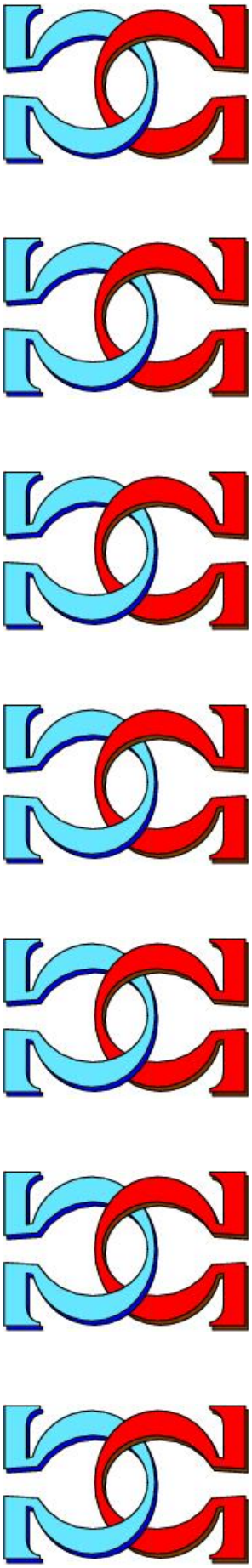

CDMTCS
Research
Report
Series

Testing the 3D QRNG by Undoing

J. M. Agüero Trejo[1], **C. S. Calude**[1], **O.C. Stoica**[2]
[1]University of Auckland, New Zealand
[2]NIPNE-HH, Romania

CDMTCS-587
December 2025

Centre for Discrete Mathematics and
Theoretical Computer Science

Testing the 3D QRNG by Undoing

J. M. Agüero Trejo[*], Cristian S. Calude[†], O. C. Stoica[‡]

December 4, 2025

Abstract

We propose a method to test whether a photonic 3D QRNG works according to the underlying theory, thereby generating highly incomputable sequences of random digits. The test relies on undoing the unitary evolution realized by the 3D QRNG. The test verifies the unitarity, the magnitude of the noise, and other potential errors, such as photon loss or systematic and reproducible fabrication errors. Therefore, the test can confirm the theoretically proven features of the 3D QRNG, for example, the incomputability, or how one has to correct it, if necessary. In addition, the test ensures that the QRNG is not affected by natural limits of quantum measurement accuracy, as those affected by the Wigner-Araki-Yanase Theorem. The test can easily be incorporated into the QRNG and used as an experimental certification.

1 Introduction

The algorithms used in cryptography are highly dependent on the quality of the random numbers used during the encryption processes; hence, the need for Quantum Random Number Generators (QRNG) is increasingly understood and accepted, especially under the expectation that quantum computers could be able to break encryption methods previously considered secure. Genuine randomness, which consists of a mathematical proof of maximal unpredictability, can only be achieved (to date) by Quantum Random Number Generators that measure value indefinite quantum observables, like the 3D-photonic QRNG [7]. In this context, it is essential to provide a broader range of users with a simple empirical test to certify the 3D QRNGs, not just those who can afford expensive technology and laboratories.

We use theoretical and experimental certification to guarantee genuine randomness. Value indefiniteness, which informally means that the random digit is created "out of nothing", and not by scrambling pre-existing digits, is the best theoretical certification, and it can only be provided by applications of the Kochen-Specker Theorem, in its localized form [2, 4, 5] studied in [7]. Bell's Theorem, which offers a different type of certification involving two systems separated in space, doesn't guarantee superiority over any pseudo-RNGs and is more challenging to build with small hardware components.

The 3D QRNGs are certified by other mathematical results, in addition to the Kochen-Specker Theorem. Below are three properties of quantum random sequences generated by a 3D QRNG.

- Every quantum random sequence is maximally unpredictable, meaning no algorithm can accurately predict any of its digits, Theorem 8 in [6].
- Every quantum random sequence is 3-bi-immune, by Theorems 6 and 7 in [6]. This is stronger than bi-immunity, which is stronger than incomputability; see also [12].
- Every quantum random sequence is Borel normal, which means that any digit and any string of digits are generated with the same probability, see Lemma 1 in [6].

[*]School of Computer Science, University of Auckland, New Zealand.
[†]School of Computer Science, University of Auckland, New Zealand.
[‡]Department of Theoretical Physics, NIPNE–HH, Bucharest, Romania. Email: cristi.stoica@theory.nipne.ro, holotronix@gmail.com. Contact author.

These results provide strong theoretical evidence of genuine randomness. However, the physical realization of any device, especially a quantum one, encounters practical obstacles, which result in errors. In integrated quantum photonics, the primary source of errors is photon loss, which occurs in the couplings and waveguides. Additionally, there could be fabrication errors associated with the beam splitter and phase shifter, as well as detection inefficiency. These errors can be detected by specific experimental tests. For example, to detect photon loss and detection inefficiency, we can use heralding and coincidence counting. The usual methods to test the randomness of RNGs, like those provided by NIST [20], are insufficient, but those proposed in [3] ensure a strong empirical support. However, these tests are not easy to use by the usual user of quantum randomness.

In this article, we propose a feasible way to realize a tester for the 3D-photonic QRNG, which can be delivered along with the 3D-photonic QRNG itself, to confirm its validity.

2 Physical constraints of implementations

The theory behind the 3D QRNG is air-tight, being based on value indefiniteness, but no matter how promising the theory may be, it is important to fabricate real-world 3D QRNGs as close as possible to the theoretical one, and to certify them.

For this, we should consider a couple of facts.

First, a very high precision is needed to ensure unitarity and to get the right probabilities, say, $1/4$, $1/2$, and $1/4$. There will always be a small error. However, this can be mitigated under certain conditions by using randomness extractors, see [15] (von Neumann method is an extractor, but it only works for a very limited type of distributions [1]).

Second, there may be a problem regarding the separation of photon counts; a solution with heralding photons will be presented in this paper.

Third, there are theoretical limitations of the practical realizability of quantum components. An important example is expressed by the Wigner-Araki-Yanase Theorem and its generalizations, which apply to measurements of observables that commute with additively conserved quantities, [11, 10, 19]. These limitations are not restricted, to quantum measurements, but also to quantum logic gates, which imposes strict limitations to quantum computing [22, 21]. According to [18], even without explicitly taking into consideration the limits imposed by the Wigner-Araki-Yanase Theorem, the quantum logic gates are constructed in practice in the right way to avoid these problems. In all studied cases the reason is the necessity to ensure unitarity. This applies to observables that are additively conserved, or those that commute with such observables; in particular, spin measurements have these limitations. Do we need this? The proposed use of 3×3 photon beam splitter QRNG can avoid these problems, if realized in a subspace of the Hilbert space that is invariant to unitary evolution, but we still need to do more research to make sure that other similar constraints don't occur. Particularly, our recent result [24] shows that the limitations of accuracy occur both for reading and writing quantum data, although no lower bound is known.

3 More on experimental certification

In addition to the experimental certification that can be obtained as detailed in reference [3], it is important to offer the interested parties the possibility to convince themselves that the random numbers generated are genuinely quantum, and not due to noise. To make sure that the device works and the produced photons have the right properties, we suggest two optional modules:

1. A module that can be coupled to the 3D QRNG and count the output photons, to verify the given probabilities, e.g. $1/4$, $1/2$, $1/4$.
2. A module that can undo the unitary transformation, and prove that the initial state of the photon was recovered, which will be discussed in Section §7.

Another important test is the conservation of 3-bi-immunity.

Together, they can assure the interested parties that the 3D QRNG is actually quantum, and its outputs satisfy the predictions of the underlying quantum theory from [6].

4 Localized Kochen-Specker Theorem

The localized variant of the Kochen-Specker Theorem gives a practical characterization of quantum measurements whose outcomes are indefinite, that is, that are not determined by preexisting properties of the system. This can be used to produce genuinely random numbers by quantum means, as in the case of the 3D-photonic QRNG.

Let $\mathbb{C}^n$, $n > 2$ be a complex Hilbert space. Let $\mathcal{O} \subseteq \left\{\mathsf{P}_\psi := |\psi\rangle\langle\psi| \mid |\psi\rangle \in \mathbb{C}^n, \langle\psi|\psi\rangle = 1\right\}$ be a nonempty set of one-dimensional projection observables on $\mathbb{C}^n$. A *context* is a subset $\mathcal{C} \subset \mathcal{O}$ of $\mathcal{O}$ with n elements so that for all $\mathsf{P}_\psi, \mathsf{P}_\phi \in \mathcal{C}$ with $\mathsf{P}_\psi \neq \mathsf{P}_\phi$, $\langle\psi|\phi\rangle = 0$.

A *value assignment function* on $\mathcal{O}$ is a partial function $v : \mathcal{O} \to \{0, 1\}$, with possible indefinite values for some observables in $\mathcal{O}$. If $v(\mathsf{P}) \in \{0, 1\}$, the observable P is *value definite*; otherwise, it is *value indefinite*. If every observable $\mathsf{P} \in \mathcal{O}$ is value definite, we say that $\mathcal{O}$ is *value definite*.

Before stating the Localized version of the Kochen-Specker Theorem, we need to define the following conditions.

- **Admissibility condition.** To agree with the predictions of quantum mechanics, a value assignment function v on $\mathcal{O}$ has to satisfy the condition: if $v(P) = 1$, then for every P' orthogonal to P, $v(P') = 0$, and if v assigns 0 to $n - 1$ elements in a context, then it must assign 1 to the remaining element.
- **Non-contextuality of definite values**. Every outcome obtained by measuring a value definite observable is *non-contextual*, i.e. it does not depend on other compatible observables which may be measured alongside it. This condition is expected in classical physics, but it is broken by quantum mechanics, as shown by the Kochen-Specker Theorem [16].
- **Eigenstate principle.** For a quantum system prepared in the state $|\psi\rangle$, the projection observable P_ψ is value definite.

We are ready to state the Localized Kochen-Specker Theorem.

Theorem 1 (Localized Kochen-Specker Theorem [2, 4, 5]) *Assume a quantum system prepared in the state $|\psi\rangle$ in a Hilbert space $\mathbb{C}^n$ with $n \geq 3$, and let $|\phi\rangle$ be any quantum state such that $0 < |\langle\psi|\phi\rangle| < 1$. Let $\mathcal{O}$ be a set of one-dimensional projection observables on $\mathbb{C}^n$ containing P_ψ and P_ϕ, and $v : \mathcal{O} \to \{0, 1\}$ a value assignment function. 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.*

In other words, the value obtained by measuring the observed system does not pre-exist, nor is it determined by pre-existing data, it is "created" from scratch during the measurement. This is pure, genuine randomness; it is what Wheeler calls an "elementary act of creation" [25].

5 The 3D-photonic QRNG

The quantum system whose measurement produces quantum random numbers based on Theorem 1 requires a Hilbert space with at least 3 dimensions. We focus on spin-1 observables of a general form

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

In particular, $\mathsf{S}_z = \mathsf{S}(0, 0)$ and $\mathsf{S}_x = \mathsf{S}(\pi/2, 0)$.

To prepare the system, we first measure the value of the spin-1 observable $\mathsf{S}_z = \mathsf{S}(0,0)$, resulting in a value definite state. To measure the system, we need to choose an operator whose eigenvectors are different but not orthogonal to the prepared state. As in [7], we will use the unitary operator corresponding to the spin state operator $\mathsf{S}_x = \mathsf{S}(\pi/2, 0)$,

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

A widely used way to implement unitary matrices is by using beam splitters in integrated photonics, for example with *multimode interferometers* (MMI). A *Mach-Zehnder Interferometer* (MZI) can be obtained by integrating two MMIs with a thermal phase shifter for the phase modulation. Since the MMIs performance is close to an ideal balanced beam splitter, it can be used to prepare the system. Therefore, the unitary operator (2) can be implemented from MZIs realized from MMIs, with very good performance. In addition to being based on value indefiniteness, this implementation does not use entanglement and does not require low temperatures, so it is more practical and accessible than, for example, the 3D QRNG from [17], which requires cooling down to $\sim$20 mK.

The matrix (2) can be realized in terms of beam splitters and single mode phase-shifts [23, 14, 13] as a product of matrices, each of them, when restricted to some two-dimensional subspace, being of the form

$$\mathsf{T}(\theta, \varphi) = \begin{pmatrix} \cos\theta & ie^{i\varphi}\sin\theta \\ i\sin\theta & e^{i\varphi}\cos\theta \end{pmatrix}, \tag{3}$$

and the restriction to the orthogonal complement, which is a one-dimensional subspace, being the identity. Here, $\cos\theta$ represents the reflectivity coefficient, $\sin\theta$ the transmittance coefficient, and φ represents the phase of an external phase shifter on the second input port.

The unitary matrix U to be realized is $N \times N$, where N can be greater than 2. The realization of U is done in terms of $N \times N$ matrices that have the form (3) when restricted to two dimensions represented by adjacent rows/columns j, $j+1$, otherwise being the identity [23, 14, 13]:

$$\begin{aligned} \mathsf{T}_{j,j+1}(\theta,\varphi) &= \begin{pmatrix} \mathsf{I}_{j-1} & 0 & 0 \\ 0 & \mathsf{T}(\theta,\varphi) & 0 \\ 0 & 0 & \mathsf{I}_{N-j-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \cos\theta & ie^{i\varphi}\sin\theta & 0 & \cdots & 0 \\ 0 & \cdots & 0 & i\sin\theta & e^{i\varphi}\cos\theta & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \end{aligned} \tag{4}$$

where I_k is the $k \times k$ identity matrix.

Then, any $N \times N$ unitary matrix U can be written in the form [14]

$$\mathsf{U} = \mathsf{D} \cdot \mathsf{T}_{j_1,j_1+1}(\theta_1,\varphi_1) \cdot \mathsf{T}_{j_2,j_2+1}(\theta_2,\varphi_2) \cdot \ldots \cdot \mathsf{T}_{j_k,j_k+1}(\theta_k,\varphi_k). \tag{5}$$

In addition, it may be needed to multiply the right-hand side of equation (5) with a diagonal matrix D having as diagonal entries only complex numbers of the form $e^{i\phi}$. In our case, the matrix (2) is decomposed as a product involving such matrices in the following ways [7]:

$$\mathsf{U}_x = \mathsf{B}_{1,2}^{-1} \cdot \mathsf{B}_{2,3} \cdot \mathsf{D} \cdot \mathsf{B}_{1,2} = \mathsf{D}' \cdot \mathsf{B}'_{1,2} \cdot \mathsf{B}_{2,3} \cdot \mathsf{B}_{1,2}, \tag{6}$$

where the matrices representing the beam splitters are

$$\mathsf{B}_{1,2} = \begin{pmatrix} \sqrt{\frac{2}{3}} & \frac{1}{\sqrt{3}} & 0 \\ \frac{i}{\sqrt{3}} & -i\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathsf{B}_{2,3} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{i\sqrt{3}}{2} \\ 0 & \frac{i\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix},$$
$$\mathsf{B}_{1,2}^{-1} = \begin{pmatrix} \sqrt{\frac{2}{3}} & -\frac{i}{\sqrt{3}} & 0 \\ \frac{1}{\sqrt{3}} & i\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathsf{B}'_{1,2} = \begin{pmatrix} \sqrt{\frac{2}{3}} & \frac{i}{\sqrt{3}} & 0 \\ -\frac{i}{\sqrt{3}} & -\sqrt{\frac{2}{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{7}$$

The matrices representing the single-mode phase-shifts are

$$\mathsf{D} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \quad \mathsf{D}' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & i & 0 \\ 0 & 0 & -1 \end{pmatrix}. \tag{8}$$

The parameters θ and φ from equation (3), for the matrices (7), are represented in Table 1.

$\mathsf{B}_{m,n}$	θ	φ
$\mathsf{B}'_{1,2}$	$-\operatorname{acos}\sqrt{\frac{2}{3}}$	π
$\mathsf{B}_{2,3}$	$\frac{2\pi}{3}$	π
$\mathsf{B}_{1,2}$	$\operatorname{acos}\sqrt{\frac{2}{3}}$	$-\frac{\pi}{2}$

Table 1: Angles and phases for the beam splitter operators.

The physical realization of the universal unitary decomposition U_x by means of three-mode multiport interferometer is represented in Figure 1, which is reproduced from [7].

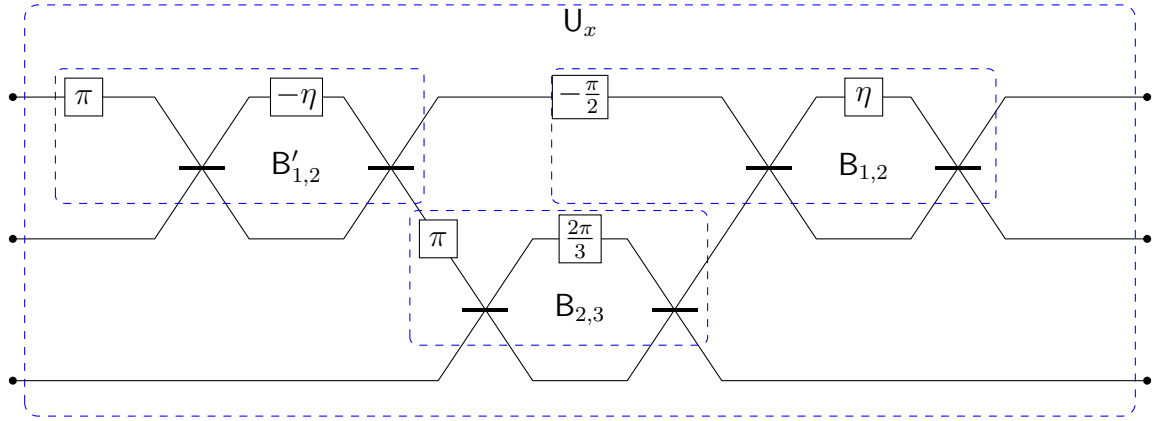

Figure 1: Reproduced from [7]. Physical realization of the universal unitary decomposition U_x by means of three-mode multiport interferometer. An arrangement of Mach–Zehnder interferometers consisting of phase shifters and balanced directional couplers illustrates its construction. Here, $\eta = \operatorname{acos}\frac{\sqrt{2}}{3}$.

6 Modeling errors

The decomposition of U_x from (6) is an idealization, in practice there will be errors. We model the errors by allowing the parameters θ and φ to be slightly different from those from Table 1, for each of the matrices from equation (7), as in Table 2.

$\widetilde{\mathsf{B}}_{m,n}$	θ	φ
$\widetilde{\mathsf{B}}'_{1,2}$	θ_1	φ_1
$\widetilde{\mathsf{B}}_{2,3}$	θ_2	φ_2
$\widetilde{\mathsf{B}}_{1,2}$	θ_3	φ_3

Table 2: Inaccurate angles and phases for the beam splitter operators.

Then, as done in [9], the matrices representing the beam splitters are:

$$\begin{aligned} \widetilde{\mathsf{B}}_{1,2} &= \begin{pmatrix} \mathsf{T}(\theta_3,\varphi_3) & 0 \\ 0 & 1 \end{pmatrix}, \quad \widetilde{\mathsf{B}}_{2,3} = \begin{pmatrix} 1 & 0 \\ 0 & \mathsf{T}(\theta_2,\varphi_2) \end{pmatrix}, \\ \widetilde{\mathsf{B}}_{1,2}^{-1} &= \begin{pmatrix} \mathsf{T}^\dagger(\theta_3,\varphi_3) & 0 \\ 0 & 1 \end{pmatrix}, \quad \widetilde{\mathsf{B}}'_{1,2} = \begin{pmatrix} \mathsf{T}(\theta_1,\varphi_1) & 0 \\ 0 & 1 \end{pmatrix}, \end{aligned} \tag{9}$$

and the matrices representing the single-mode phase-shifts are

$$\widetilde{\mathsf{D}} = \begin{pmatrix} e^{i\phi_1} & 0 & 0 \\ 0 & e^{i\phi_2} & 0 \\ 0 & 0 & e^{i\phi_3} \end{pmatrix}, \quad \widetilde{\mathsf{D}}' = \begin{pmatrix} e^{i\phi'_1} & 0 & 0 \\ 0 & e^{i\phi'_2} & 0 \\ 0 & 0 & e^{i\phi'_3} \end{pmatrix} \tag{10}$$

where $\phi_1 \approx \phi'_1 \approx 0$, $\phi_2 \approx \phi_3 \approx \phi'_3 \approx \pi$, and $\phi'_2 \approx \pi/2$.

Then, instead of equation (6) we have

$$\widetilde{\mathsf{U}}_x = \widetilde{\mathsf{B}}_{1,2}^{-1} \cdot \widetilde{\mathsf{B}}_{2,3} \cdot \mathsf{D} \cdot \widetilde{\mathsf{B}}_{1,2} = \mathsf{D}' \cdot \widetilde{\mathsf{B}}'_{1,2} \cdot \widetilde{\mathsf{B}}_{2,3} \cdot \widetilde{\mathsf{B}}_{1,2}. \tag{11}$$

The imperfect 3D QRNG is represented in Figure 2.

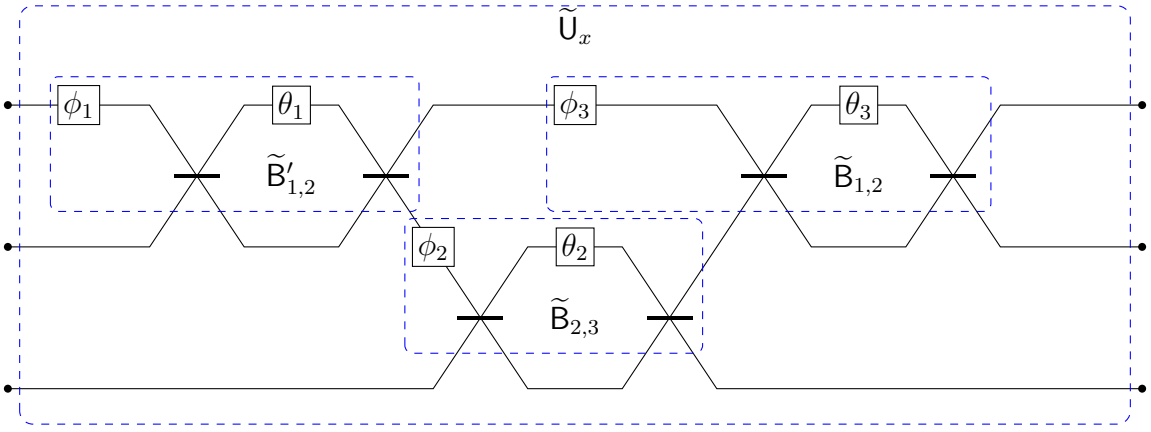

Figure 2: Imprecise 3D-QRNG.

The effect of using MMIs is that we have additional phase shifts, which contribute as additional phase shift matrices in equation (11).

7 Testing unitarity by undoing the QRNG

The test aims to verify

1. the unitarity of the realized QRNG,
2. the accuracy of its physical implementation, by making sure that the unpredictable errors, which are not systematic, are very small.

Figure 3: Phase shift gate.

First, we explain how a module can be constructed that undoes the unitary transformation and recovers the initial state of the photon. To illustrate the idea, we first describe how it can be done for a simple phase shift gate $\mathsf{P}(\varphi)$, which maps $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto e^{i\varphi}|1\rangle$, as in Figure 3.

To test this by reconstructing the original state, we add another phase shift gate with opposite phase, as in Figure 4.

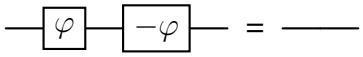

Figure 4: Undoing a phase shift gate.

This will recover the original state. Since the unitary matrix representing the phase shift is

$$\mathsf{P}(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}, \tag{12}$$

what we did to undo it was to multiply by its inverse, which is $\mathsf{P}(\varphi)^{-1} = \mathsf{P}(\varphi)^\dagger = \mathsf{P}(-\varphi)$,

$$\mathsf{P}(\varphi)\mathsf{P}(\varphi)^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\varphi} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{13}$$

The same procedure can be done with the 3×3 beam splitter 3D QRNG: take another one, invert it as needed to get the inverse unitary operation, and plug it into the one that we want to test. The reason why this recovers the original state is that the second device performs the inverse unitary transformation that the first device performs. Then, the output can be tested to verify that it is the same as the input. This will ensure that nothing was lost or disturbed in the process.

This procedure will simultaneously test the unitarity of the 3D QRNG and also the error, since if two copies, one the reverse of the other, can cancel each other's effect, then both of them are accurately fabricated.

Next, we consider an imperfect implementation of the unitary transformation from equation (11). Since all the matrices in this decomposition are supposed to be unitary, we have:

$$\widetilde{\mathsf{U}}_x \widetilde{\mathsf{U}}_x^\dagger = \mathsf{D}' \cdot \widetilde{\mathsf{B}}'_{1,2} \cdot \widetilde{\mathsf{B}}_{2,3} \cdot \widetilde{\mathsf{B}}_{1,2} \cdot \widetilde{\mathsf{B}}_{1,2}^\dagger \cdot \widetilde{\mathsf{B}}_{2,3}^\dagger \cdot \widetilde{\mathsf{B}}_{1,2}'^\dagger \cdot \mathsf{D}'^\dagger = \mathsf{I}_3. \tag{14}$$

This means that, to test the imperfect QRNG from Figure 2, we can use its mirror image to undo the time evolution. Looking at equation (3), we notice that

$$\begin{aligned} \mathsf{T}(\theta,\varphi)^\dagger &= (\mathsf{T}(\theta,0)\mathsf{T}(0,\varphi))^\dagger \\ &= \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}^\dagger \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}^\dagger \\ &= \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\varphi} \end{pmatrix} \begin{pmatrix} \cos(-\theta) & i\sin(-\theta) \\ i\sin(-\theta) & \cos(-\theta) \end{pmatrix} \\ &= \mathsf{T}(0,-\varphi)\mathsf{T}(-\theta,0). \end{aligned} \tag{15}$$

In general, for a unitary matrix $\mathsf{U} = \mathsf{T}_{j_1,j_1+1}(\theta_1,\varphi_1)\ldots\mathsf{T}_{j_k,j_k+1}(\theta_k,\varphi_k)$ as in equation (5),

$$\begin{aligned} \mathsf{U}^\dagger &= (\mathsf{T}_{j_1,j_1+1}(\theta_1,\varphi_1)\ldots\mathsf{T}_{j_k,j_k+1}(\theta_k,\varphi_k))^\dagger \\ &= \mathsf{T}_{j_k,j_k+1}(\theta_k,\varphi_k)^\dagger\ldots\mathsf{T}_{j_1,j_1+1}(\theta_1,\varphi_1)^\dagger \\ &= \mathsf{T}_{j_k,j_k+1}(0,-\varphi_k)\mathsf{T}_{j_k,j_k+1}(-\theta_k,0)\ldots \\ &\quad \ldots\mathsf{T}_{j_1,j_1+1}(0,-\varphi_1)\mathsf{T}_{j_1,j_1+1}(-\theta_1,0). \end{aligned} \tag{16}$$

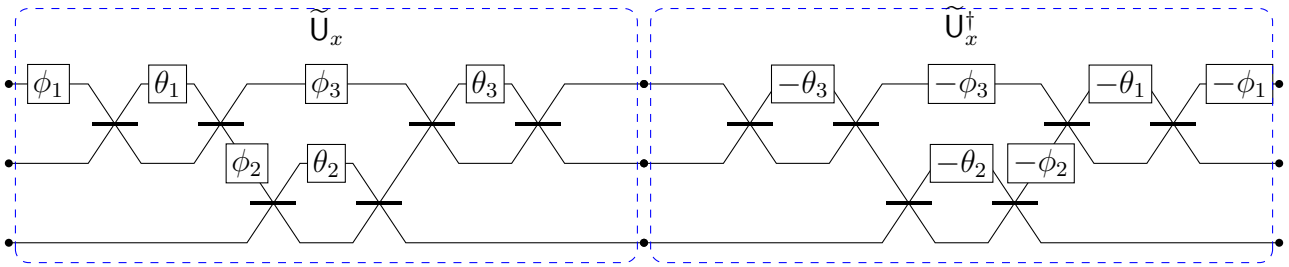

Figure 5: Testing the 3D-QRNG by undoing. At the outputs of the 3D-QRNG implementing the transformation $\widetilde{\mathsf{U}}_x$, we connect the inputs of a mirrored version, which implements the inverse transformation $\widetilde{\mathsf{U}}_x^\dagger$, and verify that we recover the input state.

From these observations, we see that to obtain the mirror QRNG, the order of the components has to be reversed, and each angle and phase have to be inverted, as in Figure 5.

The test is successful if the output of the mirror QRNG is identical to the inputs of the original QRNG. In this case, if the input is fully reconstructed, this will show that

1. even if there are errors, expressed by the difference between the angles and phases from Table 2 and from Table 1, they do not break the unitarity of the device,
2. the QRNG device and its inverted version have almost identical but opposite errors, showing that they are systematic.

If the errors are systematic, they can be corrected, or, if not corrected, one can measure the output probabilities and base on them the statistics of the randomly generated digits.

A schematic representation is given in Figure 6.

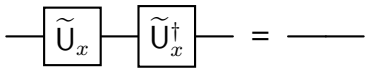

Figure 6: Undoing the unitary transformation $\widetilde{\mathsf{U}}_x$.

A way to test that $\widetilde{\mathsf{U}}_x\widetilde{\mathsf{U}}_x^\dagger = \mathsf{I}$, verifying the unitarity of the transformation $\widetilde{\mathsf{U}}_x$, is to compare the output after the inversion with the input by using interference. More precisely, use a beam splitter to split a photon into two equal-amplitude components, pass a component through the implementation of $\widetilde{\mathsf{U}}_x\widetilde{\mathsf{U}}_x^\dagger$ and then make it interfere with the other component, ensuring that there are no losses and phase differences.

Remark 1 *Note that we do not need to ensure that the operator $\widetilde{\mathsf{U}}_x$ is exactly the operator U_x from equation (2): it is sufficient to ensure that it realizes a sharp measurement and that it satisfies the conditions of Theorem 1. That is, we will allow systematic errors, due to imperfect realization, as long as their effect is kept under control and can be undone by additional phase shifts to test that all conditions are met. A positive unitarity test would show that orthogonal vectors in the input are mapped to orthogonal vectors in the output, ensuring sharpness. If all outputs trigger the detectors sometimes, when there is input only in one mode, the condition $0 < |\langle\psi|\phi\rangle| < 1$ is satisfied as well. Therefore, based on Theorem 1, passing the test of unitarity by inversion should be sufficient to ensure the value indefiniteness of the generated digits.*

8 Generalizations

The test based on inversion can be applied to implementations of other unitary matrices, including $N \times N$ matrices with $N > 3$. In particular, it works for testing the N-dimensional QRNG proposed in [8].

In addition, it is possible to perform tests by coupling more imperfect copies of the QRNG and their mirror images. This will amplify the potential errors and make their detection and quantification easier.

A possible arrangement consists of placing all the mirror images at the back

$$\left(\widetilde{\mathsf{U}}_{x,1} \cdot \ldots \cdot \widetilde{\mathsf{U}}_{x,n}\right) \cdot \left(\widetilde{\mathsf{U}}'^{\dagger}_{x,n} \cdot \ldots \cdot \widetilde{\mathsf{U}}'^{\dagger}_{x,1}\right) \cong \mathsf{I}, \tag{17}$$

or in alternating them,

$$\left(\widetilde{\mathsf{U}}_{x,1} \cdot \widetilde{\mathsf{U}}'^{\dagger}_{x,1}\right) \cdot \ldots \cdot \left(\widetilde{\mathsf{U}}_{x,n} \cdot \widetilde{\mathsf{U}}'^{\dagger}_{x,n}\right) \cong \mathsf{I}. \tag{18}$$

It is even possible to test any permutation of n QRNGs $\widetilde{\mathsf{U}}_{x,j}$ and n mirror QRNGs $\widetilde{\mathsf{U}}'^{\dagger}_{x,j}$, where $j \in \{1, \ldots, n\}$. This will allow the errors to propagate from one arm to another and interfere, which can result in evidence from errors in the phases that otherwise could be missed.

Another test is possible due to the observation that, from equation (2), $\mathsf{U}_x^{\dagger} = \mathsf{U}_x$. It follows that, if the implementation is expected to be accurate enough and self-adjoint, we should be able to undo the time evolution simply by connecting two copies of the device in Figure 5. The tests that amplify the errors, as in equations (17) and (18), are realized, in this case, simply by connecting an even number of copies of the QRNG,

$$\widetilde{\mathsf{U}}_{x,1} \cdot \ldots \cdot \widetilde{\mathsf{U}}_{x,2n} \cong \mathsf{I}. \tag{19}$$

In this case, the same test will verify not only the unitarity, but also the self-adjointness of the operator U_x.

9 Conclusions

In summary, it is of extreme importance to test all aspects of the 3D QRNG, both to ensure the quality of the product and to gain the trust of users. This includes

1. The physical testing of possible errors and deviations from the ideal ratios.
2. Testing the conservation of bi-immunity.
3. Ensuring that the limits imposed by the conservation laws, as per the Wigner-Araki-Yanase Theorem, don't affect the product. For this, we need to follow [18].
4. Testing the unitarity by using a second, reversed 3D QRNG module.

The test based on inversion can be applied for any dimension, including 2D QRNGs based on beam splitters. It can be applied to any QRNGs that rely on a known prepared state and known measurement achievable by realizing a unitary transformation. The test does not apply to QRNGs based on noise or decay, because these processes are not invertible.

The test based on inversion does not ensure the exact unitary process as in equation (2), but this is unnecessary: it suffices that a sharp measurement is obtained, that the conditions of Theorem 1 are satisfied, and that the resulting probabilities are the expected ones. The first two conditions can be verified by the experiment proposed in this article, while the third can be verified by a statistical analysis of the outcomes.

10 Acknowledgement

We are indebted to Prof. M. Zimand for comments that improved our presentation.

References

[1] A. A. Abbott and C. S. Calude. Von Neumann normalisation of a Quantum Random Number Generator. *Computability*, 1(1):59–83, 2012.

[2] 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.

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

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

[5] 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.

[6] J. M. Agüero Trejo and C. S. Calude. New Quantum Random Number Generators certified by value indefiniteness. *Theoretical Computer Science*, 2020.

[7] J. M. Agüero Trejo and C. S. Calude. Photonic ternary Quantum Random Number Generators. *Proc. R. Soc. A*, 479:1–16, 2023.

[8] J. M. Agüero Trejo and C. S. Calude. An N-dimensional Quantum Random Number Generator. *Manuscript in preparation*, 2025. In preparation.

[9] J. M. Agüero Trejo, C. S. Calude, and O. C. Stoica. The role of experimental errors in 3D-Photonic QRNGs. *Manuscript in preparation*, 2025. In preparation.

[10] H. Araki and M. Yanase. Measurement of quantum mechanical operators. *Phys. Rev.*, 120(2):622, 1960.

[11] P. Busch. Translation of "Die Messung quantenmechanischer Operatoren" by EP Wigner. *Arxiv preprint quant-ph/1012.4372*, pages 1–10, December 2010. arXiv:quant-ph/1012.4372.

[12] 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.

[13] D. Cilluffo. Commentary on the decomposition of universal multiport interferometers: how it works in practice. *Arxiv preprint quant-ph/2412.11955*, pages 1–13, 2024. arXiv:quant-ph/2412.11955.

[14] 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, 2016.

[15] M. Herrero-Collantes and J. C. Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004, 2017.

[16] 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.

[17] 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.

[18] D. Lidar. Comment on "Conservative quantum computing". *Phys. Rev. Lett.*, 91(8):089801, 2003.

[19] L. Loveridge and P. Busch. 'measurement of quantum mechanical operators' revisited. *Eur. Phys. J. D*, 62(2):297–307, 2011.

[20] National Institute of Standards and Technology (NIST). Post-quantum cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography, 2025. Accessed: 2025-04-25.

[21] M. Ozawa. Conservative quantum computing. *Phys. Rev. Lett.*, 89(5):057902, 2002.

[22] M. Ozawa. Wigner-Araki-Yanase theorem and the realizability of quantum computing (mathematical study of quantum dynamical systems and its application to quantum computer). *https://core.ac.uk/download/pdf/39174271.pdf*, 1350:76–84, 2004.

[23] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73(1):58–61, 1994.

[24] O. Stoica. Can we accurately read or write quantum data? *Preprint arXiv:2404.05633*, 2024.

[25] J. A. Wheeler. Law without law. In *Quantum Theory and Measurement*, pages 182–213, Princeton, NJ, 1983. Princeton University Press.