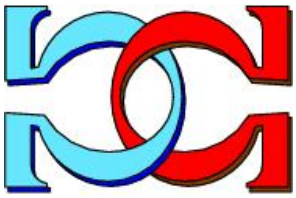

CDMTCS
Research
Report
Series

Photonic Ternary Quantum Random Number Generators

J. M. Agüero and C. S. Calude

School of Computer Science, University of Auckland, New Zealand

CDMTCS-563
June 2022

Centre for Discrete Mathematics and
Theoretical Computer Science

Photonic Ternary Quantum Random Number Generators

José Manuel Agüero Trejo and Cristian S. Calude
School of Computer Science
University of Auckland, New Zealand

Abstract

We construct a class of 3-dimensional photonic quantum random number generators and prove that each generates maximally unpredictable digits via measurements that are robust to errors. In particular, every sequence generated is strongly incomputable; hence its quality is provable better than that of every pseudo-random sequence. We also briefly contrast 2-dimensional and 3-dimensional quantum random number generators, discuss photonic implementations and show the superiority of the latter ones. These results suggest that incomputability in physics is real and practically useful.

1 Introduction

Quantum random number generators (QRNGs) have increased in the last decade because higher quality of randomness is required in many areas, from cryptography, statistics, and information science to medicine, physics, politics and religion, and the many pitfalls of pseudo-random number generators (PRNGs) are sometimes catastrophic [49]. QRNGs are generally considered to be "better than PRNGs" because they are based on the "fundamental unpredictability of well-chosen and controlled quantum processes" [39], a statement which requires more scientific arguments than a simple assertion, particularly because the notion of "true randomness" is mathematically vacuous [18].

The first photonic QRNG called *Quantis* was produced by ID Quantique in 2001, and it is based on the standard beamsplitter experiment, see Figures 1 and 2 in [40]. For an experimental analysis of the quality of *Quantis* see [19, 1, 38, 52].

Linear optical quantum computing (LOQC) [43] is a photonic paradigm of quan-

tum computing which can simulate small quantum systems. Rather than tensor together the Hilbert spaces for multiple particles, LOQC uses the Hilbert spaces associated to the spatial modes, or paths of a single photon. For example, the state of a 3-dimensional quantum particle (e.g. spin-1 particle) can be represented by a photon that can be on one of three paths and design a one-qutrit gate with a collection of beamsplitters and mirrors with three input ports and three output ports. Attenuated lasers [30] and photon multiplier tubes [27] are affordable, reliable single-photon sources and detectors.

In this paper, we present a uniform method to construct a class photonic 3D QRNGs and a method to derive the optimal preparation of quantum value indefinite states (that satisfy the Located Kochen-Specker Theorem [3]) whose measurements produce outcomes with a pre-given probability distribution.

The new method generalises the constructions of 3D QRNGs described in [44, 10], where two natural probability distributions have been considered. The new method uses a *fixed universal* unitary operator – obtained as a composition of 2-dimensional unitary operators – and an optimal value indefinite state which is repeatedly measured; the outcomes obtained by the measurements have a pre-given probability distribution. In this way, the Located Kochen-Specker Theorem [6] applies and guarantees that every sequence of quantum random ternary digits obtained in this manner is maximally unpredictable and robust to errors. In particular, every quantum random sequence generated is strongly incomputable (bi-immune [28]), that is, no algorithm can compute more than finitely many exact values of the sequence; this property, which is much stronger than incomputability, implies that the quality of the *photonic* 3D QRNG *is provably better than that of any pseudo-random generator*.

Some QRNGs, like those based on a classical beamsplitter, have no certification and rely instead on statistical analysis of experimental outcomes. Other QRNGs, like [9], are certified by Bell Theorem [14] or a located variant of Kochen-Specker Theorem [3]. The strength of a certification depends on its assumptions. The certification of the QRNGs discussed in this article is unique because i) the assumptions used have been experimentally validated, ii) the robustness of measurements was proved theoretically [5, 8], and iii) the quality of very long strings of quantum random digits generated with the QRNGs was experimentally shown to be better than that of the best PRNGs using pragmatic randomness tests [4]. No other QRNG, among the many reviewed in the recent survey of the state-of-the-art of QRNGs [41], is certified in this way.

Finally, the Kochen-Specker Theorem is valid only for Hilbert spaces of dimension at least 3, the certification given in this paper does not work for the 2D beamsplitter used by *Quantis* [39].

The paper is organised as follows. Section 2 is devoted to notation and definitions; Section 3 presents the classical and located Kochen-Specker Theorems; in Section 4 we construct a universal photonic unitary operator and in Section 5 we construct the value indefinite observable; Section 6 presents the formal certification of the 3D QRNG and Section 7 we contrast photonic 2D and 3D implementations. Section 8 includes conclusions and three open questions.

2 Notation and definitions

The sets of positive integers, reals and complex are denoted by $\mathbb{N}$, $\mathbb{R}$, and $\mathbb{C}$, respectively. Consider the alphabets $A_2 = \{0, 1\}, A_3 = \{0, 1, 2\}$. Strings over the alphabet A_3 are denoted by x, y, u, w. Infinite sequences over the alphabet A_3 are denoted by $\mathbf{x} = x_1 x_2 \ldots$; the prefix of length m of $\mathbf{x}$ is the string $\mathbf{x}(m) = x_1 x_2 \ldots x_m$. Sequences can be also viewed as A_3-valued functions defined on $\mathbb{N}$.

A sequence $\mathbf{x}$ over the alphabet A_3 is called 3-bi-immune if there is no partial computable function $\varphi : \mathbb{N} \to A_3$ such that its domain $\mathrm{dom}(\varphi)$ is infinite and $\varphi(i) = x_i$ for every $i \in \mathrm{dom}(\varphi)$, [20].

We assume knowledge of elementary computability theory and algorithmic information theory over different size alphabets [18] and quantum optics [33].

Finally, we use 2D and 3D for “two" and “three" dimensionalities, respectively.

3 Kochen-Specker Theorems

In contrast with Bell Theorem [14, 15] which gives only bounds on probability distributions under the assumption of locality, Kochen-Specker Theorem shows that assuming non-contextuality[1], it is impossible to assign “classical” definite values to all possible quantum observables in a consistent manner. A definite value is precisely a (deterministic) hidden variable specifying, in advance, the result of the measurement of an observable. Consequently, if the conditions for the Kochen-Specker Theorem are satisfied, the outcomes of all quantum measurements on a system cannot be simultaneously predetermined.

In what follows we denote the observable projecting onto the linear subspace spanned by a vector $|\psi\rangle$ as $P_\psi = \frac{|\psi\rangle\langle\psi|}{|\langle\psi|\psi\rangle|}$. We then fix a positive integer $n > 2$

[1]Informally, by “context" we understand the details that surround an event. A quantum measurement of an observable is non-contextual if its outcome is independent of the “context", i.e. is independent on how the observable is measured.

and let $O \subseteq \{P_\psi \mid |\psi\rangle \in \mathbb{C}^n\}$ be a nonempty set of one-dimensional projection observables on the Hilbert space $\mathbb{C}^n$.

Definition 1 *A set $C \subset O$ is a* context *of O if C has n elements and for all $P_\psi, P_\phi \in C$ with $P_\psi \neq P_\phi$, $\langle\psi|\phi\rangle = O$.*

Definition 2 *A* value assignment function *(on O) is a partial function $v : O \to \{0, 1\}$ assigning values to some (possibly all) observables in O.*[2]

Definition 3 *An observable $P \in O$ is* value definite *(under the assignment function v) if $v(P)$ is defined; otherwise, it is* value indefinite *(under v). Similarly, we call O* value definite *(under v) if every observable $P \in O$ is value definite.*

We assume the following hypotheses:

- **Admissibility:** Let O be a set of one-dimensional projection observables on $\mathbb{C}^n$ and let $v : O \to \{0, 1\}$ be a value assignment function. Then v is *admissible*[3] for O if for every context C of O, we have that $\sum_{P \in C} v(P) = 1$, i.e. only one projection observable in a context can be assigned the value 1.
- **Non-contextuality of definite values**: The outcome obtained by measuring a value definite observable (a pre-existing physical property) is *non-contextual*, i.e. it does not depend on other compatible observables which may be measured alongside it.

Theorem 1 (Kochen-Specker [42, 16, 17, 51]) *Let $n \geq 3$. Then there exists a (finite) set of one-dimensional projection observables O on the Hilbert space $\mathbb{C}^n$ such that there is no value assignment function v satisfying the following three conditions: i) every element in O is value definite under v, ii) v is admissible for O, iii) v is non-contextual.*

It has been shown that for every set of observables, there exists an admissible assignment function under which the set of observables is value definite, and at least one observable is non-contextual [7]. Hence the incompatibility between the Kochen-Specker assumptions is not maximal: not all observables need to be value indefinite. However, the set of value indefinite has constructive Lebesgue measure one, that is, with probability one, every observable is value indefinite [5].

Value indefinite observables are essential because, as we will show, *measuring one such observable produces a "random" outcome*. To measure a value indefinite observable, we have to "effectively find" one, so the existential Kochen-Specker Theorem is not enough.[4] Motivated by Einstein, Podolsky and Rosen's definition

[2]The partiality of the function v means that $v(P)$ can be $0, 1$ or indefinite.

[3]That is, in agreement with quantum mechanics predictions.

[4]Even in case the finite set has two elements.

of *physical reality* [29, p. 777]:

> If without in any way, disturbing a system, we can predict with certainty the value of a physical quantity, then there exists a *definite value* before observation corresponding to this physical quantity.

we adopt the following [8]:

- **Eigenstate principle**: If a quantum system is prepared in the state $|\psi\rangle$, then the projection observable P_ψ is value definite.

In detail, if a quantum system is prepared in an arbitrary state $|\psi\rangle \in \mathbb{C}^n$, then the measurement of the observable P_ψ should yield the outcome 1, hence, if $P_\psi \in O$, then $v(P_\psi) = 1$.

The main result used here is:

Theorem 2 (Located Kochen-Specker [3, 5, 8]) *Consider a quantum system described by state $|\psi\rangle$ in a Hilbert space $\mathbf{C}^n$, $n \geq 3$. Choose a state $|\phi\rangle$ that is neither orthogonal nor parallel to $|\psi\rangle$ ($0 < |\langle\psi|\phi\rangle| < 1$). If the following three conditions are satisfied: i) admissibility, ii) non-contextuality and iii) eigenstate principle, then the projection observable P_ϕ is value indefinite.*

According to Theorem 2, if a quantum system is prepared in state $|\psi\rangle$, a one-dimensional projection observable can only be value definite if it is an eigenstate of that observable. More generally,

Corollary 1 *Let O be an observable with spectral decomposition $O = \sum_{i=1}^{n} \lambda_i P_{\lambda_i}$, where λ_i denotes each distinct eigenvalue with corresponding eigenstate $|\lambda_i\rangle$. Then, O has a predetermined measurement outcome if and only if each projector in its spectral decomposition has a predetermined measurement outcome.*

Thus, Theorem 2 works also for the outcome of the measurement of an observable with non-degenerate spectra. Furthermore, let $C = \{P_1, \ldots, P_n\}$ be a context, i.e. a maximal set of compatible projection observables and let v be a value assignment function such that $v(P_1) = 1$ under C. It then follows that, if any pair (P_1, P_i) is measured, then the system will collapse into the eigenstate $|\phi\rangle$ of the projection observable P_1 with eigenvalue 1. As all observables in C are physically co-measurable and $\sum_{j=1}^{n} P_j = 1$, we deduce that $|\phi\rangle$ is an eigenstate of P_i with corresponding eigenvalue 0, hence $v(P_i) = 0$. Similarly, if $v(P_i) = 0$ for all $i \neq 1$, then $v(P_1) = 1$. Hence, the property of admissibility of v serves as a generalisation of the sum rule that corresponds to the physical interpretation of the measurement process.

4 A universal photonic unitary operator

In this section, we present a setup satisfying the conditions of Theorem 2 that guarantees the value indefiniteness of the observables, does not rely on probabilistic results, and *ensures maximal unpredictability and robustness to errors* (as in the case of multiple photon emission).

To fulfil the Hilbert space dimensional requirement, we can use a collection of theoretical beamsplitters representing the state of a spin-1[5] particle [3] as described by its corresponding unitary decomposition, where the desired probability distribution can be achieved with a careful state preparation.

4.1 A generalised spin-1 observable

The property denoted by *spin* (**S**) is the intrinsic form of angular momentum characteristic of elementary particles. By deriving the spin state operator S_x we can analyse the effect of the preparation state $|S_z\rangle$ on the outcome probabilities. We consider the description of states that point in arbitrary directions specified by the unit vector $\mathbf{u} = (u_x, u_y, u_z) = (\sin\theta\cos\vartheta, \sin\theta\sin\vartheta, \cos\theta)$, where θ, ϑ are the polar and azimuthal angles; we then define the spin observable operator **S** as a triplet of operators $\mathbf{S} = (S_x, S_y, S_z) = \hbar\boldsymbol{\sigma}$, where $\boldsymbol{\sigma}$ corresponds to the generalised Pauli matrices for a spin-1 particle. Then, by adopting units in which $\hbar$ is numerically equal to unity, we obtain the generalised observable that describes the measurement context:

$$S(\theta,\vartheta) = \mathbf{u}\cdot\mathbf{S} = \begin{pmatrix} \cos(\theta) & \frac{e^{-i\vartheta}\sin(\theta)}{\sqrt{2}} & 0 \\ \frac{e^{i\vartheta}\sin(\theta)}{\sqrt{2}} & 0 & \frac{e^{-i\vartheta}\sin(\theta)}{\sqrt{2}} \\ 0 & \frac{e^{i\vartheta}\sin(\theta)}{\sqrt{2}} & -\cos(\theta) \end{pmatrix}. \tag{1}$$

Note that S_z is given by $S(0,0)$ and S_x by $S(\frac{\pi}{2},0)$.

4.2 Unitary decomposition

By considering the orthonormal Cartesian standard basis $|1\rangle = (1,0,0), |0\rangle = (0,1,0)$ and $|-1\rangle = (0,0,1)$, and the eigenvalues $\{-1,0,1\}$ of S_x we obtain the unitary matrix U_x corresponding to the spin state operator S_x:

[5] Many results in this section hold for an arbitrary 3-dimensional particle.

$$U_x = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}. \tag{2}$$

There is a well-known relationship between the set of 2×2 unitary matrices with determinant one, $SU(2)$, and the physical observables of quantum spin in a 2-dimensional Hilbert space. Every matrix $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ in $SU(2)$ satisfies $A^\dagger = A^{-1}$ by definition, thus, we can express the linear transformation of a vector by the matrix A as follows:

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}. \tag{3}$$

This relation plays an essential role in the formulation of a transformation produced by a lossless beamsplitter and external phase shifter to represent the annihilation operators of the quantum harmonic oscillator [33]. Here, the transmittance and reflectivity parameters are described within the unitary matrix, and the input and output states are represented with modes (u, v) and (u', v') respectively:

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} \cos\theta & ie^{i\vartheta}\sin\theta \\ i\sin\theta & e^{i\vartheta}\cos\theta \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}.$$

As demonstrated in [54], given an arbitrary unitary operator, we can represent a generalised rotation through the decomposition of the unitary matrix U_x using a series of phase shifters and beamsplitters implemented in an optical experiment. To this end, θ describes the square root of the reflectivity and transmittance given by $\sin\theta$ and $\cos\theta$ respectively, and ϑ represents the phase of an external phase shifter on the second input port.

As unitary decompositions are not unique, the unavoidable imperfections in every experimental setup mean that not every choice is suitable for physical implementation. Consequently, a unitary decomposition must be carefully constructed to reduce internal loss, minimise the physical footprint, and make the implemented transformation as close as possible to the ideal one.

Imperfect parameter settings describing the optical elements of a photonic quantum circuit and propagation losses due to manufacturing errors are the main factors impeding an ideal physical realisation. In what follows, we use the method [22] because the analysis in [32] concluded that it achieves a more balanced mixing of

the optical modes, a reduced propagation loss and a better scaling of fidelity than the method [54].[6]

This arrangement can be achieved by left and right multiplying theoretical beamsplitter matrices $B_{m,n}$ and $B_{m,n}^{-1}$ to nullify successive diagonals of U_x while ensuring that no null element of U_x is affected by subsequent operations.

Let

$$B_{1,2} = \begin{pmatrix} \sqrt{\frac{2}{3}} & \frac{1}{\sqrt{3}} & 0 \\ \frac{i}{\sqrt{3}} & -i\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; B_{2,3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{i\sqrt{3}}{2} \\ 0 & \frac{i\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix},$$

$$B_{1,2}^{-1} = \begin{pmatrix} \sqrt{\frac{2}{3}} & -\frac{i}{\sqrt{3}} & 0 \\ \frac{1}{\sqrt{3}} & i\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \; D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

and note that $B_{2,3}^{-1} = B_{2,3}$.

We then obtain the following decomposition:

$$B_{2,3} \cdot B_{1,2} \cdot U_x \cdot B_{1,2}^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} = D. \tag{4}$$

Thus, from (4) we get

$$U_x = B_{1,2}^{-1} \cdot B_{2,3}^{-1} \cdot D \cdot B_{1,2} = B_{1,2}^{-1} \cdot B_{2,3} \cdot D \cdot B_{1,2}. \tag{5}$$

In particular, with D consisting of single mode phase-shifts, there exists a diagonal matrix D' and a beamsplitter matrix $B'_{1,2}$ such that $B_{1,2}^{-1} \cdot D = D' \cdot B'_{1,2}$. Indeed, setting

$$D' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -1 \end{pmatrix}, \; B'_{1,2} \begin{pmatrix} \sqrt{\frac{2}{3}} & \frac{i}{\sqrt{3}} & 0 \\ -\frac{i}{\sqrt{3}} & -\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

[6]The improvements are due to a more compact and symmetric interferometric structure.

hence we have

$$B_{1,2}^{-1}\cdot D=\begin{pmatrix}\sqrt{\frac{2}{3}} & -\frac{i}{\sqrt{3}} & 0\\ \frac{1}{\sqrt{3}} & i\sqrt{\frac{2}{3}} & 0\\ 0 & 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{pmatrix}=\begin{pmatrix}\sqrt{\frac{2}{3}} & \frac{i}{\sqrt{3}} & 0\\ \frac{1}{\sqrt{3}} & -i\sqrt{\frac{2}{3}} & 0\\ 0 & 0 & -1\end{pmatrix}$$

$$=\begin{pmatrix}1 & 0 & 0\\ 0 & i & 0\\ 0 & 0 & -1\end{pmatrix}\cdot\begin{pmatrix}\sqrt{\frac{2}{3}} & \frac{i}{\sqrt{3}} & 0\\ -\frac{i}{\sqrt{3}} & -\sqrt{\frac{2}{3}} & 0\\ 0 & 0 & 1\end{pmatrix}=D'\cdot B'_{1,2}.$$

Observing that $B_{2,3}\cdot D=D\cdot B_{2,3}$ we get:

$$U_x=B_{1,2}^{-1}\cdot B_{2,3}\cdot D\cdot B_{1,2}=D'\cdot B'_{1,2}\cdot B_{2,3}\cdot B_{1,2},$$

which allows us to set the reflectivity, transmittance and phase shift values for a physical realization via Mach-Zehnder interferometers:

$B_{m,n}$	θ	ϑ
$B'_{1,2}$	$-\frac{\eta}{2}$	π
$B_{2,3}$	$\frac{2\pi}{3}$	π
$B_{1,2}$	$\frac{\eta}{2}$	$\frac{3\pi}{2}$

with $\eta=2\arccos\left(\sqrt{\frac{2}{3}}\right)$. This yields the correspondence between the equation (4) and its physically realisable optical implementation in Fig. 1.

4.3 Invariance of value-indefinite observables

To justify the use of the *2-dimensional* matrices representing beamsplitters to construct the *3-dimensional* unitary operator, we have to prove that the 2-dimensional decomposition induces a mapping that preserves the *3-dimensionality*, hence value indefiniteness. In other words, we have to prove that the constructed system is genuinely in the Hilbert space $\mathbb{C}^3$. That is, Kochen-Specker Theorem applies; it is known this theorem is false in dimension two.

Recall that the group $O(3)$ formed by the orthogonal transformations in a 3-dimensional vector space establishes significant results closely related to the conservation of angular momentum; in particular, the representation theory of the rotation group $SO(3)$ is strongly associated with the theory of the spin of elementary

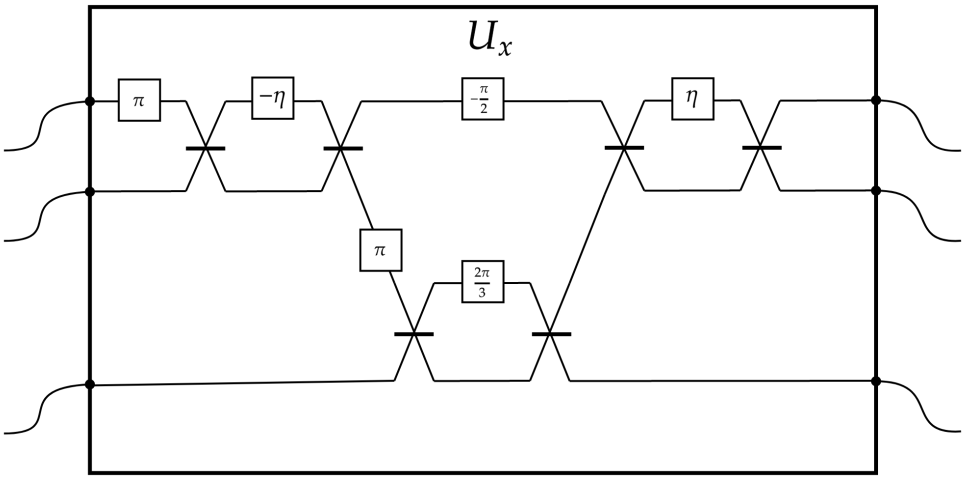

Figure 1: Physical realization of the universal unitary decomposition U_x by means of 3-mode multiport interferometer. An arrangement of Mach-Zehnder interferometers consisting of phase shifters and balanced directional couplers illustrate its construction. Here, $\eta = \arccos\left(\sqrt{\frac{2}{3}}\right)$.

particles [48] allowing the derivation of the generalised spin-1 observable. Furthermore, there is an essential relationship between the groups $SU(2)$ and $SO(3)$, which is established by a bijective and continuous group homomorphism Φ – the Lie group homomorphism – mapping $SU(2)$ onto $SO(3)$ with a corresponding continuous inverse map Φ^{-1}, see [35].

Consider the vector space V spanned by the orthonormal basis

$$\{\sigma_1, \sigma_2, \sigma_3\} \equiv \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

formed with the *Pauli matrices* $\sigma_x, \sigma_y, \sigma_z$. Note that

$$\sigma_i \sigma_j = \delta_{ij} I + \sum_k \epsilon_{ijk} \sigma_k,$$

where

$$\epsilon_{ijk} = \begin{cases} 1, & \text{if } ijk \text{ is an even permutation,} \\ -1, & \text{if } ijk \text{ is an odd permutation,} \\ 0, & \text{otherwise,} \end{cases}$$

with the inner product defined by $\langle A, B\rangle = \frac{1}{2}\operatorname{Tr}(AB)$, for A, B in the basis. The orthonormality of the chosen basis for V yields the correspondence with $\mathbb{C}^3$. If $U \in SU(2)$ and $A \in V$, then

$$UAU^{-1} = (U^{-1})^* AU^* = (UAU^{-1})$$

and

$$\operatorname{Tr}\big(UAU^{-1}\big) = \operatorname{Tr}\big(U^{-1}UA\big) = \operatorname{Tr}(A) = 0,$$

thus $UAU^{-1} \in V$. Furthermore,

$$U_1U_2AU_2^{-1}U_1^{-1} = (U_1U_2)A(U_1U_2)^{-1}$$

and

$$\operatorname{Tr}\big(UAU^{-1}UBU^{-1}\big) = \frac{1}{2}\operatorname{Tr}(AB) = \langle A, B\rangle,$$

where $A, B \in V$ and $U, U_1, U_2 \in SU(2)$. The linear map $\Phi_U : V \to V$ defined by $\Phi_U(A) = UAU^{-1}$ satisfies the following conditions:

$$\Phi_{U_1U_2} = \Phi_{U_1}\Phi_{U_2}; \langle \Phi_U(A), \Phi_U(B)\rangle = \langle A, B\rangle.$$

In particular, Φ_U is an orthogonal transformation of V. Hence Φ is a homomorphism from $SU(2)$ to $O(3)$. Finally, note that Φ_I equals the identity I. In particular, since $SO(3)$ restricts the elements of $O(3)$ to the ones with determinant one, it follows that Φ maps $SU(2)$ into $SO(3)$.[7]

Thus, the action of the 2-dimensional decomposition of U_x on a spin-1 observable is a Lie group preserving mapping to the measurement of a spin-1 system along the x axis as described by U_x (see Section 4 4.1).

Furthermore, as U_x preserves the measurement context described by the spin state operator $S_x = S(\frac{\pi}{2}, 0)$, if the projection observable P_ϕ is value indefinite, then the projection observable $P_{U_x(\phi)}$ is also value indefinite. We have proved:

Theorem 3 *The operator U_x defined by (5) preserves 3-dimensionality, hence value indefiniteness.*

5 Construction of a value indefinite quantum state

In this section we construct a value indefinite quantum state which by measurement produces outcomes with a given probability distribution (p_1, p_2, p_3) where

[7] An alternative derivation can be obtained by noting that $SU(2)$ is isomorphic to unit quaternions.

$\sum_i p_i = 1$ and $0 < p_i < 1$. Consider the standard Cartesian basis and the spin state operator S_x from Section 4 4.2.

The desired probability distribution is

$$\begin{aligned} \mathcal{P}(S_x, 1) &= |\langle 1_x|\phi^*\rangle|^2 = p_1, \\ \mathcal{P}(S_x, 0) &= |\langle 0_x|\phi^*\rangle|^2 = p_2, \\ \mathcal{P}(S_x, -1) &= |\langle -1_x|\phi^*\rangle|^2 = p_3, \end{aligned} \tag{6}$$

were $|1_x\rangle, |0_x\rangle$ and $|-1_x\rangle$ represent the eigenvectors of S_x with respect to the standard Cartesian basis and $|\phi\rangle$ is the preparation state. A preparation state is *valid* if the conditions in (6) are satisfied.

Thus, for a selection of valid preparation states $|\phi^*\rangle$ we use Corollary 1 to obtain:

$$\begin{aligned} \mathcal{P}(S_x, 1) &= \left|\frac{1}{2}\langle 1|\phi^*\rangle + \frac{1}{\sqrt{2}}\langle 0|\phi^*\rangle + \frac{1}{2}\langle -1|\phi^*\rangle\right|^2 = p_1, \\ \mathcal{P}(S_x, 0) &= \left|\frac{1}{\sqrt{2}}\langle 1|\phi^*\rangle - \frac{1}{\sqrt{2}}\langle -1|\phi^*\rangle\right|^2 = p_2, \\ \mathcal{P}(S_x, -1) &= \left|\frac{1}{2}\langle 1|\phi^*\rangle - \frac{1}{\sqrt{2}}\langle 0|\phi^*\rangle + \frac{1}{2}\langle -1|\phi^*\rangle\right|^2 = p_3. \end{aligned} \tag{7}$$

Then, if we choose

$$x = \pm\sqrt{2}\sqrt{p_2} + z = \langle 1|\phi^*\rangle, y = \pm\sqrt{p_2} \mp \sqrt{2}\sqrt{p_3} + z\sqrt{2} = \langle 0|\phi^*\rangle,$$

$$z = \pm\frac{\sqrt{p_1}}{2} \mp \frac{\sqrt{p_2}}{\sqrt{2}} \pm \frac{\sqrt{p_3}}{2} = \langle -1|\phi^*\rangle,$$

we obtain

$$\mathcal{P}(S_x, 1) = |\langle 1_x|\phi^*\rangle|^2 = p_1, \mathcal{P}(S_x, 2) = |\langle 0_x|\phi^*\rangle|^2 = p_2,$$

$$\mathcal{P}(S_x, -1) = |\langle -1_x|\phi^*\rangle|^2 = p_3.$$

We have proved:

Theorem 4 *The following quantum states are value indefinite with respect to the standard Cartesian basis:*

$$
\begin{aligned}
|\phi\rangle^* = &\left[\pm\sqrt{2}\sqrt{p_2} + z\right]|1\rangle \\
&+ \left[\pm\sqrt{p_2} \mp \sqrt{2}\sqrt{p_3} + z\sqrt{2}\right]|0\rangle + \left[\pm\frac{\sqrt{p_1}}{2} \mp \frac{\sqrt{p_2}}{\sqrt{2}} \pm \frac{\sqrt{p_3}}{2}\right]|-1\rangle\,.
\end{aligned} \tag{8}
$$

for every combination of the signs + *and* −.

According to Theorem 4, given a probability distribution (p_1, p_2, p_3), every quantum states in (8) is a valid preparation state for the 3D QRNG and this is obtained by choosing a combination of signs for $|\phi^*\rangle$.

Example 1 For the probability distribution $(\frac{1}{4}, \frac{1}{2}, \frac{1}{4})$, by setting

$$
(+\sqrt{p1}, +\sqrt{p2}, +\sqrt{p3}) = \left(\frac{1}{2}, \frac{1}{\sqrt{2}}, \frac{1}{2}\right),
$$

we can obtain the valid preparation state

$$
|\phi\rangle = [1+z]\,|1\rangle + \left[\frac{1}{\sqrt{2}} - \frac{\sqrt{2}}{2} + z\sqrt{2}\right]|0\rangle + \left[\frac{1}{4} - \frac{1}{2} + \frac{1}{4}\right]|-1\rangle = |1\rangle\,.
$$

Similarly, for the probability distribution $(\frac{1}{3}, \frac{1}{3}, \frac{1}{3})$, we get the following valid preparation states

$$
\begin{gathered}
\pm\frac{1}{\sqrt{3}}\left(|1\rangle + |-1\rangle\right) \pm \frac{1}{\sqrt{6}}\left(|1\rangle - |-1\rangle\right), \frac{1}{\sqrt{6}}|1\rangle \pm \sqrt{\frac{2}{3}}|0\rangle - \frac{1}{\sqrt{6}}|-1\rangle, \\
-\frac{1}{\sqrt{6}}|1\rangle \pm \sqrt{\frac{2}{3}}|0\rangle + \frac{1}{\sqrt{6}}|-1\rangle\,.
\end{gathered}
$$

6 Certification

First, we discuss the formal property of the proposed 3D QRNGs, which guarantees that *the quality of their quantum random bits is provable better than the one produced by* any *pseudo-random number generator*. Mathematically, the property guarantees that *every sequence produced by such* 3D QRNG *is incomputable*, that is, *no sequence produced by such a* 3D QRNG *can be reproduced exactly by any algorithm*. In detail, consider a process that algorithmically repeats the process of state preparation and measurement, as described in Sections 4 and 5 4.2, and let $\mathbf{x} = x_1 x_2 \ldots$ be the infinite sequence produced by the measurement outputs;

here each x_i is 0 or 1 or 2. Let $\mathcal{O}, \mathcal{C}$ be two fixed sets of observables and contexts, whose respective components O_i, C_i denote the observable and the corresponding context of the i-th measurement. Let $f : \mathbb{N} \times \mathcal{O} \times \mathcal{C} \to A_3$ be the function defined by $f(i, O_i, C_i) = x_i$ for every i. The incomputability of **x**, which is equivalent to the incomputability of f, follows from the non-contextuality of definite values.

A stronger result can be obtained by using the non-probabilistic model for unpredictability [6, 7]. To this end, we consider an *experiment* E producing a single-digit $x \in A_3$. With a particular trial of E, we associate the parameter λ (the state of the universe), which fully describes the trial; λ is a resource from which one can extract finite information to predict the outcome of the experiment E. The trials of E generate a succession of events of the form "E is prepared, performed, the result recorded, E is reset", algorithmically iterated finitely many times.

Definition 4 *An* extractor *is a physical device selecting a finite amount of information from λ without altering the experiment E; the outcome is a string of digits $\langle\lambda\rangle$ over A_3.*

Definition 5 *A* predictor *for E is an algorithm P_E which* halts *on every input and* produces *and element of A_3 or* prediction withheld.

The predictor, P_E, can use the information $\langle\lambda\rangle$ as input but must be *passive,* that is, it must not disturb or interact with E in any way.

Definition 6 *A predictor P_E provides a* correct prediction *using the extractor $\langle\,\rangle$ for an instantiation of E with parameter λ on the input $\langle\lambda\rangle$, in case it outputs an element of A_3 (that is, it does not refrain from making a prediction) that is equal to x, the result of the experiment.*

Definition 7 *Fix an extractor $\langle\,\rangle$ and a positive integer k. The predictor P_E is* $k, \langle\,\rangle$-correct *if there exists an $n \geq k$ such that when E is repeated n times with associated parameters $\lambda_1, \ldots, \lambda_n$ and produces the outputs $x_1, x_2, \ldots, x_n$, then P_E outputs the sequence $P_E(\langle\lambda_1\rangle), P_E(\langle\lambda_2\rangle), \ldots, P_E(\langle\lambda_n\rangle)$ with the following two properties: (i) no prediction in the sequence is incorrect, and (ii) in the sequence there are k correct predictions.*

If P_E is $k, \langle\,\rangle$-correct the probability that P_E is in fact operating by chance and may not continue to give correct prediction is bounded by $3^{-n}\binom{n}{k} < \frac{2^n}{3^n} \leq \left(\frac{2}{3}\right)^k$. This probability tends exponentially to 0 when $k \to \infty$, so the confidence we have in a $k, \langle\,\rangle$-correct predictor increases exponentially with k.

If P_E is $k, \langle\,\rangle$-correct for all k, then P_E never makes an incorrect prediction, and the number of correct predictions can be made arbitrarily large by repeating E enough times. If P_E is not $k, \langle\,\rangle$-correct for all k, then we cannot exclude the

possibility that every correct prediction P_E makes is simply due to chance. Consequently, we can define the predictability of a single trial:

Definition 8 *The outcome x of a single trial of the experiment E performed with parameter λ is* predictable *(with certainty) if there exist an extractor $\langle\,\rangle$ and a predictor P_E which is $k, \langle\,\rangle$-correct for all k, and $P_E(\langle\lambda\rangle) = x$.*

In this case, if the predictor P_E outputs x, then P_E never makes an incorrect prediction no matter how many times it is used, practically finitely many, theoretically infinitely many.

Theorem 5 *A sequence $\mathbf{x} \in A_3^\omega$ is* 3-bi-immune *if and only if no single digit of $\mathbf{x}$ can be predicted by any predictor.*

Proof. Let $\mathbf{x} \in A_3^\omega$ be a 3-bi-immune sequence and assume that a digit x_i of $\mathbf{x}$ can be predicted. Fix an extractor $\langle\,\rangle, \lambda$, and assume that there exists a predictor P_E for $\mathbf{x}$ which is $k, \langle\,\rangle$-correct for all $k \in \mathbb{N}$ and $P_E(\langle\,\lambda_i\rangle) = x_i$. Define the partial function $\varphi : \mathbb{N} \to A_3$ with the domain $\mathrm{dom}(\varphi) = \{j \in A_3 \mid P_E(\langle\,\lambda_j\rangle)$ is not withheld$\}$ and $\varphi(j) = P_E(\langle\,\lambda_j\rangle), j \in \mathbb{N}$.

By definition, P_E is an algorithm which halts on every input and for infinitely many $j \in \mathbb{N}, \varphi(j) = x_j$, hence the set $\{j \in \mathbb{N} \mid \varphi(j) = x_j\}$ is computable, contradicting the 3-bi-immunity of $\mathbf{x}$. Accordingly, $j \notin \mathrm{dom}(\varphi)$ if and only if $P_E(\langle\,\lambda_j\rangle)$ is withheld.

For the other implication suppose no single digit of $\mathbf{x}$ can be predicted and assume for the sake of contradiction that $\mathbf{x}$ is not 3-bi-immune. Hence there exists a partial computable function $\varphi : \mathbb{N} \to A_3$ with infinite domain and $\varphi(i) = x_i$ for every $i \in \mathrm{dom}(\varphi)$. Algorithmically we can extract an infinite computable subset S of $\mathrm{dom}(\varphi)$ and set $\lambda_j = j$ for the experiment which consists in the computation of $\varphi(j), j \in S$. Thus, we can construct the predictor P_E which is k-correct for all $k \in \mathbb{N}$ by the formula:

$$P_E\langle\lambda_j\rangle) = P_E(j) = \begin{cases} \varphi(j), & \text{if } j \in S, \\ \text{“}\textit{prediction withheld}\text{”}, & \text{otherwise.} \end{cases}$$

This is a contradiction as all x_j with $j \in S$ are correctly predicted by P_E. □

Assuming the **Eigenstate principles**, and the

> **epr principle**: If a repetition of measurements of an observable generates a computable sequence, then this implies these observables were value definite.

the following results follow from Theorem 3 in [7]:

Theorem 6 *Let* $\mathbf{x}$ *be an infinite sequence obtained by measuring a quantum value indefinite observable in* $\mathbb{C}^3$ *in an algorithmic infinite repetition of the experiment* E*. Then no single-digit* x_i *can be predicted.*

From Theorem 5 we get:

Corollary 2 *Let* $\mathbf{x}$ *be an infinite sequence obtained by measuring a quantum value indefinite observable in* $\mathbb{C}^3$ *in an algorithmic infinite repetition of the experiment* E*, then* $\mathbf{x}$ *is* 3*-bi-immune.*

Given Theorem 4, every quantum state in (8) is value indefinite and measuring it with the universal unitary operator U_x produces a quantum random ternary digit.

Corollary 3 *Every* 3D QRNG *that uses a value indefinite observable (8) and the universal unitary operator (5) always generates sequences for which no single digit can be predicted. In particular, every such sequence is* 3*-bi-immune.*

7 Photonic implementations

In this section we discuss 2D and 3D photonic implementations of QRNGs.

7.1 Spin and dimensionality of photons

Although photons are a spin-1 particle, they are considered massless. Thus, the description of the projector of the spin operator onto the momentum operator is referred to as *helicity*. Hence, one of the spin states would be symmetric to a rotation about an axis that is normal to the direction of travel for the photon, indicating zero momentum. One can think of this as acting in the rest frame where the velocity is zero, and since a photon travels at the speed of light, this state is usually dismissed.

Nonetheless, the mathematical peculiarities of photons indicate that there is valuable 3-dimensional information encoded in the traditionally dismissed state. A 2-dimensional view of the photonic structure does not fulfil the dimensional requirements imposed by Theorem 1, but, a 3-dimensional analysis allows the use of this result to localise value indefiniteness within a photonic quantum process. To illustrate the relevance of the underlying 3-dimensional structure of photons, consider the case of virtual photons, which can be described as "light that passes between two particles of matter without explicit measurement of its properties". In the case of virtual photons, the helicity state zero has to be considered since we can no longer think of them as massless. Rather than regarding photons as being *real* or *virtual*, one can argue that all photons are virtual photons or that they occur

in a continuum of those terms; this continuum can be observed as virtual attributes exhibited by real photons, which are evident in the case of nanophotonics [12], or in a vacuum where "virtual photons can be transformed into real ones that can be observed experimentally". The structure and behaviour of virtual and real photons are complex phenomena that are not yet fully understood. Its peculiarities in its dimensionality, as described mathematically and observed experimentally, make it necessary to preserve this dimensionality in a quantum system that utilises photons to guarantee value indefiniteness.

7.2 A 2D vs. 3D QRNG

Recent literature uses Bell-type inequalities to assert the unpredictability of quantum measurements and formulate random number generation protocols. These protocols rely on correlations that violate the constraints described by Bell's Theorem to *certify* that there is no *local* hidden variable describing the measurement outcomes. Thus, extracting statistical randomness from the local measurement of entangled states.

Other physical implementations use a 2-dimensional beamsplitter, relying on the assumption that a photon going through a beamsplitter will act as a “quantum bit flip" (or “quantum coin" [57]).

Several variants of Bell's Theorem, Bell-type inequalities and protocols based on these results have been used throughout the years. A notable example is the GHZ approach, referred to as *Bell's Theorem Without Inequalities* [34], because it avoids statistical averaging and inequalities, and the *CHSH inequality* [21], which includes Bell's inequality as a particular case.

Despite their popularity to certify the quality of quantum random bits generated by 2D QRNGs, see [53, 55], the choice of probability space, among other parameters used to derive Bell-type inequalities, may lead to ambiguity when analysing the probabilities of finding correlations among the measurement outcomes which, in some experimental circumstances, may lead to relaxation or formulation of additional assumptions when taking into account experimental imperfections [56, 46, 26, 37]. Due to its probabilistic framework and in some cases, its inability to meet the criteria for value indefiniteness as a consequence of its dimensionality [58], this type of certification does not guarantee the *maximal unpredictability* of its measurement outcomes.

In contrast, localising value indefiniteness enables a photonic 3D QRNG to *certify* the *maximal unpredictability* of its outcomes in a non-probabilistic fashion (as detailed in Section 6). Thus, this type of QRNG offers a provable security advantage over any PRNG used as an entropy source for cryptographic systems.

7.3 Single-photon sources and detectors

The effects of the inherent imperfections in the physical implementation of a QRNG have to be carefully studied since the choice of theoretical certification has a fundamental impact on the error sensitivity of the experimental implementation. To illustrate this point, we consider the case of single-photon sources and detectors.

In an ideal case, a stream of single photons emitted at controlled intervals will traverse the beamsplitter setup, and an ideal single-photon detector will detect its final trajectory. However, every experimental realisation of such a device faces various limitations that depend on the specific implementation.

There are several flavours of single-photon sources available to date. The difficulties involved in the experimental realisation of a single-photon source lead to attenuated lasers as an alternative. Weak laser light can produce a proxy for single-photon states via a coherent state approximation and a low enough intensity. In particular, an attenuated light (e.g. generated by a light-emitting diode) offers a sufficient, inexpensive and straightforward alternative when accounting for a photon generation with a more significant separation than the coherence time of the source; here, separation does not represent a problem as the limiting factor tends to be the dead time of the detector (the time interval after a detection when the detector is unable to perceive incoming photons) [50, 36].

In this case, the number of photos emitted fluctuates around a particular mean value following the Poisson distribution: multiple photons could be emitted at once, or one could get an empty pulse. If the mean number of photons per pulse is reduced to ensure the probability of emitting more than one photon at once is negligible, so most pulses will be empty, which implies a decrease in bit rate and a disruption of the system performance (as the detectors must be active for every pulse [11, 31]). Thus, a delicate balance is required for practical applications.

For QRNGs reliant on Bell-type certification, multiple photon emission is a severe problem. Successively emitted photon pairs may overlap within the detection time window, simultaneously triggering a detection event that contributes to an artificial rate of photon count coincidences, hence the possibility of falsely satisfying Bell's inequality; the higher the frequency of multiple photon emission, the greater the chances of this occurring [13].

This is not a problem for the implementation presented in this paper, which is based on uncorrelated states. Moreover, Theorem 2 provides robustness against non-ideal preparation state fidelity (via the condition $0 < |\langle\psi|\phi\rangle| < 1$). The certification method discussed in Section 6 guarantees the *maximal unpredictability*

and *strong incomputability*, properties distinguishing the QRNGs discussed in the paper from all others [**?**, 41]. As the quality of the generated random digits remains unaffected, the outcomes corresponding to photon count coincidences can be discarded to reduce bias or included to increase the number of extractable bits. In the latter case, an un-biasing technique would be required as a post-processing step. This solution is prone to the adverse effects of normalisation techniques on other symptoms of randomness, not yet fully understood [2]

8 Conclusion

We have described a class of 3D QRNGs based on a universal photonic unitary operator and proven that it generates maximally unpredictable digits via measurements that are robust to errors. In particular, every sequence generated is strongly incomputable; hence its quality is provable better than that of every pseudo-random sequence.

Next, we briefly contrasted 2D and 3D QRNGs, discussed photonic implementations and showed the superiority of the latter ones. The strong incomputability of every sequence generated by the 3D QRNGs studied in this paper contributes to the much-studied and debated problem of incomputability in physics [24, 47, 23, 25]. This paper argues that incomputability in physics is real and practically applicable, a fundamental phenomenon for understanding nature.

As many applications require binary random strings, the following computable alphabetic morphism $\varphi\colon A_3 \to A_2$

$$\varphi(a) = \begin{cases} 0, & \text{if } a = 0, \\ 1, & \text{if } a = 1, \\ 0, & \text{if } a = 2, \end{cases}$$

transforms by sequential concatenation ternary strings/sequences into binary ones and preserves the certification discussed in Section 6 for the probability distribution 1/4,1/2,1/4; for proofs see Section 7 in [10].

Are the main assumptions, Admissibility, Non-contextuality, Eigenstate and epr principles, used in the proof of Theorem 2, physically "acceptable"? A cautiously affirmative answer to this question comes from the results obtained by testing the incomputability of quantum random strings of length 2^{32} (obtained with the implementation of the 3D QRNG [44]) using Chaitin-Schwartz Theorem in [4]. We conjecture that better results will be obtained with a similar implementation of the 3D QRNG in [10].

Finally, we conjecture that i) the certification of the 3D QRNGs presented in this paper can be strengthened to Martin-Löf randomness [18, 45], and ii) in contrast to 3D beamsplitters, 2D beamsplitters "lose" information, hence they do not generate maximally unpredictable random sequences.

Acknowledgment

We thank ... for discussions and comments, which improved the paper.

References

[1] A. A. Abbott, L. Bienvenu, and G. Senno. Non-uniformity in the quantis random number generator. Report CDMTCS-472, Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, Auckland, New Zealand, Nov. 2014.

[2] A. A. Abbott and C. S. Calude. Von neumann normalisation of a quantum random number generator. *Computability*, 1(1):59–83, 2012.

[3] A. A. Abbott, C. S. Calude, J. Conder, and K. Svozil. Strong Kochen-Specker theorem and incomputability of quantum randomness. *Physical Review A*, 86(062109), Dec 2012.

[4] A. A. Abbott, C. S. Calude, M. J. Dinneen, and N. Huang. Experimentally probing the algorithmic randomness and incomputability of quantum randomness. *Physica Scripta*, 94(4):045103, Feb 2019.

[5] A. A. Abbott, C. S. Calude, and K. Svozil. Value indefiniteness is almost everywhere. *Physical Review A*, 89(3):032109–032116, 2014.

[6] A. A. Abbott, C. S. Calude, and K. Svozil. A non-probabilistic model of relativised predictability in physics. *Information*, 6(4):773–789, 2015.

[7] A. A. Abbott, C. S. Calude, and K. Svozil. On the unpredictability of individual quantum measurement outcomes. In L. D. Beklemishev, A. Blass, N. Dershowitz, B. Finkbeiner, and W. Schulte, editors, *Fields of Logic and Computation II*, volume 9300 of *Lecture Notes in Computer Science*, pages 69–86. Springer, 2015.

[8] A. A. Abbott, C. S. Calude, and K. Svozil. A variant of the Kochen-Specker theorem localising value indefiniteness. *Journal of Mathematical Physics*, 56, 102201, `http://dx.doi.org/10.1063/1.4931658`, Oct 2015.

[9] A. Acín and L. Masanes. Certified randomness in quantum physics. *Nature*, 540(7632):213–219, 12 2016.

[10] J. M. Agüero Trejo and C. S. Calude. A new quantum random number generator certified by value indefiniteness. *Theoretical Computer Science*, 862:3–13, Mar. 2021.

[11] S. Al-Kathiri, W. Al-Khateeb, M. Hafizulfika, M. R. Wahiddin, and S. Saharudin. Characterization of mean photon number for key distribution system using faint laser. In *2008 International Conference on Computer and Communication Engineering*, pages 1237–1242, Kuala Lumpur, Malaysia, May 2008. IEEE.

[12] D. L. Andrews and D. S. Bradshaw. The role of virtual photons in nanoscale photonics: The role of virtual photons in nanoscale photonics. *Annalen der Physik*, 526(3-4):173–186, Apr. 2014.

[13] A. V. Belinskii and D. N. Klyshko. Interference of light and Bell's Theorem. *Physics-Uspekhi*, 36:653–693, 1993.

[14] J. S. Bell. On the problem of hidden variables in quantum mechanics. *Reviews of Modern Physics*, 38:447–452, 1966.

[15] J. S. Bell. *Speakable and Unspeakable in Quantum Mechanics*. Cambridge University Press, Cambridge, 1987.

[16] A. Cabello. A simple proof of the Kochen-Specker Theorem. *European Journal of Physics*, 15(179–183), 1994.

[17] A. Cabello, J. M. Estebaranz, and G. García-Alcaine. Bell-Kochen-Specker Theorem: A proof with 18 vectors. *Physics Letters A*, 212:183–187, 1996.

[18] C. Calude. *Information and Randomness—An Algorithmic Perspective*. Springer, Berlin, 2002 (2nd ed.).

[19] C. S. Calude, M. J. Dinneen, M. Dumitrescu, and K. Svozil. Experimental evidence of quantum randomness incomputability. *Physical Review A*, 82, 022102:1–8, 2010.

[20] C. S. Calude, K. Frilya Celine, Z. Gao, S. Jain, L. Staiger, and F. Stephan. Bi-immunity over different size alphabets. *Theoretical Computer Science*, 2021, `https://doi.org/10.1016/j.tcs.2021.09.005`.

[21] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters*, 23(15):880–884, Oct. 1969.

[22] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley. Optimal design for universal multiport interferometers. *Optica*, 3(12):1460–1465, Dec 2016.

[23] B. Cooper. The incomputable reality. *Nature*, 482(7386):465–465, 2012.

[24] B. S. Cooper and P. Odifreddi. Incomputability in nature. In S. B. Cooper and S. S. Goncharov, editors, *Computability and Models: Perspectives East and West*, pages 137–160. Plenum Press, New York, 2003.

[25] J. F. Costa. Incomputability at the foundations of physics (A study in the philosophy of science). *Journal of Logic and Computation*, 23(6):1225–1248, 09 2013.

[26] T. Das, M. Karczewski, A. Mandarino, M. Markiewicz, B. Woloncewicz, and M. Żukowski. Remarks about Bell-nonclassicality of a single photon. *Physics Letters A*, 435:128031, May 2022.

[27] S. Donati and T. Tambosso. Single-photon detectors: From traditional pmt to solid-state spad-based technology. *IEEE Journal of Selected Topics in Quantum Electronics*, 20(6):204–211, 2014.

[28] R. Downey and D. Hirschfeldt. *Algorithmic Randomness and Complexity*. Springer, Berlin, 2010.

[29] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, May 1935.

[30] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov. Invited review article: Single-photon sources and detectors. *Review of Scientific Instruments*, 82(7):071101, 2011.

[31] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov. Invited Review Article: Single-photon sources and detectors. *Review of Scientific Instruments*, 82(7):071101, July 2011.

[32] F. Flamini, N. Spagnolo, N. Viggianiello, A. Crespi, R. Osellame, and F. Sciarrino. Benchmarking integrated linear-optical architectures for quantum information processing. *Scientific Reports*, 7(1):15133, Dec. 2017.

[33] C. Gerry and P. L. Knigh. *Introductory Quantum Optics*. Cambridge University Press, Cambridge, UK, 2005.

[34] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem without inequalities. *American Journal of Physics*, 58:1131–1143, Dec. 1990.

[35] B. Hall. *Lie Groups, Lie Algebras, and Representations: An Elementary Introduction*. Springer, May 2015.

[36] M. Herrero-Collantes and J. C. Garcia-Escartin. Quantum random number generators. *Rev. Mod. Phys.*, 89(1):015004, Feb. 2017.

[37] K. Hess, H. D. Raedt, and K. Michielsen. Hidden assumptions in the derivation of the theorem of Bell. *Physica Scripta*, T151:014002, Nov. 2012.

[38] ID Quantique SA. *Quantis Certifications*. idQuantique, Geneva, Switzerland, April 2016.

[39] ID Quantique SA. *Random Number Generation – White Paper. Quantum versus Classical Random Number Generators*. idQuantique, Geneva, Switzerland, May 2020.

[40] ID Quantique SA. *Random Number Generation – White Paper. What is the Q in QRNG?* idQuantique, Geneva, Switzerland, May 2020.

[41] M. M. Jacak, P. Jóźwiak, J. Niemczuk, and J. E. Jacak. Quantum generators of random numbers. *Scientific Reports*, 11(1):16108, 2021.

[42] S. B. Kochen and E. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics*, 17:59–87, 1967. Reprinted in E. Specker. *Selecta*. Brikhäuser Verlag, Basel, 1990.

[43] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, 79:135–174, Jan 2007.

[44] A. Kulikov, M. Jerger, A. Potočnik, A. Wallraff, and A. Fedorov. Realization of a quantum random generator certified with the Kochen-Specker theorem. *Phys. Rev. Lett.*, 119:240501, Dec 2017.

[45] K. Landsman. Randomness? what randomness? *Foundations of Physics*, 50:61–104, Jan 2020.

[46] J.-Å. Larsson. Loopholes in Bell inequality tests of local realism. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424003, Oct. 2014.

[47] G. Longo. Incomputability in physics. In F. Ferreira, B. Löwe, E. Mayordomo, and L. Mendes Gomes, editors, *Programs, Proofs, Processes*, pages 276–285, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[48] C. K. Lung. *Mathematical Structures Of Quantum Mechanics*. World Scientific Publishing Company, Oct. 2011.

[49] J. Markoff. Flaw found in an online encryption method, https://tinyurl.com/32xuxvkn.

[50] L. Oberreiter and I. Gerhardt. Light on a beam splitter: More randomness with single photons: More randomness with single photons. *Laser & Photonics Reviews*, 10(1):108–115, Jan. 2016.

[51] A. Peres. Two simple proofs of the Kochen-Specker theorem. *Journal of Physics A: Mathematical and General*, 24(4):L175–L178, 1991.

[52] M. Petrov, I. Radchenko, D. Steiger, R. Renner, M. Troyer, and V. Makarov. Independent quality assessment of a commercial quantum random number generator. *EPJ Quantum Technology*, 9(1):17, 2022.

[53] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell's theorem. *Nature*, 464:1021–1024, 2010.

[54] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 73:58–61, Jul 1994.

[55] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji, H. Fu, J. Ornstein, R. P. Mirin, S. W. Nam, and E. Knill. Device-independent randomness expansion with entangled photons. *Nature Physics*, 2021, https://doi.org/10.1038/s41567-020-01153-4.

[56] A. F. G. Solis-Labastida, M. Gastelum, and J. G. Hirsch. The Violation of Bell-CHSH Inequalities Leads to Different Conclusions Depending on the Description Used. *Entropy*, 23(7):872, July 2021.

[57] K. Svozil. The quantum coin toss—testing microphysical undecidability. *Physics Letters A*, 143:433–437, 1990.

[58] K. Svozil. Three criteria for quantum random-number generators based on beam splitters. *Physical Review A*, 79(5):054306, 2009.