Three-Dimensional Quantum Random Generator: Theory, Realisation and Testing or Suplementary Material to “How Real Is Incomputability in Physics”???

José Manuel Agüero[1] Trejo, Cristian S. Calude[1] Michael J. Dinneen[1],
Arkady Fedorov[2,3], Anatoly Kulikov[2,3], Rohit Navarathna[2,3], Karl Svozil[4]

[1]School of Computer Science, University of Auckland, New Zealand
[2]School of Mathematics and Physics, University of Queensland, Australia
[3]ARC Centre of Excellence for Engineered Quantum Systems, Queensland, Australia
[4]Institute für Theoretische Physik, TU Wien, Vienna, Austria

October 14, 2022

Abstract

Something

[21, 2]

1 Introduction

There are several methods to generate quantum randomness, among them radioactive decay [19, 20], diodes, as well as quantum coin tosses [34, 16, 15]. In what follows we shall concentrate on the latter type of quantum random number generators from generalized beam splitters [27], with the additional benefit of certification relative to quantum contextuality [35, 25].

Thereby, the (meta)physical message—rather a hypothesis—according to one of the current nobel prize winners in physics is that of irreducible randomness [39]:

> . . . for the individual event in quantum physics, not only do we not know the cause, there is no cause.

The essential feature of quantum randomness resides in its ontological *underdetermination*, as compared to epistemic, subjective but not objective [14] uncertainty reducible to ignorance of classical physical states and evolution, even in the case of chaotic behaviour.

Quantum underdetermination can be expressed in terms of gaps in the physical description [12, 13, § III.12-14]: due to the unitarity of the quantum evolution information cannot be created nor annihilated. Therefore, if a quantized system encodes a finite amount of information any query in excess of this information must inevitably be indeterminate and value indefinite relative to the original quantum state. One could, of course, suppose that such a request can be fulfilled by the entanglement with the measurement apparatus and thus the environment at large [22, 23], resulting in an unbounded nesting argument with an ever increasing Heisenberg cut. Yet the fact remains that, due to the finite (possibly relational [38]) amount of information encoded in a quantized system, information in excess of this amount cannot reside or be encoded in any pre-selected state.

Underdetermination gets also expressed in the Kochen-Specker theorem and other configurations of observables with a scarcity of two-valued states associated with simultaneous classical truth assignments [17, Theorem 0]. This is also true for Boole's conditions of possible experience in non-local configurations under strict Einstein causality [36, 40, 41].

As a result the current quantum canon can charactrized in theological, scholastic terms as *Creatio Continua*, the continuous creation of randomness on a massive scale. Another alternative is the postulate of non-local hidden parameters; an assumption that lacks any current empirical basis.

2 3D QRNG – Theory

The 3D QRNG constructs a value-indefinite observable and then measures it, in a repetitive manner; the probability distribution of the outcomes is $1/4, 1/2, 1/4$.

In this section we present the theoretical framework allowing the construction of value-indefinite observables, their tolerance to measurement errors and the certification of the degree of randomness of their outcomes.

2.1 Notation and definitions

The set of positive integers will be denoted by $\mathbb{N}$. Consider the alphabet $A_b = \{0, 1, \ldots, b-1\}$, where $b \geq 2$ is an integer; the elements of A_b are to be considered the digits used in natural positional representations of numbers in the interval $[0, 1)$ at base b. By A_b^* and A_b^ω we denote the sets of (finite) strings and (infinite) sequences over the alphabet A_b. Strings will be denoted by x, y, u, w; the length of the string $x = x_1 x_2 \ldots x_m$, $x_i \in A_b$, is denoted by $|x|_b = m$ (the subscript b will be omitted if it is clear from the context); A_b^m is the set of all strings of length m. Sequences will be denoted by $\mathbf{x} = x_1 x_2 \ldots$; the prefix of length m of $\mathbf{x}$ is the string $\mathbf{x}(m) = x_1 x_2 \ldots x_m$. Strings will be ordered quasi-lexicographically according to the natural order $0 < 1 < 2 < \cdots < b-1$ on the alphabet A_b. For example, for $b = 2$, we have $0 < 1 < 00 < 01 < 10 < 11 < 000\ldots$. We assume knowledge of elementary computability theory over different size alphabets [8].

By $\mathbb{C}$ we denote the set of complex numbers. We then fix a positive integer $n \geq 2$ and let $O \subseteq \{P_\psi : |\psi\rangle \in \mathbb{C}^n\}$ be a non-empty set of one-dimensional projection observables on the Hilbert space $\mathbb{C}^n$.

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 $P_\psi \neq P_\phi, \langle\psi|\phi\rangle = O$. A *value assignment function* (on O) is a partial function $v : O \to \{0, 1\}$ assigning values to some (possibly all) observables in O. The partiality of the function v means that $v(P)$ can be $0, 1$ or indefinite. An observable $P \in O$ is *value definite* (under the assignment function v) if $v(P)$ is defined, i.e. it is 0 or 1; 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 then fix a positive integer $n \geq 2$ and let $O \subseteq \{P_\psi : |\psi\rangle \in \mathbb{C}^n\}$ be a non-empty set of one-dimensional projection observables on the Hilbert space $\mathbb{C}^n$. 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 $P_\psi \neq P_\phi, \langle\psi|\phi\rangle = O$. A *value assignment function* (on O) is a partial function $v : O \to \{0, 1\}$ assigning values to some (possibly all) observables in O. The partiality of the function v means that $v(P)$ can be $0, 1$ or indefinite. An observable $P \in O$ is *value definite* (under the assignment function v) if $v(P)$ is defined, i.e. it is 0 or 1; otherwise, it is *value indefinite* (under v). Similarly, O is *value definite* (under v) if every observable $P \in O$ is value definite.

2.2 Localised Kochen-Specker Theorem

We next present the main result used to construct a value indefinite observable. First, we assume the following premises:

- **Admissibility.** Fix a set O of one-dimensional projection observables on $\mathbb{C}^n$ and the value assignment function $v : O \to \{0, 1\}$. Then v is *admissible* if for every context C of O, we have that $\sum_{P \in C} v(P) = 1$. This condition postulates that only one projection observable in a context can be assigned the value 1. This gurantees the agreement with quantum mechanics predictions.

- **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.

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

The last assumption is motivated by Einstein, Podolsky and Rosen definition of *physical reality* [11, 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*

prior to observation corresponding to this physical quantity.

It gives a criterion for value-definitiness: 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 $v(P_\psi) = 1$.

We can state now main result:

Theorem 1 (Localised Kochen-Specker Theorem [3, 4, 21, 6]) *Assume a quantum system prepared in the state $|\psi\rangle$ in a dimension $n \geq 3$ Hilbert space $\mathbf{C}^n$, and let $|\phi\rangle$ be any quantum state such that $0 < |\langle\psi|\phi\rangle| < 1$. If the following three conditions are satisfied: i) admissibility, ii) non-contextuality and iii) eigenstate principle, then the projection observable P_ψ is value indefinite.*

Theorem 1 states that, under the given assumptions, any quantum state $|\phi\rangle$ that is neither orthogonal nor parallel to $|\psi\rangle$ is *value indefinite*. This result has two major consequences:

1. it shows how to effectively construct a value indefinite observable, and
2. it guarantees that the status of "value-indefiniteness" is invariant under the small errors in measurements: this is a very important property as no measurement is exact.

How "good" is such a 3D QRNG, i.e. what randomness properties can be *certified* for their outcomes? For example, can we prove that the outcomes of the 3D QRNG are "better" than the outcomes produced by *any* pseudo-random number generator (PRNG)?

We note that Theorem 1, as the original Kochen-Specker Theorem, is not true in $\mathbf{C}^2$ [18], so the requirement to work in $\mathbf{C}^3$.

For certification we use the following new assumption:

- **epr principle**: If a repetition of measurements of an observable generates a computable sequence, then these observables are value definite.

Based on the Eigenstate and epr principles we can prove that the answer to the last question is affirmative. Any infinite repetition of the experiment measuring a quantum value indefinite observable generates an incomputable infinite sequence $x_1x_2\ldots$: no PRNG has this randomness property.

A stronger result is in fact true. Informally, a sequence $\mathbf{x}$ is bi-immune if no algorithm can generate infinitely many correct values of its elements (pairs, (i, x_i)). Formally, a. sequence $\mathbf{x} \in A_b^\omega$ ($b \geq 2$) is *bi-immune* if there is no partially computable function φ from $\mathbb{N}$ to A_b having an infinite domain $\mathrm{dom}(\varphi)$ with the property that $\varphi(i) = x_i$ for all $i \in \mathrm{dom}(\varphi)$ [7]).

Theorem 2 ([1, 6]) *Assume the Eigenstate and epr principles. An infinite repetition of the experiment measuring a quantum value indefinite observable in $\mathbb{C}^b$*

always generates a b-bi-immune sequence $\mathbf{x} \in A_2^\omega$*, for every* $b \geq 2$*.*

In particular, every sequence generated by the 3D QRNG is 3-bi-immune.

Theorem 3 ([6]) *Assume the epr and Eigenstate principles. Let* $\mathbf{x}$ *be an infinite sequence obtained by measuring a quantum value indefinite observable in* $\mathbb{C}^b$ *in an infinite repetition of the experiment E. Then no single bit* x_i *can be predicted.*

In particular, no single digit of every sequence $\mathbf{x} \in A_3^\omega$ generated by the 3D QRNG can be algorithmically predicted.

The following simple morphism $\varphi\colon A_3 \to A_2$ transforms a ternary sequence into a binary sequence:

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

which can be extended sequentially for strings, $\mathbf{y}(n) = \varphi(\mathbf{x}(n)) = \varphi(x_1)\varphi(x_2) \ldots \varphi(x_n)$ and sequences $\mathbf{y} = \varphi(\mathbf{x}) = \varphi(x_1)\varphi(x_2)\ldots\varphi(x_n)\ldots$. This transformation preserves 2-bimmunity:

Theorem 4 ([6]) *Assume the epr and Eigenstate principles. Let* $\mathbf{y} = \varphi(\mathbf{x})$*, where* $\mathbf{x} \in A_3^\omega$ *is a ternary sequence generated by the QRNG and* φ *is the alphabetic morphism defined in (1). Then, no single bit of* $\mathbf{y} \in A_2^\omega$ *can be predicted.*

As noted in [6], Theorem 1 shows that, given a system prepared in state $|\psi\rangle$, a one-dimensional projection observable can only be value definite if it is an eigenstate of that observable. Consequently, for any diagonalisable observable O with spectral decomposition $O = \sum_{i=1}^{n} \lambda_i P_{\lambda_i}$, where λ_i denotes each distinct eigenvalue with corresponding eigenstate $|\lambda_i\rangle$, O has a predetermined measurement outcome if and only if each projector in its spectral decomposition has a predetermined measurement outcome. Thus, the previous result holds true to the outcome of the measurement of any observable with non-degenerate spectra. Such generalisation is particularly useful in the case when we use the value assignment function to represent a value definite observable. These results have been used to design the following quantum operators of the 3D QRNG. These QRNGs operate in a succession of events of the form "preparation, measurement, reset", iterated indefinitely many times in an algorithmic fashion [1]. The first 3D QRNG was designed in [1], realized in [21] and analysed in [2]. While the analysis failed to observe a strong advantage of the quantum random sequences due to incomputability, it has motivated the improvement in [6], in which the problematic probability zero branch $S_x = 0$ in Figure 1.

The next 3D QRNG is presented in Figure 2. The unitary matrix U_x corresponding

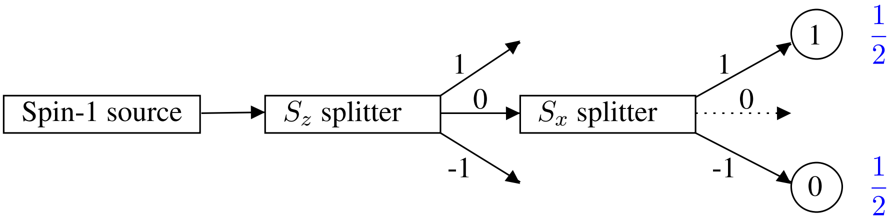

Figure 1: QRNG setup proposed in [1]; the values $\frac{1}{2}, \frac{1}{2}$ (in blue) correspond to the outcome probabilities

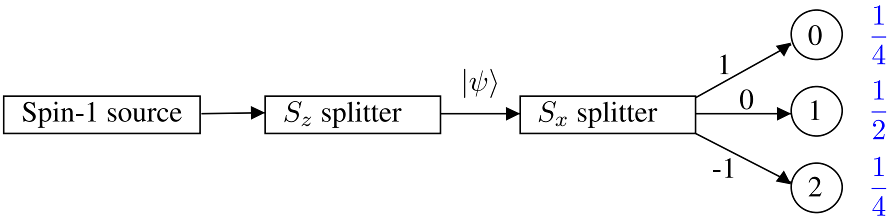

Figure 2: Blueprint for a new QRNG; the values $\frac{1}{4}, \frac{1}{2}, \frac{1}{4}$ (in blue) correspond to the outcome probabilities of setups prepared in the state $|\psi\rangle = |\pm 1\rangle$

to the spin state operator S_x is

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

As U_x can be decomposed into two-dimensional transformations [10]

$$U_x = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -i & 0 \\ 0 & 0 & -i \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} & 0 \\ i\sqrt{\frac{2}{3}} & -\frac{i}{\sqrt{3}} & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} \frac{\sqrt{3}}{2} & 0 & -\frac{i}{2} \\ 0 & 1 & 0 \\ \frac{i}{2} & 0 & -\frac{\sqrt{3}}{2} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & \sqrt{\frac{2}{3}} \\ 0 & i\sqrt{\frac{2}{3}} & -\frac{i}{\sqrt{3}} \end{pmatrix}.$$

a physical realisation of the unitary operator by a lossless beam splitter [28, 37] was obtained; the new outcome probabilities are 1/4,1/2,/1/4.

3 3D QRNG – Realization

4 Testing

4.1 Theory

A primality test is an algorithm for determining whether an input positive integer is prime. Primality is considered computationally *easy* because polynomial algorithms in the size of the input solve it; the first was in 2004 [5]. However, every primality polynomial algorithms is "practically slow", so probabilistic algorithms[1] are instead used [33]. In contrast, factorization of positive integers is thought, but not proved, to be a computationally *difficult* problem. Currently, one cannot factorize a positive integer of 500 decimal digits that is the product of two randomly chosen prime numbers. This fact is exploited in the RSA cryptosystem implementing public-key cryptography [29].

The practical failure of polynomial primality tests lead to probabilistic algorithms for primality [24, 26, 30, 31, 33, 33]. To check the primality of a positive integer n, the Solovay-Strassen test generates first k natural numbers uniformly distributed between 1 and $n-1$, inclusive, and, for each $i(=i_1,\ldots,i_k)$, checks the validity of the Solovay-Strassen predicate $W(i,n)$. If $W(i,n)$ is true then "i is a witness of n's compositeness"; in this case n is certainly composite. Otherwise, the test is inconclusive, but in this case the probability that n is prime is greater than $1-2^{-k}$. This results is based on the fact that *at least half* the i's between 1 and $n-1$ satisfy $W(i,n)$ if n is composite, and *none* of them satisfy $W(i,n)$ if n is prime [32].

Chaitin and Schwartz [9] showed that, if c is a large enough positive integer and s is a long enough c-Kolmogorov random binary string [8], then n is prime if and only if $Z(s,n)$ is true, where Z is a predicate constructed directly from $O(\log n)$ conjunctions of negations of W predicates. This result cannot be used to de-randomise Chaitin and Schwartz probabilistic algorithm because the set of c-Kolmogorov random strings is highly incomputable [8]. However, the result can be used to test the quality of long binary strings by comparing their "power" in the with that of c-Kolmogorov random strings of the same length. Following [2] we will test primality of Carmichael numbers which are composite positive integers n satisfying the congruence $b^{n-1} \equiv 1 \pmod{n}$ for all integers b relatively prime to n. A Carmichael number passes a Fermat primality test to every base relatively prime to the number, but few of them pass the Solovay-Strassen test. Increasingly Carmichael numbers become "rare".[2] Manuel: do we discuss only the fourth SSCS test?

[1] Currently the best runs in time O($(log\ n)^6$).

[2] There are 1,401,644 Carmichael numbers in the interval $[1, 10^{18}]$.

4.2 Experimental Results

To realise the protocols shown in Figs. 1,2 we use a superconducting quantum system, called a transmon [21]. The transmon has a weakly anharmonic multilevel structure [**?**], and its three lowest energy eigenstates $|0\rangle, |1\rangle$ and $|2\rangle$ can be used as the logical states of a qutrit.

To implement the protocol shown in Fig. 1 we follow the recipe from Ref. [21] where we mapped the eigenstates of the S_z operator to the states of the qutrit as follows

$$\{|z,-1\rangle, |z,0\rangle, |z,+1\rangle\} \to \{|2\rangle, |0\rangle, |1\rangle\}. \tag{2}$$

This mapping provide an advantage of preparing $|z, 0\rangle$ state by by cooling down the transmon to the base temperature of a dilution refrigerator ($\sim$ 20 mK).

To perform an arbitrary rotation of the qutrit quantum state $R_{\hat{n}}^{i,i+1}(\phi)$ we applied microwave pulses resonant to the $|0\rangle \leftrightarrow |1\rangle$ or $|1\rangle \leftrightarrow |2\rangle$ transition frequencies, respectively. Two rotations $R_y^{12}(\pi) \cdot R_y^{01}(\pi/2)$ of the state before the dispersive measurement were sued to engineer measurement in the eigenbasis of S_x. The resulting measurement outcomes of the transmon energy eigenstates could be mapped to the following outcomes of the measurement of S_x operator: $\{|0\rangle, |1\rangle, |2\rangle\} \to \{|x,+1\rangle, |x,-1\rangle, |x,0\rangle\}$.

To implement the protocol shown in Fig. 2 we used a slightly different encoding:

$$\{|z,-1\rangle, |z,0\rangle, |z,+1\rangle\} \to \{|1\rangle, |2\rangle, |0\rangle\}. \tag{3}$$

In this case, state $|z,+1\rangle$ was prepared by cooling of the transmon. The following measurement in the eigenbasis of S_x was engineered by the applying the same rotations $R_y^{01}(\pi/2) \cdot R_y^{12}(\pi/2)$ before the dispersive measurements. The measurement outcomes of the transmon would mapped to the following outcomes of the measurement of S_x operator: $\{|0\rangle, |1\rangle, |2\rangle\} \to \{|x,0\rangle, |x,-1\rangle, |x,+1\rangle\}$.

In order to measure the transmon, it was capacitively coupled to a co-planar waveguide resonator. The difference between the frequency of the resonator (f_r = 7.63 GHz) and the $|0\rangle \leftrightarrow |1\rangle$ (f_{01} = 5.49 GHz) and $|1\rangle \leftrightarrow |2\rangle$ (f_{12} = 5.16 GHz) transitions of the transmon were chosen to be much larger than the coupling between the two systems (f_r = 7.63 GHz). This allowed us to use the dispersive approximation, where the frequency of the resonator shifts by 0 MHz, 8.5 MHz or 15.5 MHz depending on whether the transmon is in the $|0\rangle$, $|1\rangle$ or $|2\rangle$ state [**?**]. The response of the resonator to a microwave pulse of frequency $f_r - 9$ MHz was classified using a convolutional neural network (CNN) as described in Ref. [**?**].

The procedure used to generate the random numbers required an initial calibration procedure typical of cQED setups. This involved calibration of f_r, f_{01} and the $R_y^{01}(\pi)$ and $R_y^{01}(\pi/2)$ pulses. Two $R_y^{01}(\pi/2)$ pulses were used to fine tune f_{01} using a Ramsey measurement. The $R_y^{01}(\pi)$ and $R_y^{01}(\pi/2)$ pulses were then fine tuned with repeated pulses. A similar procedure was followed to calibrate for f_{12} and the $R_y^{12}(\pi)$ and $R_y^{12}(\pi/2)$ pulses.

After initial calibration, we optimize the readout frequency and the Josephson parametric amplifier in order to perform single shot readout. The CNN is then trained for 50 training cycles using 1024 measurements of the readout resonator after preparing each of the three states, $|0\rangle$,$|1\rangle$ and $|2\rangle$ as described in Ref. [**?**].

The procedure so far involves repeated measurements where the transmon is reset to the $|0\rangle$ state by waiting 35 μs for it to reach thermal equilibrium (at a decay rate of 250 kHz). To increase the rate at which the transmon is reset to the $|0\rangle$ state, we use an active reset protocol described in Ref. [**?**, **?**]. This involves a *reset pulse* to transfer the $|2\rangle$ state population to the readout resonator and letting it decay much faster (at a decay rate of 4 MHz). An $R_y^{12}(\pi)$ pulse is then used to transfer the $|1\rangle$ state population to the $|2\rangle$ state, and the reset pulse is used again to transfer the $|2\rangle$ state population to the readout resonator. The $R_y^{12}(\pi)$ (40 ns), reset pulse (370 ns) and a wait time (50 ns) for the readout resonator to decay is used four times in series to ensure the transmon is in the ground state, taking 1.84 us in total. The reset protocol was tested using standard acquisition methods and the CNN to ensure the CNN was performing as intended. The reset time, the preparation pulses for the protocol and the measurement pulse time amounted to 3.2 us, corresponding to a trit rate of 312.5 kHz.

To ensure robust generation of 100 Gbit of random numbers, the procedure outlined in Algorithm 2. was followed, involving intermittent checks of the CNN without reset, retraining the CNN if necessary and re-calibrating the transmon as shown in Algorithm 1if that fails.

Algorithm 1 Calibration

```
procedure CALIBRATE        ▷ Calibrates the transmon preparation and readout
    $T_{\text{rep}} \leftarrow 40$ $\mu$s
    set measurement frequency to $f_r$
    set previously calibrated settings
    Ramsey frequency calibration for $f_{01}$
    Calibrate $R_y^{01}(\pi)$ and $R_y^{01}(\pi/2)$ pulses
    Ramsey frequency calibration for $f_{12}$
    Calibrate $R_y^{12}(\pi)$ and $R_y^{12}(\pi/2)$ pulses
    Calibrate reset pulse frequency
    set measurement frequency to $f_r - 9$ MHz
    Create convolutional neural network (CNN)
    Train CNN for 50 training cycles
end procedure
```

The microwave pulses used to prepare the transmon for measurements were cali

In the dispersive regime, where the cavity resonance frequency is sufficiently de-

Algorithm 2 Generation

```
procedure RunIndex
    if files exist then
        $r \leftarrow 1+$ last random_xxx.rbf file number
    else
        return $r \leftarrow 0$
    end if
    return $r$
end procedure
$T_{\text{rep}} \leftarrow 40\ \mu$s
Prepare $|0\rangle$,$|1\rangle$ and $|2\rangle$                ▷ Cyclically for each repetition
Create convolutional neural network (CNN)
Train CNN for 50 training cycles
$f \leftarrow$ measurement accuracy
                                      ▷ Assignment fidelity as defined in Ref. [?]
$c \leftarrow 0$                                 ▷ Calibration counter used to terminate
$l \leftarrow 0$                                  ▷ Low $f$ counter used to calibrate
$r \leftarrow$RunIndex
while r < 750 do
    while $f < 0.86$ do
        if $l > 20$ then
            if $c > 5$ then
                ERROR                         ▷ Calibrated 5 times already. Failed
            end if
            Calibrate
            $c \leftarrow c + 1$
            $l \leftarrow 0$
        end if
        $l \leftarrow l + 1$
        Train CNN for 20 more training cycles
        $f \leftarrow$ measurement accuracy
    end while
    $T_{\text{rep}} \leftarrow 3.2\ \mu$s
    Program protocol pulses
    Measure $2^{26}$ repetitions
    Store measurements in random_r.rbf
    $T_{\text{rep}} \leftarrow 40\ \mu$s
end while
On Error Log error and restart
```

tuned from the qutrit transition frequencies, the qutrit-cavity interaction causes cavity frequency shifts dependent on the populations of the energy eigenstates of the transmon [**?**]. These shifts, called dispersive shifts, are used for realizing dispersive readout of superconducting qubits and qutrits by measuring microwave transmission through the cavity (for a specific example of the measurement of a qutrit, see Ref. [**?**, **?**]).

To distinguish between three different transmon states with high fidelity we use a Josephson parametric amplifier. In addition, we set the readout pulse frequency close to the cavity frequency corresponding to the $|1\rangle$ state of the qutrit, which allowed the three possible qutrit states to be well separated on I-Q plane of the time-integrated signal detected via the heterodyne scheme. The readout frequency was fine-tuned to maximise the three-level readout fidelity.

Initialisation of the transmon in its ground state by waiting allowed a bit rate of 50 kbit/s [21]. To increase the bit rate we used an active reset protocol [**?**, **?**].

Short summary of the rest protocol. What pulses, how long it takes to reset.

Adding some words about NN with reference to our APL paper. Final description of the protocol: fidelities, time budgets and the final bitrate.

5 Conclusions

References

[1] 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.

[2] 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.

[3] A. A. Abbott, C. S. Calude, and K. Svozil. A quantum random number generator certified by value indefiniteness. *Mathematical Structures in Computer Science*, 24:e240303, 6 2014.

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

[5] M. Agrawal, N. Kayal, and N. Saxena. Primes is in P. *Annals of Mathematics*, 160:781–793, 2004.

[6] 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.

[7] L. Bienvenu, A. R. Day, and R. Hölzl. From bi-immunity to absolute undecidability. *J. Symbolic Logic*, 78(4):1218–1228, 12 2013.

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

[9] G. J. Chaitin and J. T. Schwartz. A note on Monte Carlo primality tests and algorithmic information theory. *Communications on Pure and Applied Mathematics*, 31(4):521–527, 1978.

[10] 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.

[11] 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.

[12] P. Frank. *Das Kausalgesetz und seine Grenzen*. Springer, Vienna, 1932.

[13] P. Frank and R. S. Cohen (Editor). *The Law of Causality and its Limits (Vienna Circle Collection)*. Springer, Vienna, 1997.

[14] W. Heisenberg. *Physics and Philosophy: The Revolution in Modern Science*. Harper, New York, 1958.

[15] ID Quantique SA. *QUANTIS. Quantum number generator*. idQuantique, Geneva, Switzerland, 2001-2022. accessed on Sep 8, 2019.

[16] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger. A fast and compact quantum random number generator. *Review of Scientific Instruments*, 71:1675–1680, 2000.

[17] S. Kochen and E. P. Specker. Logical structures arising in quantum theory. In *Symposium on the Theory of Models, Proceedings of the 1963 International Symposium at Berkeley*, pages 177–189, Amsterdam, 1965. North Holland.

[18] S. B. Kochen and E. Specker. The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics (now Indiana University Mathematics Journal)*, 17(1):59–87, 1967.

[19] K. W. F. Kohlrausch. *Der experimentelle Beweis für den statistischen Charakter des radioaktiven Zerfallsgesetzes*, pages 192–212. Springer, Berlin, Heidelberg, 1926.

[20] H. Kragh. Subatomic determinism and causal models of radioactive decay, 1903-1923. RePoSS: Research Publications on Science Studies 5. Department of Science Studies, University of Aarhus, November 2009.

[21] 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.

[22] F. London and E. Bauer. *La theorie de l'observation en mécanique quantique; No. 775 of Actualités scientifiques et industrielles: Exposés de physique générale, publiés sous la direction de Paul Langevin*. Hermann, Paris, 1939. English translation in [23].

[23] F. London and E. Bauer. The theory of observation in quantum mechanics. In J. A. Wheeler and W. H. Zurek, editors, *Quantum Theory and Measurement*, pages 217–259. Princeton University Press, Princeton, NJ, 1983. consolidated translation of French original [22].

[24] G. Miller. Riemann's hypothesis and tests for primality. *J. Comp. Syst. Sci.*, 13:300–317, 1976.

[25] 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.

[26] M. O. Rabin. Probabilistic algorithm for testing primality. *J. Number Th.*, 12,:128–138, 1980.

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

[28] 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.

[29] H. Riesel. *Classical Methods of Factorization*, pages 141–172. Birkhäuser Boston, Boston, MA, 2012.

[30] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 6(1):84–85, 1977.

[31] R. Solovay and V. Strassen. Erratum: A fast Monte-Carlo test for primality. *SIAM Journal on Computing*, 7(1):118, 1978.

[32] R. M. Solovay. On random r.e. sets. In A. I. Arruda, N. C. A. da Costa, and R. Chuaqui, editors, *Non-Classical Logics, Model Theory, and Computability*, pages 283–307. North-Holland, Amsterdam, 1977.

[33] A. Stiglic. *Probabilistic Primality Test*, pages 980–980. Springer US, Boston, MA, 2011.

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

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

[36] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger. Violation of Bell's inequality under strict Einstein locality conditions. *Physical Review Letters*, 81:5039–5043, 1998.

[37] B. Yurke, S. L. McCall, and J. R. Klauder. SU(2) and SU(1,1) interferometers. *Physical Review A*, 33:4033–4054, 1986.

[38] A. Zeilinger. A foundational principle for quantum mechanics. *Foundations of Physics*, 29(4):631–643, 1999.

[39] A. Zeilinger. The message of the quantum. *Nature*, 438:743, 2005.

[40] A. Zeilinger, G. Weihs, T. Jennewein, and M. Aspelmeyer. Happy centenary, photon. *Nature*, 433(7023):230–238, Jan. 2005.

[41] A. Zeilinger, G. Weihs, T. Jennewein, and M. Aspelmeyer. Erratum: Happy centenary, photon. *Nature*, 446(7133):342–342, Mar. 2007.