precise operational sense, PV-EQRNG exhibits an "effective collapse" of the exponential blow-up of exhaustive pattern-based randomness testing with the total sequence length, traded for the physical resource of high-degree entanglement.

15.7.4 Quantitative parametrisation in statistical distance and security parameters

For many cryptographic and randomness-standard applications it is useful to instantiate the preceding theorem with explicit distance measures and security parameters, so that the guarantees obtained from PV-EQRNG certification can be plugged directly into composable security analyses. We briefly outline such a parametrisation here.

Let $\mathcal{X}_L = \{0,1\}^L$ denote the space of binary strings of length L, and let U_L be the uniform distribution on $\mathcal{X}_L$. For two probability distributions P, Q on $\mathcal{X}_L$ we write

$$d_{\mathrm{TV}}(P,Q) \;=\; \tfrac{1}{2}\sum_{x\in\mathcal{X}_L}\big|P(x)-Q(x)\big| \tag{59}$$

for their total-variation (statistical) distance. Operationally, $d_{\mathrm{TV}}(P,Q)$ is the maximum distinguishing advantage of any statistical test trying to decide whether a sample was drawn from P or from Q.

In the PV-EQRNG setting, fix a block length T and consider the length-T outputs $S^{(j)} \in \{0,1\}^T$ on each subsystem $j = 1,\dots,n$, as in the previous subsubsection. Let $P^{(j)}_{\mathrm{dev}}$ denote the actual distribution of $S^{(j)}$ produced by the physical device on subsystem j, after all classical post-processing specified by the protocol, and let U_T denote the ideal i.i.d. Bernoulli$(1/2)$ distribution on $\{0,1\}^T$. A natural target guarantee for randomness certification is then

$$d_{\mathrm{TV}}\big(P^{(j)}_{\mathrm{dev}},\mathsf{U}_T\big) \;\le\; \varepsilon_{\mathrm{rand}}, \qquad \text{for all } j\in\{1,\dots,n\}, \tag{60}$$

for some prescribed *randomness deviation parameter* $\varepsilon_{\mathrm{rand}} > 0$. In many cryptographic frameworks a bound of the form (60) for all outputs implies that the device's outputs are $\varepsilon_{\mathrm{rand}}$-indistinguishable from ideal uniform bits in any higher-level protocol that uses them as random coins.

The test battery $\mathcal{T}$ described in the operational theorem implements a hypothesis test on the behaviour of the device. For concreteness, suppose $\mathcal{T}$ produces a binary decision $\mathrm{Acc} \in \{\textsc{accept},\textsc{reject}\}$ based on: (i) classical randomness tests on the public sequence $P = S^{(1)}$ and (ii) quantum-correlation tests on a subset of shots. We can characterise $\mathcal{T}$ by two standard statistical parameters:

- a *completeness error* (significance level) α, such that under the ideal PV-EQRNG model $\Pr[\mathrm{Acc} = \textsc{reject} \mid \text{ideal}] \le \alpha$;
- a *soundness error* $\beta(\varepsilon_{\mathrm{rand}})$, such that for any device whose single-subsystem output distribution deviates from uniform by more than $\varepsilon_{\mathrm{rand}}$ on at least one subsystem,

$$\Pr\big[\mathrm{Acc} = \textsc{accept} \,\big|\, \exists j:\; d_{\mathrm{TV}}\big(P^{(j)}_{\mathrm{dev}},\mathsf{U}_T\big) > \varepsilon_{\mathrm{rand}}\big] \;\le\; \beta(\varepsilon_{\mathrm{rand}}). \tag{61}$$

In words, α bounds the probability that an honest, ideal device is incorrectly rejected, while $\beta(\varepsilon_{\mathrm{rand}})$ bounds the probability that a device whose outputs are "too far" from ideal passes the tests nevertheless.

Conditioned on the event that the test battery *accepts* the public data, a simple Bayesian argument then yields an *a posteriori* guarantee of the form

$$\Pr\Big[\exists j:\ d_{\mathrm{TV}}\big(P_{\mathrm{dev}}^{(j)}, \mathsf{U}_T\big) > \varepsilon_{\mathrm{rand}} \ \Big|\ \mathrm{Acc} = \textsc{accept}\Big] \ \le\ \varepsilon_{\mathrm{sec}}, \tag{62}$$

where $\varepsilon_{\mathrm{sec}}$ is an overall *security parameter* depending on $(\alpha, \beta(\varepsilon_{\mathrm{rand}}))$ in a protocol-specific way (for example, one may take $\varepsilon_{\mathrm{sec}} \le \beta(\varepsilon_{\mathrm{rand}})/(1-\alpha)$ under a worst-case prior). If the standard uses a single global parameter $\varepsilon_{\mathrm{tot}}$ to bound the distinguishing advantage between the real PV-EQRNG outputs and an idealised source, one can set $\varepsilon_{\mathrm{tot}}$ to dominate both $\varepsilon_{\mathrm{rand}}$ and $\varepsilon_{\mathrm{sec}}$:

$$\varepsilon_{\mathrm{tot}} \ \ge\ \varepsilon_{\mathrm{rand}} + \varepsilon_{\mathrm{sec}}, \tag{63}$$

so that any distinguisher's advantage against the full PV-EQRNG realisation is bounded by $\varepsilon_{\mathrm{tot}}$.

Within this parametrisation, the entanglement–testing trade-off theorem can be read as a statement about the scaling of *sample complexity*: to achieve a given triple of parameters $(\varepsilon_{\mathrm{rand}}, \varepsilon_{\mathrm{sec}}, \alpha)$, one needs a minimum number $T = T(\varepsilon_{\mathrm{rand}}, \varepsilon_{\mathrm{sec}}, \alpha)$ of observed shots, determined by standard concentration bounds and the design of $\mathcal{T}$, but this T is independent of n. Once T is fixed, the classical computational cost $C(\mathcal{T})$ of evaluating $\mathcal{T}$ scales with T and the complexity of individual tests, but not with the number of subsystems. At the same time, the number of certified secret bits scales as $N_{\mathrm{sec}} = (n-1)\,T$, so that the security parameter $\varepsilon_{\mathrm{tot}}$ remains fixed while the certified output length can, in principle, grow without bound.

If one prefers to work in an entropy-based parametrisation, the total-variation bound (60) can be translated into a lower bound on the (min-)entropy of each secret block. For example, if $d_{\mathrm{TV}}\big(P_{\mathrm{dev}}^{(j)}, \mathsf{U}_T\big) \le \varepsilon_{\mathrm{rand}}$ then the (conditional) min-entropy satisfies a bound of the form

$$H_\infty\big(S^{(j)}\big) \ \ge\ T - \Delta(\varepsilon_{\mathrm{rand}}), \tag{64}$$

for an explicitly computable penalty term $\Delta(\varepsilon_{\mathrm{rand}})$ depending on the chosen convention for smooth min-entropy. This provides a direct bridge between PV-EQRNG certification and entropy-based security definitions in quantum cryptography.

In all cases, the key qualitative feature persists: for fixed target values of the statistical distance and security parameters, the required certification length T and the classical cost $C(\mathcal{T})$ are independent of the entanglement degree n, while the number of certified secret bits grows linearly in n. Multipartite entanglement thus appears explicitly as a physical resource that can be spent to reduce the classical statistical complexity per certified bit, without weakening the quantitative security guarantees expressed in the standard's own parameters.

15.7.5 Complexity-theoretic framing: a physical-model-dependent collapse

The above phenomenon should not be misunderstood as a literal complexity-class collapse such as EXP = P. In classical complexity theory such equalities are defined in terms of worst-case running time of Turing machines over *arbitrary* inputs. By contrast, the PV-EQRNG scaling effect is:

- restricted to the promise class of outputs generated by a device that implements the specified parity-entangled quantum state and measurement pattern, and
- inherently *physical-model-dependent*: it uses the laws of quantum mechanics, and the symmetry and nonlocality of the entangled state, as an oracle supplying strong structural information about the distribution of outputs.

Formally, one can view the PV-EQRNG certification problem as a property-testing problem over a restricted family of stochastic processes: the property is "the device is within distance ε of the ideal PV-EQRNG model", and the tester is the finite battery $\mathcal{T}$ applied to the public string and to a subset of runs. [52] The key point is that the *sample complexity* of this property test—the total number of shots T that must be observed—depends on the desired accuracy and confidence parameters $(\varepsilon, \alpha, \beta)$, but not on the eventual number of secret bits extracted. Entanglement ensures that once the property holds for the device as a whole, it automatically applies to all subsystems, and hence to all secret outputs.

Thus, within this physically specified model, the family of randomness certification tasks indexed by the total secret output length N_{sec} exhibits the following scaling behaviour:

$$\text{Classical certification cost} \;=\; C(\mathcal{T}) = C\big(T(\varepsilon, \alpha, \beta)\big), \tag{65}$$

which is independent of N_{sec}. If one were to insist, in a purely classical setting with no entanglement structure, on separately running a complete pattern test on each length-T block that makes up a length-N_{sec} string, the cost would grow linearly (or worse) in N_{sec} and, under an "exhaustive patterns" definition, exponentially in T.

The PV-EQRNG architecture therefore realises a *physical-model-dependent collapse of the classical testing overhead per secret bit*: by increasing the entanglement degree n one can, in principle, certify arbitrarily large total outputs with a fixed, finite amount of classical testing, without changing the statistical strength of the certification. This is a qualitative, complexity-theoretic effect, but it is explicitly conditioned on the correctness of the underlying physical model of the generator.

15.7.6 Entanglement as a computational resource

The above trade-off between multipartite entanglement and classical testing complexity is conceptually aligned with the broader insight that entanglement is a key resource underlying quantum computational speed-ups. [20, 21] Jozsa and Linden showed that if an n-qubit quantum computation, on pure states, generates only bounded-size entanglement blocks (independent of n), then the computation can be efficiently simulated classically. [20] Vidal demonstrated that quantum circuits whose entanglement entropy remains logarithmically bounded can likewise be simulated with polynomial classical resources via tensor-network methods. [21] These results indicate that sufficiently large-scale entanglement is *necessary* for genuine exponential quantum advantages, although not sufficient by itself.

Shor's factoring and discrete-logarithm algorithm provides a canonical example. [22] The central quantum subroutine is the Quantum Fourier Transform (QFT) on an n-qubit register, which maps computational basis states to highly delocalised superpositions, creating strong entanglement between the control register and the register on which modular exponentiation is performed. The QFT and the preceding oracle call jointly encode an *exponential amount* of classical information about the periodic structure of the function $x \mapsto a^x \bmod N$ into the amplitudes of a polynomial-size quantum state. A small number of measurements, followed by efficient classical post-processing, suffice to extract the hidden period and thus factor N in polynomial time. In this sense, the QFT uses multipartite entanglement to compress an otherwise exponential classical search over function values into a physically accessible global interference pattern. [34]

The PV-EQRNG scaling phenomenon is structurally analogous:

- In Shor's algorithm, entanglement and interference allow one to access a global property of a function (its period) with classical resources that scale only polynomially in the input size, despite the fact that naively computing the function on all inputs would be exponential.

- In PV-EQRNG, multipartite entanglement allows one to access a global property of a randomness source (its closeness to an ideal entangled quantum model) with classical testing resources that are essentially independent of the total number of bits produced, despite the fact that exhaustive pattern-based testing of a single very long output would be exponentially hard.

In both cases the "exponential work" that would confront a classical procedure is effectively offloaded into the structure of a highly entangled quantum state: the combinatorial explosion of possibilities is represented in parallel by the amplitudes and correlations of the state, and measurement of a small number of subsystems, together with carefully designed post-processing, suffices to recover the relevant global property.

The PV-EQRNG protocol therefore provides a concrete, operational instance of a more general heuristic: *the degree of multipartite entanglement, n, functions as a computational resource that can be traded against classical complexity in specific tasks.* Here the task is not solving a traditional decision or search problem, but certifying the quality of randomness in a setting where exhaustive classical testing would be exponentially hard.

15.7.7 Limitations and scope

Two limitations of this entanglement-enabled scaling must be emphasised.

First, the intrinsic incompleteness of classical randomness testing remains: no finite test battery can certify algorithmic randomness of a specific finite sequence, and the exponential growth in the space of possible patterns is not eliminated. [3–5] What changes is that PV-EQRNG shifts the focus from testing individual long strings to testing the underlying *quantum process* that generates many statistically conjugate strings. Once the process has been constrained by tests on a representative public sequence and by Bell/parity tests, the same guarantees extend to arbitrarily many secret outputs.

Second, the length T of the public certification string cannot be reduced arbitrarily without weakening the statistical guarantees. Standard concentration bounds imply that, to bound the bias of a binary source within $\pm\varepsilon$ at significance level α, a minimum number of observed bits $T = T(\varepsilon, \alpha)$ is required; this sample-complexity lower bound is independent of n. Likewise, estimating higher-order correlations to a given precision requires a minimum number of shots. PV-EQRNG does not change these basic statistical facts; it allows the collected evidence to be *reused* across many entangled subsystems.

Finally, practical implementations are constrained by experimental considerations. Preparation, control and measurement of large multipartite entangled states are technologically challenging, and noise, loss and decoherence typically increase with system size. Beyond a platform-dependent scale, increasing the entanglement degree n may degrade Bell violations, increase error rates and reduce the net security/throughput trade-off. These practical limitations do not alter the conceptual scaling argument, but they bound the range of n for which the entanglement–testing trade-off can be effectively exploited in real devices.

Within these limits, the qualitative conclusion is robust: PV-EQRNG architectures use multipartite entanglement not only to certify that randomness is of provably quantum origin (via Bell nonlocality), but also to reduce, in an operational sense, the classical testing complexity required to certify large random outputs. Entanglement degree n acts as a physical resource that can be spent to collapse the dependence of classical testing cost on total output length for this physically specified family of randomness sources.

15.8 Closing remarks

Entanglement-based QRNGs with public randomness verification, as pioneered in [1, 2, 10] and recently implemented in photonic platforms [11, 12], provide a fundamentally new capability:

the ability to generate secret random strings whose quality can be certified in a transparent and publicly auditable manner, without compromising secrecy.

This standard has introduced and analysed a parity-based, protocol-verified entangled quantum random number generator (PV-EQRNG) architecture in which multipartite entanglement is used not only to guarantee the quantum origin of randomness, but also to change the structure of the classical certification problem. In the theoretical reference standard for entangled QRNG it is emphasised that classical randomness testing can be understood as a pattern-search problem: each test probes the frequency or correlation of a particular binary pattern, and the family of potential tests is infinite, with the number of patterns of length k growing as 2^k. [3–5] An exhaustive pattern-frequency analysis of a single long sequence would therefore entail resources that grow exponentially with the pattern size or correlation range; in practice, only a finite and necessarily incomplete battery (e.g. NIST SP 800-22) is ever applied. [17]

In Clause 15.7 we showed that, for the restricted but physically well-motivated family of sources realisable by PV-EQRNG, multipartite entanglement enables a qualitatively different scaling. Each use of an n-qubit entangled state yields n classical bit sequences $S^{(1)}, \ldots, S^{(n)}$ whose single-qubit marginals are (ideally) identical and unbiased, and whose multi-qubit correlations satisfy strict parity/XOR constraints and Bell-type relations. [2, 10] Under the protocol, at least one sequence is published as a certification string P, while up to $n-2$ sequences are kept secret as cryptographic outputs. In the ideal model all sequences $S^{(j)}$ are statistically conjugate: they are generated by the same symmetric entangled state and measurement pattern and hence share the same distribution. Any systematic departure from ideal randomness in the secret outputs must also manifest in P, up to statistical fluctuations.

This symmetry allows entanglement to be traded against classical testing effort. A fixed-length public string P of length T, together with a finite battery $\mathcal{T}$ of classical randomness tests and quantum-correlation checks, constrains the underlying generator to be $\varepsilon(T, \alpha)$-close to an ideal model on *every* subsystem, for a chosen significance level α. Crucially, this constraint is independent of how many other sequences $S^{(j)}$ are kept secret or how they are post-processed. In an idealised limit where arbitrarily large n-qubit entangled states can be prepared and measured with bounded error, the same finite testing effort applied to a single representative sequence P suffices to certify the randomness quality of an arbitrarily large total number of secret bits, obtained by concatenating the remaining $n-1$ sequences. If the public certification length T and test family $\mathcal{T}$ are held fixed while n grows, the effective classical testing cost per certified secret bit scales as

$$\frac{\mathrm{cost}(\mathcal{T}, T)}{(n-2)\,T} \longrightarrow 0 \quad \text{as } n \to \infty,$$

even though an exhaustive pattern search on a generic sequence of the same total length would be infeasible due to the exponential proliferation of patterns. In this operational sense, PV-EQRNG realises a physically promise-dependent reduction of the exponential testing burden: for this particular entangled source family, the classical work needed to confront exponential pattern complexity is bounded by a constant that depends on the *block length* T but not on the total output length.

This should not be interpreted as an unconditional collapse of classical complexity classes in the Turing-machine sense. The abstract problem of deciding whether an arbitrary finite bit string is "truly random" remains mathematically ill-posed in algorithmic randomness theory, and the exponential growth of potential statistical tests with pattern size is not eliminated. [3–5] What PV-EQRNG changes is the *structure* of the certification problem: instead of exhaustively testing each long output string in isolation, one tests a single representative string together with a small set of entanglement-induced constraints. The exponential richness of possible patterns is offloaded, in a precise way, into the entangled quantum hardware and probed indirectly through a bounded amount of classical and quantum statistical evidence. The total amount of evidence required to bound deviations from ideal behaviour at a given significance level is still governed

by standard statistics and sets a minimum scale for the certification length T, but this scale is independent of n, while the number of certified secret bits grows linearly in n.

From a broader viewpoint this provides an explicit and conceptually simple instance of the general principle, articulated by Jozsa and Linden, that sufficiently large-scale entanglement is a necessary physical resource for genuine quantum computational speed-up. [20] In Shor's algorithm for factoring and discrete logarithms, highly non-local entangled states created by the quantum Fourier transform encode an exponential number of classical possibilities in parallel, allowing a global property (the period of a function) to be extracted with only polynomial classical post-processing. [22] In PV-EQRNG, multipartite entanglement plays an analogous role for statistical certification: a large ensemble of classically intractable pattern relations among many output strings is enforced "in hardware" by the entangled source, so that testing a single string and a small set of correlators carries implications for an arbitrarily large secret output. In this sense PV-EQRNG can be viewed as a constructive, operational realisation of the Jozsa–Linden view of entanglement as the key resource enabling qualitative reductions in classical complexity, here instantiated not in a conventional decision problem but in the certification of non-deterministic binary sequences.

This perspective also meshes naturally with the device-independent approach to randomness certification, in which Bell inequality violations are used to bound the entropy of outcomes independently of detailed device modelling. [24, 53] Parity-based PV-EQRNG can be extended towards such device-independent or semi-device-independent regimes by strengthening the Bell-type tests applied to the public data and by making the security analysis more adversarial. The key qualitative feature remains: entanglement couples many outputs so that a bounded set of public statistical tests constrains an unbounded amount of secret randomness.

The analysis presented here suggests several directions for further research. On the theoretical side, one may formalise the PV-EQRNG scaling as a family of *entanglement-assisted statistical complexity* results: within clearly specified physical promise classes, quantify how the multipartite entanglement degree n trades off against the classical effort needed to certify a target entropy rate or deviation bound. This would connect the present work to resource theories of entanglement and to the burgeoning literature on classical simulation of low-entanglement quantum processes. A complementary path is to explore impossibility results: for example, to show that if the source is restricted to product states or to entanglement confined to $O(1)$-sized blocks, then no protocol can achieve a similar asymptotic decoupling between certification effort and total output length, thus making the role of high-degree entanglement in statistical complexity reduction mathematically sharp.

On the more applied side, PV-EQRNG architectures provide a concrete platform in which these ideas can be tested and refined experimentally. Scaling up the entanglement degree n while controlling noise and decoherence, integrating stronger Bell-type tests, and combining PV-EQRNG with established device-independent randomness expansion techniques are natural next steps. Beyond cryptographic randomness generation, the same conjugation mechanism that relates many outputs via a common entangled source could, in principle, be adapted to other statistical inference tasks in which exhaustive pattern testing is classically prohibitive. In all such developments, the guiding theme is that multipartite entanglement can serve as a quantitative resource for reducing classical statistical complexity: PV-EQRNG offers a minimal, operationally transparent example of this principle in the domain of randomness testing.

This Technical Reference Standard consolidates definitions, theoretical foundations, protocol families, security models and use cases for such entanglement-based QRNGs. It is intended as a foundation for subsequent profile-specific standards, certification schemes and implementation guides. Stakeholders deploying or developing EQRNG technology **SHALL** regard this document as a living reference, to be updated as theory and practice of quantum randomness continue to evolve.

References

[1] Janusz E. Jacak, Witold A. Jacak, Wojciech A. Donderowicz, and Lucjan Jacak. Entanglement quantum random number generator with public randomness certification. World Intellectual Property Organization Patent WO2019132679, PCT/PL2017/000133, 2017, pub. 2019. URL: https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2019132679.

[2] Janusz E. Jacak, Witold A. Jacak, Wojciech A. Donderowicz, and Lucjan Jacak. Quantum random number generators with entanglement for public randomness testing. *Scientific Reports*, 10:164, 2020. doi:10.1038/s41598-019-56706-2.

[3] EITCI Institute Quantum Standards Group. Reference standard for the entangled quantum random number generator with the public randomness certification – theoretical concepts (definitions, true randomness, use cases). Technical Report RS-EITCI-QSG-EQRNG-THEORY-STD-VER-1.0, EITCI Institute, 2019. URL: https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-theoretical-concepts.

[4] EITCI Institute Quantum Standards Group. Reference standard for the entangled quantum random number generator with the public randomness certification – protocols, processes, devices and operative principles. Technical Report RS-EITCI-QSG-EQRNG-PROTOCOLS-STD-VER-1.0, EITCI Institute, 2019. URL: https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-protocols.

[5] EITCI Institute Quantum Standards Group. Reference standard for the entangled quantum random number generator with the public randomness certification – testing and verification schemes including sustaining secrecy. Technical Report RS-EITCI-QSG-EQRNG-TESTING-STD-VER-1.0, EITCI Institute, 2019. URL: https://eitci.org/technology-certification/qsg/eqrng/eitci-qsg-eqrng-testing.

[6] Monika M. Jacak, Piotr Jóźwiak, Jakub Niemczuk, and Janusz E. Jacak. Quantum generators of random numbers. *Scientific Reports*, 11:16108, 2021. doi:10.1038/s41598-021-95388-7.

[7] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang. Quantum random number generation. *npj Quantum Information*, 2:16021, 2016. doi:10.1038/npjqi.2016.21.

[8] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartín. Quantum random number generators. *Reviews of Modern Physics*, 89:015004, 2017. doi:10.1103/RevModPhys.89.015004.

[9] Vaisakh Mannalatha, Sandeep Mishra, and Anirban Pathak. A comprehensive review of quantum random number generators: concepts, classification and the origin of randomness. *Quantum Information Processing*, 22:439, 2023. doi:10.1007/s11128-023-04175-y.

[10] Piotr Jóźwiak, Janusz E. Jacak, and Witold A. Jacak. New concepts and construction of quantum random number generators. *Quantum Information Processing*, 23:132, 2024. doi:10.1007/s11128-024-04335-8.

[11] Tanvirul Islam, Anindya Banerji, Chin Jia Boon, Rui Wang, Ayesha Reezwana, James A. Grieve, Rodrigo Piera, and Alexander Ling. A privacy-preserving publicly verifiable quantum random number generator. *Scientific Reports*, 14:12437, 2024. doi:10.1038/s41598-024-61552-y.

[12] Nidhin Kolangatt et al. Publicly verifiable quantum random-number generator with a four-qubit photonic system. *Physical Review A*, 110:032615, 2024. doi:10.1103/PhysRevA.110.032615.

[13] Sonia Mazzucchi, Nicolò Leone, Stefano Azzini, Lorenzo Pavesi, and Valter Moretti. Entropy certification of a realistic quantum random-number generator based on single-particle entanglement. *Physical Review A*, 104:022416, 2021. doi:10.1103/PhysRevA.104.022416.

[14] Nicolò Leone, Stefano Azzini, Sonia Mazzucchi, Valter Moretti, and Lorenzo Pavesi. Certified quantum random-number generator based on single-photon entanglement. *Physical Review Applied*, 17:034011, 2022. doi:10.1103/PhysRevApplied.17.034011.

[15] International Organization for Standardization. Information technology – security techniques – random bit generation. International Standard ISO/IEC 18031, ISO/IEC, 2011. and subsequent amendments. URL: https://www.iso.org/standard/81645.html.

[16] Meltem Sönmez Turan et al. Recommendation for the entropy sources used for random bit generation. Special Publication 800-90B, National Institute of Standards and Technology, 2018. URL: https://csrc.nist.gov/publications/detail/sp/800-90b/final.

[17] Andrew Rukhin et al. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Special Publication 800-22 Revision 1a, National Institute of Standards and Technology, 2010. URL: https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final.

[18] European Telecommunications Standards Institute. Quantum key distribution (qkd); protocol and data format of rest-based key delivery api. ETSI GS QKD 014, ETSI, 2019. URL: https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_QKD014v010101p.pdf.

[19] ITU-T Study Group 17. Quantum noise random number generator architecture. ITU–T Recommendation X.1702, International Telecommunication Union, 2019. URL: https://www.itu.int/rec/T-REC-X.1702.

[20] Richard Jozsa and Noah Linden. On the role of entanglement in quantum-computational speed-up. *Proceedings of the Royal Society A*, 459(2036):2011–2032, 2003. doi:10.1098/rspa.2002.1097.

[21] Guifré Vidal. Efficient classical simulation of slightly entangled quantum computations. *Physical Review Letters*, 91(14):147902, 2003. doi:10.1103/PhysRevLett.91.147902.

[22] 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. doi:10.1137/S0097539795293172.

[23] Yu-Huai Li, Xuan Han, Yuan Cao, Xiao Yuan, Zheng-Ping Li, Jian-Yu Guan, Juan Yin, Qiang Zhang, Xiongfeng Ma, Cheng-Zhi Peng, and Jian-Wei Pan. Quantum random number generation with uncharacterized laser and sunlight. *npj Quantum Information*, 5:97, 2019. doi:10.1038/s41534-019-0208-1.

[24] Stefano Pironio, Antonio Acín, Serge Massar, Antoine Boyer de La Giroday, D. N. Matsukevich, Peter Maunz, Steven Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, 2010. doi:10.1038/nature09008.

[25] Yang Liu et al. Device-independent quantum random-number generation. *Nature*, 562:548–551, 2018. doi:10.1038/s41586-018-0559-3.

[26] Lynden K. Shalm et al. Device-independent randomness expansion with entangled photons. *Nature Physics*, 17:452–456, 2021. doi:10.1038/s41567-020-01153-4.

[27] Pramod Kavuri et al. Traceable random numbers from a non-local quantum advantage. *Nature*, 642:916–921, 2025. doi:10.1038/s41586-025-09054-3.

[28] Pierre L'Ecuyer and Richard Simard. Testu01: A C library for empirical testing of random number generators. *ACM Transactions on Mathematical Software*, 33(4):22, 2007. doi:10.1145/1268776.1268777.

[29] Yong Zhang et al. A simple low-latency real-time certifiable quantum random number generator. *Nature Communications*, 12:1056, 2021. doi:10.1038/s41467-021-21069-8.

[30] Marco Avesani, Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. *Nature Communications*, 9:5365, 2018. doi:10.1038/s41467-018-07585-0.

[31] International Organization for Standardization. Information technology – security techniques – test and analysis methods for random bit generators within iso/iec 19790 and iso/iec 15408. International Standard ISO/IEC 20543, ISO/IEC, 2019. URL: https://www.iso.org/standard/68296.html.

[32] Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi. Source-device-independent quantum random number generation. *Physical Review Letters*, 118:060503, 2017. doi:10.1103/PhysRevLett.118.060503.

[33] Telecommunication Engineering Centre. Quantum random number generator (qrng) – generic requirements. Technical Report GR/QS-91020, Telecommunication Engineering Centre, India, 2024. URL: https://www.tec.gov.in/pdf/GRs/Standard_GR_QRNG_TEC_91020_2024_Final%20(1).pdf.

[34] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 10th anniversary edition edition, 2010. doi:10.1017/CBO9780511976667.

[35] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81:865–942, 2009. doi:10.1103/RevModPhys.81.865.

[36] Marco Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Springer, Cham, 2016. doi:10.1007/978-3-319-21891-5.

[37] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540:213–219, 2016. doi:10.1038/nature20119.

[38] P. K. Aravind. Borromean entanglement of the GHZ state. In M. Ferrero and A. van der Merwe, editors, *New Developments on Fundamental Problems in Quantum Physics*, pages 53–59. Springer, Dordrecht, 1997. doi:10.1007/978-94-017-2732-7_4.

[39] Louis H. Kauffman and Samuel J. Lomonaco. Quantum entanglement and topological entanglement. *New Journal of Physics*, 4:73, 2002. doi:10.1088/1367-2630/4/1/373.

[40] Alexei Kitaev and John Preskill. Topological entanglement entropy. *Physical Review Letters*, 96:110404, 2006. doi:10.1103/PhysRevLett.96.110404.

[41] Michael Levin and Xiao-Gang Wen. Detecting topological order in a ground state wave function. *Physical Review Letters*, 96:110405, 2006. doi:10.1103/PhysRevLett.96.110405.

[42] Tanvirul Islam, Anindya Banerji, Chin Jia Boon, Wang Rui, Ayesha Reezwana, James A. Grieve, Rodrigo Piera, and Alexander Ling. A privacy-preserving publicly verifiable quantum random number generator. *Sci. Rep.*, 14:11337, 2024. doi:10.1038/s41598-024-61552-y.

[43] Mayalakshmi Kolangatt, Anirudh Verma, Sujai Matta, Kanad Sengupta, and C. M. Chandrashekar. Four-qubit photonic system for publicly verifiable quantum random numbers and generation of public and private key. *Phys. Rev. A*, 110:032615, 2024. doi:10.1103/PhysRevA.110.032615.

[44] W. Wootters and W. Żurek. A single quantum cannot be cloned. *Nature*, 299:802, 1982.

[45] D. Bouwmeester, J. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger. Observation of three-photon greenberger-horne-zeilinger entanglement. *Phys. Rev. Lett.*, 82:1345, 1999. doi:10.1103/PhysRevLett.82.1345.

[46] J. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger. Experimental test of quantum nonlocality in three-photon greenberger-horne-zeilinger entanglement. *Nature*, 403:515, 2000. doi:10.1038/35000514.

[47] Charles H. Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988. doi:10.1137/0217014.

[48] Ronen Shaltiel. An introduction to randomness extractors. In Luca Aceto et al., editors, *Automata, Languages and Programming*, volume 6756 of *Lecture Notes in Computer Science*, pages 21–41. Springer, Berlin, Heidelberg, 2011. URL: https://link.springer.com/chapter/10.1007/978-3-642-22012-8_2.

[49] Xiongfeng Ma, Feihu Xu, He Xu, Xiongfeng Tan, Bing Qi, and Hoi-Kwong Lo. Post-processing for quantum random-number generators: entropy evaluation and randomness extraction. *Physical Review A*, 87:062327, 2013. doi:10.1103/PhysRevA.87.062327.

[50] National Institute of Standards and Technology. Security requirements for cryptographic modules. Federal Information Processing Standards Publication FIPS 140-3, NIST, 2019. URL: https://csrc.nist.gov/publications/detail/fips/140/3/final, doi:10.6028/NIST.FIPS.140-3.

[51] International Organization for Standardization. Information technology – security techniques – security requirements for cryptographic modules. International Standard ISO/IEC 19790, ISO/IEC, 2012-2025. URL: https://www.iso.org/standard/82423.html.

[52] Oded Goldreich. *Introduction to Property Testing*. Cambridge University Press, Cambridge, 2017. doi:10.1017/9781108135252.

[53] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. *Journal of the ACM (JACM)*, 68(31):1–47, 2021. doi:10.1145/3441309.