PROCEEDINGS A

royalsocietypublishing.org/journal/rspa

Research

Cite this article: Trejo JMA, Calude CS. 2023 Photonic ternary quantum random number generators. *Proc. R. Soc. A* **479**: 20220543. https://doi.org/10.1098/rspa.2022.0543

Received: 13 August 2022
Accepted: 28 April 2023

Subject Areas:
quantum physics, mathematical physics, algorithmic information theory

Keywords:
three-dimensional Hilbert space, randomness, maximal unpredictability, incomputability

Author for correspondence:
Cristian S. Calude
e-mail: cristian@cs.auckland.ac.nz

Photonic ternary quantum random number generators

José Manuel Agüero Trejo and Cristian S. Calude

School of Computer Science, University of Auckland, Auckland, New Zealand

JMAT, 0000-0001-9631-0326; CSC, 0000-0002-8711-6799

We construct a class of three-dimensional photonic quantum random number generators (QRNGs) and prove that each of them generates maximally unpredictable digits via measurements that are robust to errors. This shows that every sequence generated is strongly incomputable; hence its quality is provably better than that of every pseudo-random sequence. These results suggest that incomputability in physics is real and practically applicable. Finally, we present photonic implementations of three-dimensional QRNGs and discuss device independence.

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 and the many pitfalls of pseudo-random number generators (PRNGs), sometimes catastrophic [1]. QRNGs are generally considered to be 'better than PRNGs' because they are based on the 'fundamental unpredictability of well-chosen and controlled quantum processes' [2], a statement that requires more scientific arguments than a simple assertion, particularly because the notion of 'true randomness' is mathematically vacuous [3].

The first photonic QRNG called *Quantis* was produced by ID Quantique in 2001, and it is based on the standard beamsplitter experiment, see figs 1 and 2 in [4]. For an experimental analysis of the quality of *Quantis*, see [5–8].

In this paper, we present a uniform method to construct a class of photonic three-dimensional QRNGs based on a universal unitary operator and a method to

THE ROYAL SOCIETY PUBLISHING

derive a valid preparation of quantum value indefinite states (that satisfy the located Kochen–Specker Theorem [9]) whose measurements produce outcomes with a pre-given probability distribution.

The new method generalizes the constructions of three-dimensional QRNGs described in [10,11], where two natural probability distributions have been considered. The method uses a *fixed universal* unitary operator—obtained as a composition of two-dimensional unitary operators—and a valid value indefinite state repeatedly measured; the outcomes obtained by the measurements have a pre-given probability distribution. In this way, the located Kochen–Specker Theorem [12] 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 [13]); 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* three-dimensional QRNG *is provably better than that of any pseudo-random generator*.

Some QRNGs, like those based on a standard beamsplitter, have no certification and rely instead on a statistical analysis of experimental outcomes. Other QRNGs, like [14], are certified by Bell Theorem [15] or a located variant of Kochen–Specker Theorem [9]. The strength of certification depends on its assumptions. The certification of the three-dimensional QRNGs discussed in this article is unique because (i) the assumptions used have been experimentally validated [16], (ii) the robustness of measurements was proved theoretically [17,18], and (iii) the quality of very long strings of quantum random digits generated with the three-dimensional QRNGs was experimentally shown to be better than that of the best PRNGs using non-statistical randomness tests [16]. No other QRNG, among the many reviewed in the recent survey of the state-of-the-art of QRNGs [19], is certified to such a degree.

Finally, the Kochen–Specker Theorem is valid only for Hilbert spaces of dimension at least three; hence the certification given in this paper does not work for the two-dimensional QRNGs [20], in particular for the beamsplitter used by *Quantis* [2].

The paper is organized as follows. Section 2 is devoted to notation, definitions and prerequisite results; in §3, we construct a universal photonic unitary operator, and in §4, we construct a class of valid quantum value indefinite observables. Section 5 presents the formal certification of the quantum random generator and shows that every sequence produced by the three-dimensional QRNG is incomputable: *no sequence produced by such a* three-dimensional QRNG *can be reproduced exactly by any algorithm, in particular, by any pseudo-random generator*. In §6, we present a photonic realization of the three-dimensional QRNG. Section 7 discusses device independence. Section 8 includes conclusions and two open questions. The appendix contains short comments on the Kochen–Specker theorem (§a), the dimensionality of photons and value indefiniteness (§b).

2. Notation, definitions and prerequisite results

The positive integers, reals and complex sets 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 also be 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 $i \in \mathrm{dom}(\varphi)$ [21].

Next, we present the necessary notions and assumptions of quantum theory, followed by the main result, which allows the 'algorithmic location' of value indefinite observables. A definite value is precisely a (deterministic) hidden variable specifying, in advance, the result of the measurement of an observable.

We denote the observable projecting onto the linear subspace spanned by a vector $|\psi\rangle$ as $P_\psi = |\psi\rangle\langle\psi|/|\langle\psi|\psi\rangle|$. We then fix a positive integer $n > 2$ and let $O \subseteq \{P_\psi \mid |\psi\rangle \in \mathbb{C}^n\}$ be a non-empty set of one-dimensional projection observables on the Hilbert space $\mathbb{C}^n$.

The quantum measurement of an observable is non-contextual if its outcome is independent of the 'context', i.e. is independent of how the observable is measured. The formal definitions are as follows. 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 $P_\psi \neq P_\phi$, $\langle\psi|\phi\rangle = 0$. A *value assignment function* (on O) is a partial function $v : O \to \{0, 1\}$ assigning values to some (possibly all) observables in O.[1] 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*[2] 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.

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 insufficient.[3] Motivated by Einstein *et al*.'s definition of *physical reality* ([22], 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 [18]:

— **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 $v(P_\psi) = 1$.

Theorem 2.1 (Located Kochen–Specker [9,17,18]). *Consider a quantum system described by the state $|\psi\rangle$ in a Hilbert space $\boldsymbol{C}^n$, $n \geq 3$. 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.*

We assume knowledge of elementary computability and algorithmic information theories over different size alphabets [3] and quantum optics [23]. Finally, we use two- and three dimensions for 'two' and 'three' dimensionalities, respectively.

3. A universal photonic unitary operator

In this section, we present a set-up satisfying the conditions of theorem 2.1 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[4] particle [9] as described by its corresponding

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

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

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

[4]Many results in this section hold for an arbitrary three-dimensional particle.

unitary decomposition, where the desired probability distribution can be achieved with careful state preparation.

(a) Spectral decomposition

In this section, we prove a slightly more general form of theorem 2.1 in terms of spectral decomposition.

According to theorem 2.1, 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.

Theorem 3.1. *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 2.1 works 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 admissibility property of v serves as a generalization of the sum rule corresponding to the physical interpretation of the measurement process.

(b) A generalized spin-1 observable

The property *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 preparation state $|S_z\rangle$ effect 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 $\mathbf{S}$ as a triplet of operators $\mathbf{S} = (S_x, S_y, S_z) = \hbar\boldsymbol{\sigma}$, where $\boldsymbol{\sigma}$ corresponds to the generalized Pauli matrices for a spin-1 particle. Then, by adopting units in which $\hbar$ is numerically equal to unity, we obtain the generalized observable that describes the measurement context

$$S(\theta, \vartheta) = \mathbf{u} \cdot \mathbf{S} = \begin{pmatrix} \cos(\theta) & \frac{e^{-i\vartheta}\sin(\theta)}{\sqrt{2}} & 0 \\ \frac{e^{i\vartheta}\sin(\theta)}{\sqrt{2}} & 0 & \frac{e^{-i\vartheta}\sin(\theta)}{\sqrt{2}} \\ 0 & \frac{e^{i\vartheta}\sin(\theta)}{\sqrt{2}} & -\cos(\theta) \end{pmatrix}. \tag{3.1}$$

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

(c) 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

$$U_x = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2} & 1 \\ \sqrt{2} & 0 & -\sqrt{2} \\ 1 & -\sqrt{2} & 1 \end{pmatrix}. \tag{3.2}$$

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 two-dimensional Hilbert space.

Every matrix $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ 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:

$$\begin{pmatrix} u' \\ v' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\beta^* & \alpha^* \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}. \tag{3.3}$$

This relation plays an essential role in formulating a transformation produced by a lossless beamsplitter and external phase shifter to represent the annihilation operators of the quantum harmonic oscillator [23]. 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:

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

As demonstrated in [24], given an arbitrary unitary operator, we can represent a generalized 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.

The non-unicity of unitary decompositions and the unavoidable imperfections in every experimental set-up imply that only some choices are suitable for physical implementation. Consequently, a unitary decomposition must be carefully constructed to reduce internal loss, minimize 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 realization. In what follows, we use the method [25] because the analysis in [26] concluded that it achieves a more balanced mixture of the optical modes, a reduced propagation loss and a better scaling of fidelity than the method [24].[5]

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

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

and

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

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

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

royalsocietypublishing.org/journal/rspa Proc. R. Soc. A 479: 20220543

We then obtain the following decomposition:

$$B_{2,3}\cdot B_{1,2}\cdot U_x\cdot B_{1,2}^{-1}=\begin{pmatrix}1&0&0\\0&-1&0\\0&0&-1\end{pmatrix}=D. \tag{3.4}$$

Thus, from (3.4), we get

$$U_x=B_{1,2}^{-1}\cdot B_{2,3}^{-1}\cdot D\cdot B_{1,2}=B_{1,2}^{-1}\cdot B_{2,3}\cdot D\cdot B_{1,2}. \tag{3.5}$$

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

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

hence we have

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

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

(d) Invariance of value-indefinite observables

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

Recall that the group $O(3)$ formed by the orthogonal transformations in a three-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 particles [27] allowing the derivation of the generalized spin-1 observable. Furthermore, there is an important 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 [28].

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 $\langle A, B\rangle = (1/2)\mathrm{Tr}(AB)$, 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

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

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

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

and

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

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 $SU(2)$ onto $SO(3)$.[6]

Thus, the action of the two-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 §3b).

Furthermore, as U_x preserves the measurement context described by the spin state operator $S_x = S((\pi/2), 0)$, 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 3.2. *The operator U_x defined by (3.5) preserves three-dimensionality, hence value indefiniteness, i.e. if ψ is value indefinite, then $U_x(\psi)$ is also value indefinite.*

4. Construction of value indefinite quantum states

In this section, we construct value indefinite quantum states, which, by measurement, produce outcomes with a given probability distribution (p_1, p_2, p_3), where $\sum_i p_i = 1$ and $0 < p_i < 1$. Consider the standard Cartesian basis and the spin state operator S_x from §3b.

The desired probability distribution is

$$\left.\begin{aligned} \mathcal{P}(S_x, 1) &= \left|\langle 1_x|\phi^*\rangle\right|^2 = p_1, \\ \mathcal{P}(S_x, 0) &= \left|\langle 0_x|\phi^*\rangle\right|^2 = p_2 \\ \text{and} \qquad \mathcal{P}(S_x, -1) &= \left|\langle -1_x|\phi^*\rangle\right|^2 = p_3, \end{aligned}\right\} \tag{4.1}$$

where $|1_x\rangle, |0_x\rangle$ 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 called *valid* if the conditions in (4.1) are satisfied.

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

Thus, for a selection of valid preparation states $|\phi^*\rangle$, we use corollary 3.1 to obtain

$$\left.\begin{aligned}\mathcal{P}(S_x,1)&=\left|\frac{1}{2}\langle 1|\phi^*\rangle+\frac{1}{\sqrt{2}}\langle 0|\phi^*\rangle+\frac{1}{2}\langle -1|\phi^*\rangle\right|^2=p_1,\\ \mathcal{P}(S_x,0)&=\left|\frac{1}{\sqrt{2}}\langle 1|\phi^*\rangle-\frac{1}{\sqrt{2}}\langle -1|\phi^*\rangle\right|^2=p_2\\ \text{and}\quad \mathcal{P}(S_x,-1)&=\left|\frac{1}{2}\langle 1|\phi^*\rangle-\frac{1}{\sqrt{2}}\langle 0|\phi^*\rangle+\frac{1}{2}\langle -1|\phi^*\rangle\right|^2=p_3.\end{aligned}\right\}\tag{4.2}$$

For example, if we choose

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

and

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

we obtain

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

and

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

We have proved:

Theorem 4.1. *The following quantum states are value indefinite with respect to the standard Cartesian basis*

$$\begin{aligned}|\phi\rangle^*=&\left[\pm\sqrt{2}\sqrt{p_2}+z\right]|1\rangle\\ &+\left[\pm\sqrt{p_2}\mp\sqrt{2}\sqrt{p_3}+z\sqrt{2}\right]|0\rangle+\left[\pm\frac{\sqrt{p_1}}{2}\mp\frac{\sqrt{p_2}}{\sqrt{2}}\pm\frac{\sqrt{p_3}}{2}\right]|-1\rangle.\end{aligned}\tag{4.3}$$

for every combination of the signs + and −.

According to theorem 4.1, given a probability distribution (p_1,p_2,p_3), every quantum state in (4.3) is a valid preparation state for the three-dimensional QRNG, and this is obtained by choosing a combination of signs for $|\phi^*\rangle$.

Example 4.2. For the probability distribution $(1/4,1/2,1/4)$, 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 $(1/3,1/3,1/3)$, we get the following valid preparation states:

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

5. Certification

In this section, we prove that *every sequence produced by the proposed* three-dimensional QRNGs *is incomputable*, that is, *no sequence produced by such a* three-dimensional QRNG *can be reproduced exactly by any algorithm, in particular, by any pseudo-random generator. This shows that the quality of the quantum random digits produced by every* three-dimensional QRNG *described in this paper is provable better than the one produced by* any *pseudo-random number generator*.

In detail, consider a process that algorithmically repeats the process of state preparation and measurement, as described in §3, 4 and (c), and let $\mathbf{x} = x_1x_2\ldots$ 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 $\mathbf{x}$, which is equivalent to the incomputability of f, follows from the non-contextuality of definite values; see Section B in [9] for details. We say that a measurement outcome is predictable if f is *computable*; otherwise, f is incomputable, so it offers no method of prediction [29].

A stronger result can be obtained by using the non-probabilistic model for unpredictability [12,30]. 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 is recorded, E is reset', algorithmically iterated finitely many times.

Definition 5.1. 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. 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*, i.e. it must not disturb or interact with E in any way.

Definition 5.2. 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 (i.e. it does not refrain from making a prediction) that is equal to x, the result of the experiment.

Definition 5.3. 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 operating by chance and may not continue to give correct prediction is bounded by $3^{-n}\binom{n}{k} < 2^n/3^n \leq (2/3)^k$. 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 5.4. 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 5.5. *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 converse 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 of 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:

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

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

Assume the **Eigenstate principle**, and the

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

Then, the following results, which follow from Theorem 3 in [30], guarantee the maximum unpredictability of measurements of value indefinite observables:

Theorem 5.6. *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 5.5, we get

Corollary 5.7. *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 4.1, every quantum state in (4.3) is value indefinite and measuring it with the universal unitary operator U_x produces a quantum random ternary digit.

Corollary 5.8. *Every* three-dimensional QRNG *that uses a value indefinite observable* (4.3) *and the universal unitary operator* (3.5) *always generates sequences for which no single digit can be predicted. In particular, every such sequence is 3-bi-immune.*

Every PRNG generates a computable sequence of random digits, hence all digits are algorithmically predictable. By contrast, according to corollary 5.8, no single digit is predictable, so the three-dimensional QRNG is provable better than any PRNG.

6. Photonic realizations of three-dimensional QRNGs

With reference to the notation in §3, we observe that $B_{2,3} \cdot D = D \cdot B_{2,3}$, hence we get

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

These relations allow us to set the reflectivity, transmittance and phase shift values for a physical realization via Mach–Zehnder interferometers: the following table provides the correspondence between equation (3.4) and its physically realizable optical implementation in figure 1.

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

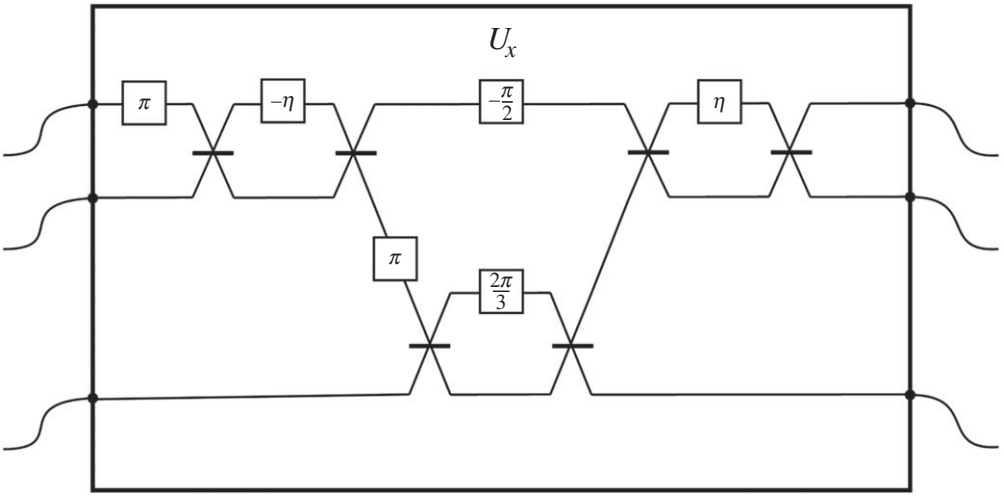

Figure 1. Physical realization of the universal unitary decomposition U_x by means of three-mode multiport interferometer. An arrangement of Mach–Zehnder interferometers consisting of phase shifters and balanced directional couplers illustrates its construction. Here, $\eta = \arccos(\sqrt{2/3})$.

The generic arrangement in figure 1 can be realized with multi-mode interferometers (MMIs). Single-mode waveguides are coupled into a multi-mode fibre characterized by a certain number of allowed modes. Phase modulation can be achieved by using a thermal phase shifter. In silicon devices, it can be implemented by connecting a resistive strip of silicon, beside the waveguide, to a metal pad, to which voltage is applied to control the temperature. By integrating two MMIs (acting as balanced beamsplitters) with a thermal phase shifter, a Mach–Zehnder Interferometer with tunable reflectivity implements the arrangement in figure 1.

The effects of the inherent imperfections in the physical implementation of a three QRNG have to be considered since the certification presented in §5 could be sensitive to experimental implementation errors. For illustration, 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 set-up, and a perfect single-photon detector will detect its final trajectory. However, every experimental realization faces various limitations. There are several flavours of single-photon sources. 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; separation is not 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) [20,31]. Multiple photon emission is not a problem either because the arrangement in figure 1 is based on uncorrelated states [32,33]. Moreover, theorem 2.1, via the condition $0 < |\langle\psi||\phi\rangle| < 1$, provides robustness against non-ideal preparation state fidelity. Experimentally, some valid preparation states may be

easier to obtain with higher fidelity, so an optimal choice will ensure the fidelity remains within the given bound. In this way, the certification in §5 guarantees the *maximal unpredictability* and *strong incomputability*, properties distinguishing the three-dimensional QRNGs from all others [19,34]. In contrast to the three-dimensional QRNGs, multiple photon emission is a severe problem for two-dimensional QRNGs reliant on Bell-type certification. 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 [35].

7. Device independence

Various batteries of statistical tests such as NIST [36] are commonly used to probe the randomness of the strings generated by a QRNG protocol. However, statistical randomness testing cannot discern whether the tested strings originate from a genuine quantum process and have not been generated algorithmically [16]. Various self-testing and semi-self-testing protocols have been formulated [37–39] to address this issue.

Recent literature uses Bell-type inequalities and contextuality-based approaches to assert the unpredictability of quantum measurements and formulate random number generation protocols. The former relies on correlations that violate the constraints described by Bell's Theorem to *certify* that there is no *local* hidden variable describing the measurement outcomes. Here, statistical randomness is extracted from the local measurement of entangled states while device-independently witnessing quantum entanglement or non-locality by observing violations of Bell-type inequalities. The latter relies on bounds derived from results, such as *non-located* versions of the Kochen–Specker theorem (see appendix A), expressing the inability of a non-contextual hidden variable model to reproduce the predictions of quantum mechanics; a measure of minimum entropy quantifies the quality of randomness.

Due to their probabilistic framework and, in some cases, their inability to meet the criteria for value indefiniteness due to dimensionality [40], these types of certification do not guarantee the *maximal unpredictability* of its measurement outcomes. Nonetheless, these approaches offer valuable alternatives for applications where trust cannot be placed in the complete characterization of the device. These approaches can be seen as randomness expansion protocols, requiring 'highly' random inputs to achieve full device independence [41,42]. Using the outputs produced by the three-dimensional QRNGs as inputs for self-testing and semi-self-testing randomness expansion protocols is a way to guarantee the quantum nature and maximal unpredictability of the outcomes generated by these protocols.

8. Conclusion

We have described a class of three-dimensional QRNGs based on a universal photonic unitary operator and a method to construct a class of value indefinite quantum states and proved that it generates maximally unpredictable digits via measurements that are robust to errors. In particular, every sequence generated is strongly incomputable. As discussed in §5, this proves that *their quality of randomness is better than that of every pseudo-random sequence.*

Finally, we discussed photonic implementations of three-dimensional QRNGs (§6), showed their superiority over two-dimensional QRNGs based on Bell-type certification (§5) and the use of three-dimensional QRNGs in device-independent protocols (see §7).

The strong incomputability of every sequence generated by the three-dimensional QRNGs studied in this paper contributes to the much-studied and debated problem of incomputability in physics [43–46]. This paper suggests 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 $\varphi : A_3 \to A_2$

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

transforms by sequential concatenation ternary strings/sequences into binary ones and preserves the certification discussed in §5 for the probability distribution $1/4, 1/2, 1/4$; for proofs, see [21] and §7 in [11].

Finally, we conjecture that (i) the certification of the three-dimensional QRNGs presented in this paper can be strengthened to Martin–Löf randomness [3,47], and (ii) in contrast to three-dimensional beamsplitters, two-dimensional beamsplitters 'lose' information; hence they do not generate maximally unpredictable random sequences.

Data accessibility. This article has no additional data.

Authors' contributions. J.M.A.T.: formal analysis, validation, writing—review and editing; C.S.C.: conceptualization, formal analysis, validation, writing—original draft.

Both authors gave final approval for publication and agreed to be held accountable for the work performed therein.

Conflict of interest declaration. We declare we have no competing interests.

Funding. No funding has been received for this article.

Acknowledgements. We thank A. A. Abbot, E. H. Allen, M. J. Stay, C. Stoica, L. Velez and K. Svozil for discussions and comments, and the anonymous referees for constructive suggestions; they all improved the paper.

Appendix A

(a) Kochen–Specker Theorem

In contrast to the Bell Theorem [15,48], which gives only bounds on probability distributions under the locality assumption, the Kochen–Specker Theorem shows that assuming non-contextuality, it is impossible to assign 'classical' definite values to all possible quantum observables in a consistent manner.

Theorem Appendix A.1 (Kochen–Specker [49–52]). *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, and (iii) v is non-contextual.*

If the conditions for the Kochen–Specker Theorem are satisfied, the outcomes of all quantum measurements on a quantum system cannot be simultaneously predetermined.

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 [30]. Hence the incompatibility between the Kochen–Specker assumptions is not maximal: not all observables need be value indefinite. However, the set of values indefinite has constructive Lebesgue measure one, that is, with probability one, every observable is value indefinite [17].

Finally, all proofs of theorem A.1 are *non-constructive*, in the sense that the proof of the existence of the finite set of observables is not algorithmic. This implies that this theorem cannot be used directly to construct QRNGs. By contrast, the proof of theorem 2.1 is constructive. More details about the Kochen–Specker contextuality can be found in [53].

(b) Spin, dimensionality of photons and value indefiniteness

Although photons are spin-1 particles, they are considered massless. *Helicity* is the projection of the spin onto the direction of momentum. 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, which indicates zero momentum; hence, one can think of this state 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.

However, the mathematical peculiarities of photons indicate that there is valuable three-dimensional information encoded in the traditionally dismissed state. A two-dimensional view of the photonic structure does not fulfil the dimensional requirements imposed by theorem A.1. Still, a three-dimensional analysis allows this result to localize value indefiniteness with a photonic quantum process. To illustrate the relevance of the underlying three-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 or that they occur in a continuum of real and virtual; this continuum can be observed as virtual attributes exhibited by real photons, as in the case of nanophotonics [54], 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. Their peculiarities in dimensionality, as described mathematically and observed experimentally, require that dimensionality is preserved in a quantum system that uses photons to guarantee value indefiniteness.

References

1. Markoff J. Flaw found in an online encryption method. See https://tinyurl.com/32xuxvkn.
2. ID Quantique SA. 2020 *Random Number Generation – White Paper. Quantum versus Classical Random Number Generators*. Geneva, Switzerland: idQuantique.
3. Calude C. 2002 *Information and randomness—an algorithmic perspective*, 2nd edn. Berlin, Germany: Springer.
4. ID Quantique SA. 2020 *Random number generation – White Paper. What is the Q in QRNG?* Geneva, Switzerland: idQuantique.
5. Calude CS, Dinneen MJ, Dumitrescu M, Svozil K. 2010 Experimental evidence of quantum randomness incomputability. *Phys. Rev. A* **82**, 022102. (doi:10.1103/PhysRevA.82.022102)
6. Abbott AA, Bienvenu L, Senno G. 2014 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.
7. ID Quantique SA. 2016 *Quantis certifications*. Geneva, Switzerland: idQuantique.
8. Petrov M, Radchenko I, Steiger D, Renner R, Troyer M, Makarov V. 2022 Independent quality assessment of a commercial quantum random number generator. *EPJ Quantum Technol.* **9**, 17. (doi:10.1140/epjqt/s40507-022-00136-z)
9. Abbott AA, Calude CS, Conder J, Svozil K. 2012 Strong Kochen-Specker theorem and incomputability of quantum randomness. *Phys. Rev. A* **86**, 062109. (doi:10.1103/PhysRevA.86.062109)
10. Kulikov A, Jerger M, Potočnik A, Wallraff A, Fedorov A. 2017 Realization of a quantum random generator certified with the Kochen-Specker theorem. *Phys. Rev. Lett.* **119**, 240501. (doi:10.1103/PhysRevLett.119.240501)
11. Trejo JMA, Calude CS. 2021 A new quantum random number generator certified by value indefiniteness. *Theor. Comput. Sci.* **862**, 3–13. (doi:10.1016/j.tcs.2020.08.014)
12. Abbott AA, Calude CS, Svozil K. 2015 A non-probabilistic model of relativised predictability in physics. *Information* **6**, 773–789. (doi:10.3390/info6040773)
13. Downey R, Hirschfeldt D. 2010 *Algorithmic randomness and complexity*. Berlin, Germany: Springer.
14. Acín A, Masanes L. 2016 Certified randomness in quantum physics. *Nature* **540**, 213–219. (doi:10.1038/nature20119)
15. Bell JS. 1966 On the problem of hidden variables in quantum mechanics. *Rev. Mod. Phys.* **38**, 447–452. (doi:10.1103/RevModPhys.38.447)
16. Abbott AA, Calude CS, Dinneen MJ, Huang N. 2019 Experimentally probing the algorithmic randomness and incomputability of quantum randomness. *Phys. Scr.* **94**, 045103. (doi:10.1088/1402-4896/aaf36a)

17. Abbott AA, Calude CS, Svozil K. 2014 Value indefiniteness is almost everywhere. *Phys. Rev. A* **89**, 032 109–032 116. (doi:10.1103/PhysRevA.89.032109)
18. Abbott AA, Calude CS, Svozil K. 2015 A variant of the Kochen-Specker theorem localising value indefiniteness. *J. Math. Phys.* **56**, 102201. (doi:10.1063/1.4931658)
19. Jacak MM, Jóźwiak P, Niemczuk J, Jacak JE. 2021 Quantum generators of random numbers. *Sci. Rep.* **11**, 16108. (doi:10.1038/s41598-021-95388-7)
20. Herrero-Collantes M, Garcia-Escartin JC. 2017 Quantum random number generators. *Rev. Mod. Phys.* **89**, 015004. (doi:10.1103/RevModPhys.89.015004)
21. Calude CS, Frilya Celine K, Gao Z, Jain S, Staiger L, Stephan F. 2021 Bi-immunity over different size alphabets. *Theor. Comput. Sci.* **894**, 31–49. (doi:10.1016/j.tcs.2021.09.005)
22. Einstein A, Podolsky B, Rosen N. 1935 Can quantum-mechanical description of physical reality be considered complete?. *Phys. Rev.* **47**, 777–780. (doi:10.1103/PhysRev.47.777)
23. Gerry C, Knigh PL. 2005 *Introductory quantum optics*. Cambridge, UK: Cambridge University Press.
24. Reck M, Zeilinger A, Bernstein HJ, Bertani P. 1994 Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73**, 58–61. (doi:10.1103/PhysRevLett.73.58)
25. Clements WR, Humphreys PC, Metcalf BJ, Kolthammer WS, Walmsley IA. 2016 Optimal design for universal multiport interferometers. *Optica* **3**, 1460–1465. (doi:10.1364/OPTICA.3.001460)
26. Flamini F, Spagnolo N, Viggianiello N, Crespi A, Osellame R, Sciarrino F. 2017 Benchmarking integrated linear-optical architectures for quantum information processing. *Sci. Rep.* **7**, 15133. (doi:10.1038/s41598-017-15174-2)
27. Lung CK. 2011 *Mathematical structures of quantum mechanics*. Singapore: World Scientific Publishing Company.
28. Hall B. 2015 *Lie groups, lie algebras, and representations: an elementary introduction*. New York, NY: Springer.
29. Sipser M. 2013 *Introduction to the theory of computation*, 3rd edn. Cambridge, MA: International Thomson Publishing.
30. Abbott AA, Calude CS, Svozil K. 2015 On the unpredictability of individual quantum measurement outcomes. In *Fields of logic and computation II* (eds LD Beklemishev, A Blass, N Dershowitz, B Finkbeiner, W Schulte), vol. 9300 *Lecture Notes in Computer Science*, pp. 69–86. New York, NY: Springer.
31. Oberreiter L, Gerhardt I. 2016 Light on a beam splitter: more randomness with single photons: more randomness with single photons. *Laser Photon. Rev.* **10**, 108–115. (doi:10.1002/lpor.201500165)
32. van Enk SJ, Fuchs CA. 2001 Quantum state of an ideal propagating laser field. *Phys. Rev. Lett.* **88**, 027902. (doi:10.1103/PhysRevLett.88.027902)
33. Walls DF, Milburn GJ. 2008 *Quantum optics*, 2nd edn. Berlin, Germany: Springer.
34. Kavulich JT, Van Deren BP, Schlosshauer M. 2020 Searching for evidence of algorithmic randomness and incomputability in the output of quantum random number generators. *Phys. Lett. A* **388**, 127032. (doi:10.1016/j.physleta.2020.127032)
35. Belinskii AV, Klyshko DN. 1993 Interference of light and Bell's Theorem. *Phys. Usp.* **36**, 653–693. (doi:10.1070/PU1993v036n08ABEH002299)
36. Rukhin A *et al.* 2010 *A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication 800-22 Rev. 1a*. Gaithersburg, MD: National Institute of Standards and Technology (NIST).
37. Lin X, Wang R, Wang S, Yin ZQ, Chen W, Guo GC, Han ZF. 2022 Certified randomness from untrusted sources and uncharacterized measurements. *Phys. Rev. Lett.* **129**, 050506. (doi:10.1103/PhysRevLett.129.050506)
38. Mannalath V, Mishra S, Pathak A. 2022 A comprehensive review of quantum random number generators: concepts, classification and the origin of randomness. (http://arxiv.org/abs/2203.00261)
39. Ma X, Yuan X, Cao Z, Qi B, Zhang Z. 2016 Quantum random number generation. *NPJ Quantum Inf.* **2**, 16021. (doi:10.1038/npjqi.2016.21)
40. Svozil K. 2009 Three criteria for quantum random-number generators based on beam splitters. *Phys. Rev. A* **79**, 054306. (doi:10.1103/PhysRevA.79.054306)
41. Larsson JÅ. 2014 Loopholes in Bell inequality tests of local realism. *J. Phys. A: Math. Theor.* **47**, 424003. (doi:10.1088/1751-8113/47/42/424003)

42. Lapkiewicz R, Li P, Schaeff C, Langford NK, Ramelow S, Wieśniak M, Zeilinger A. 2011 Experimental non-classicality of an indivisible quantum system. *Nature* **474**, 490–493. (doi:10.1038/nature10119)
43. Cooper BS, Odifreddi P. 2003 Incomputability in nature. In *Computability and models: perspectives east and west* (eds SB Cooper, SS Goncharov), pp. 137–160. New York, NY: Plenum Press.
44. Longo G. 2010 Incomputability in physics. In *Programs, proofs, processes* (eds F Ferreira, B Löwe, E Mayordomo, L Mendes Gomes), pp. 276–285. Berlin, Heidelberg. Springer.
45. Cooper B. 2012 The incomputable reality. *Nature* **482**, 465–465. (doi:10.1038/482465a)
46. Costa JF. 2013 Incomputability at the foundations of physics (A study in the philosophy of science). *J. Logic Comput.* **23**, 1225–1248. (doi:10.1093/logcom/ext048)
47. Landsman K. 2020 Randomness? What Randomness? *Found. Phys.* **50**, 61–104. (doi:10.1007/s10701-020-00318-8)
48. Bell JS. 1987 *Speakable and unspeakable in quantum mechanics*. Cambridge, UK: Cambridge University Press.
49. Kochen SB, Specker E. 1967 The problem of hidden variables in quantum mechanics. *J. Math. Mech.* **17**, 59–87. (doi:10.1512/iumj.1968.17.17004) Reprinted in E. Specker. *Selecta*. Brikhäuser Verlag, Basel, 1990.
50. Cabello A. 1994 A simple proof of the Kochen-Specker theorem. *Eur. J. Phys.* **15**, 179. (doi:10.1088/0143-0807/15/4/004)
51. Cabello A, Estebaranz JM, García-Alcaine G. 1996 Bell-Kochen-Specker Theorem: a proof with 18 vectors. *Phys. Lett. A* **212**, 183–187. (doi:10.1016/0375-9601(96)00134-X)
52. Peres A. 1991 Two simple proofs of the Kochen-Specker theorem. *J. Phys. A: Math. Gen.* **24**, L175–L178. (doi:10.1088/0305-4470/24/4/003)
53. Budroni C, Cabello A, Gühne O, Kleinmann M, Larsson JA. 2022 Kochen–Specker contextuality. *Rev. Mod. Phys.* **94**, 045007. (doi:10.1103/RevModPhys.94.045007)
54. Andrews DL, Bradshaw DS. 2014 The role of virtual photons in nanoscale photonics: the role of virtual photons in nanoscale photonics. *Annalen der Physik* **526**, 173–186. (doi:10.1002/andp.201300219)