A Quantum Random Generator Certified by Kochen-Specker Theorem

Cristian S. Calude
University of Auckland, New Zealand

Joint work with A. A. Abbott, M. J. Dinneen, N. Huang, K. Svozil

Marie Curie FP7 Grant RANPHYS

4th Edition of *Romanian Cryptology Days*
Bucharest, September 2017

Random numbers are required for a variety of applications from secure communications to Monte-Carlo simulation.

There are many random number generators:

1. pseudo-random generators, software produced
   - PCG, Random123, xoroshilro128+
2. hardware generators, devices that generate random numbers from physical processes
   - macroscopic, e.g. coin, dice, roulette wheels, lottery machines,
   - microscopic, e.g. thermal noise, photoelectric effect, quantum effects.

In particular, there are many quantum random generators, from lab experiments to openly accessible on the internet and commercial (Quantis).

Why do we need another quantum random generator?

Because no current quantum random generator (QRNG) is provably better than the other generators, in particular, pseudo-random generators.

Is this so? Many advantages promised by QRNGs rely on the belief that the outcomes of quantum measurements are

intrinsically/irreducibly unpredictable.

This belief underlies:

- the use of QRNGs to produce "quantum random" sequences that are "truly unpredictable",
- the generation of cryptographic keys unpredictable to any adversary.

Is this belief reasonable?

Popper (1950), in arguing that unpredictability is indeterminism, defines prediction in terms of "physical predicting machines".

Wolpert (2008) formalised this notion much further in developing a general abstract model of physical inference.

A more modern and technical definition of unpredictability was given by Eagle (2005) in defining randomness as maximal unpredictability. But, does maximal unpredictability exist?

The first two models of predictability lack generality by requiring the predictor to be embedded in its environment; the third is relative to a particular physical theory.

Two forms of randomness

- Product randomness modelled as algorithmic randomness (algorithmic information theory)
  - true/perfect randomness **does not exist** (Ramsey theorem)
  - there are degrees of randomness (based on resources)
  - unpredictability is a requirement of randomness
- Process randomness
  - no mathematical formalisation
  - can be accessed/validated only with theory (e.g. quantum theory) and product randomness
- "...randomness is not in the world, it is in the interface between our theoretical descriptions and 'reality' as accessed by measurement. Randomness is unpredictability with respect to the intended theory and measurement." (G. Longo)

- Quantum randomness is
  - postulated and
  - generally reduced to the indeterminism of quantum measurements: because the outcome is indeterministic there is no way to predict it, hence it is random

- However, indeterminism does not imply randomness and randomness does not imply indeterminism:
  - pseudo-randomness
  - coin-tossing (chaoticity)
  - Omega number
  - Schrödinger equation

Value definiteness

For a given quantum system in a particular state, we say that an observable is value definite if the measurement of that observable is predetermined to take a (potentially hidden) value.

If no such predetermined value exists, the observable is value indefinite.

Value definiteness (cont.)

In addressing the question of when we should conclude that a physical quantity is value definite, Einstein, Podolsky and Rosen (EPR) gave *a sufficient criterion of physical reality* which we adopt as:

> **EPR principle**: *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.*

EPR principle justifies also

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

A *context* in $\mathbb{C}^n$ is a maximal set of n compatible (commuting) observables. In Hilbert space contexts can be identified with orthonormal bases.

Value assignment are partial functions $v : \mathcal{O} \to \{0, 1\}$: $v(P)$ is undefined if P is value indefinite.

Kochen-Specker Theorem. *In a Hilbert space of dimension at least* 3 *there is a finite set of (projection) observables* $\mathcal{O}$ *such that no value assignment function* $v : \mathcal{O} \to \{0, 1\}$ *can have the following three properties:*

1. *Value definiteness* (VD)*:* v *is total, i.e.* $v(P)$ *is defined for all* $P \in \mathcal{O}$*.*
2. *Noncontextuality* (NC)*:* v *is a function of* P *only.*
3. *Satisfy quantum mechanical predictions* (QM)*: For every context* $C \subset \mathcal{O}$*:* $\sum_{P \in C} v(P) = 1$*.*

Possible choices

We may reject:

- QM (but then we depart from quantum theory), or
- NC (definite values depend on measurement context), or
- VD (some observables are value indefinite).

A (rather accepted) option is to assume QM and NC and adopt value indefiniteness as a model of quantum indeterminism.

In this case Kochen-Specker theorem says that *some* observables are *value indefinite*, hence *some* quantum measurements are indeterminate.

Theorem 1. [Abbott, Calude, Conder, Svozil (2012)] *Assume the EPR and Eigenstate principles.*
Consider a quantum system prepared in the state $|\psi\rangle$ *in dimension* $n \geq 3$ *Hilbert space* $\mathbb{C}^n$*, and let* $|\phi\rangle$ *be any state neither orthogonal nor parallel to* $|\psi\rangle$*.*
Then the projection observable $P_\phi = |\phi\rangle\langle\phi|$ *is value indefinite under any non-contextual value assignment satisfying* QM*.*

Accepting that definite values *exist* for certain observables (Eigenstate principle) and behave non-contextually (EPR principle) is enough to locate and *derive rather than postulate* quantum value indefiniteness. In fact, value definite observables are not the norm, they are the exception:

Theorem 2. [Abbott, Calude, Svozil (2014) (2015) – 2] The set of value indefinite observables has constructive measure 1.

Under the adopted interpretation:

- Kochen-Specker theorem shows that quantum-mechanics is indeterministic.
- **Theorems 1 and 2**
  - indicate precisely which observables are value indefinite and
  - the extent of this indeterminism.

We are ready to ask the main question:

Are quantum mechanical measurements unpredictable?

A non-probabilistic model of prediction based on the ability of a computable operating agent to correctly predict using finite information extracted from the system of the specified experiment was developed in Abbott, Calude, Svozil (2015).

Predictions should remain correct in any arbitrarily long (but finite) set of repetitions of the experiment.

We consider an experiment E producing a single bit $x \in \{0, 1\}$; with a particular trial of E we associate the parameter λ (the state of the universe) which fully describes the trial. We can view λ as a resource that one can extract finite information from in order to predict the outcome of the experiment E.

An extractor is a physical device selecting a finite amount of information from λ without altering the experiment E. Mathematically, the extractor produces a finite string of bits $\xi(\lambda)$.

A predictor for E is an algorithm P_E which halts on every input and outputs **0** or **1** or **prediction withheld**.

P_E can use as input the information $\xi(\lambda)$, but must be passive, that is, it must not disturb or interact with E in any way.

Consider an experiment E performed in dimension $n \geq 3$ Hilbert space in which a quantum system is prepared in a state $|\psi\rangle$ and a value indefinite observable P_ϕ is measured producing a single bit x.

Assume the EPR and Eigenstate principles.

Theorem 3. [Abbott, Calude, Svozil (2015) – 1] *If E is an experiment measuring a quantum value indefinite observable, then for every predictor P_E using any extractor ξ, P_E is not correct for ξ.*

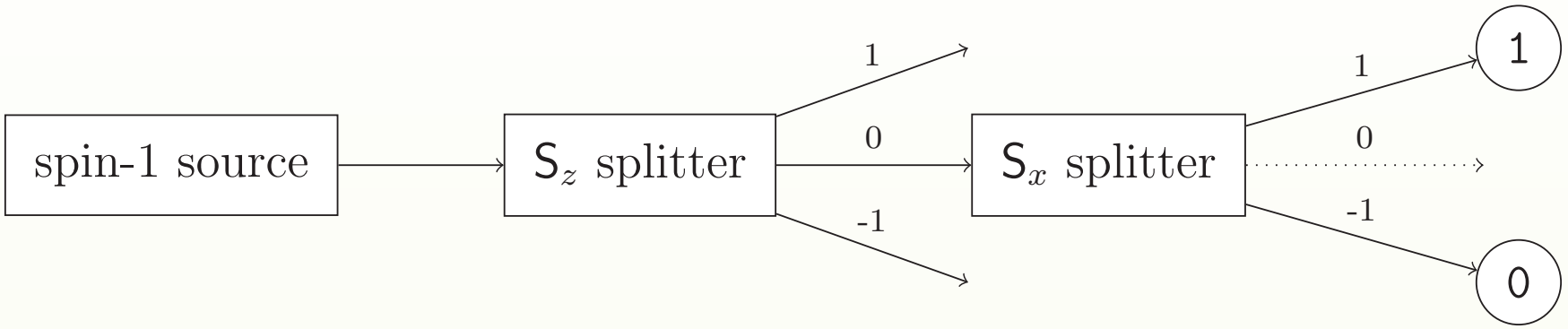
Theorem 4. [Abbott, Calude, Svozil (2015) – 1] *In an infinite repetition of the experiment E measuring a quantum value indefinite observable which generates the infinite sequence $x_1 x_2 \ldots$, no single bit x_i can be predicted.*

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

Theorem 5. [Abbott, Calude, Conder, Svozil (2012)] *Assume epr principle. An infinite repetition of the experiment E measuring a quantum value indefinite observable generates a bi-immune infinite sequence $x_1 x_2 \ldots$.*

Theorem 4 does not imply **Theorem 5**.

Spin-1 QRNG

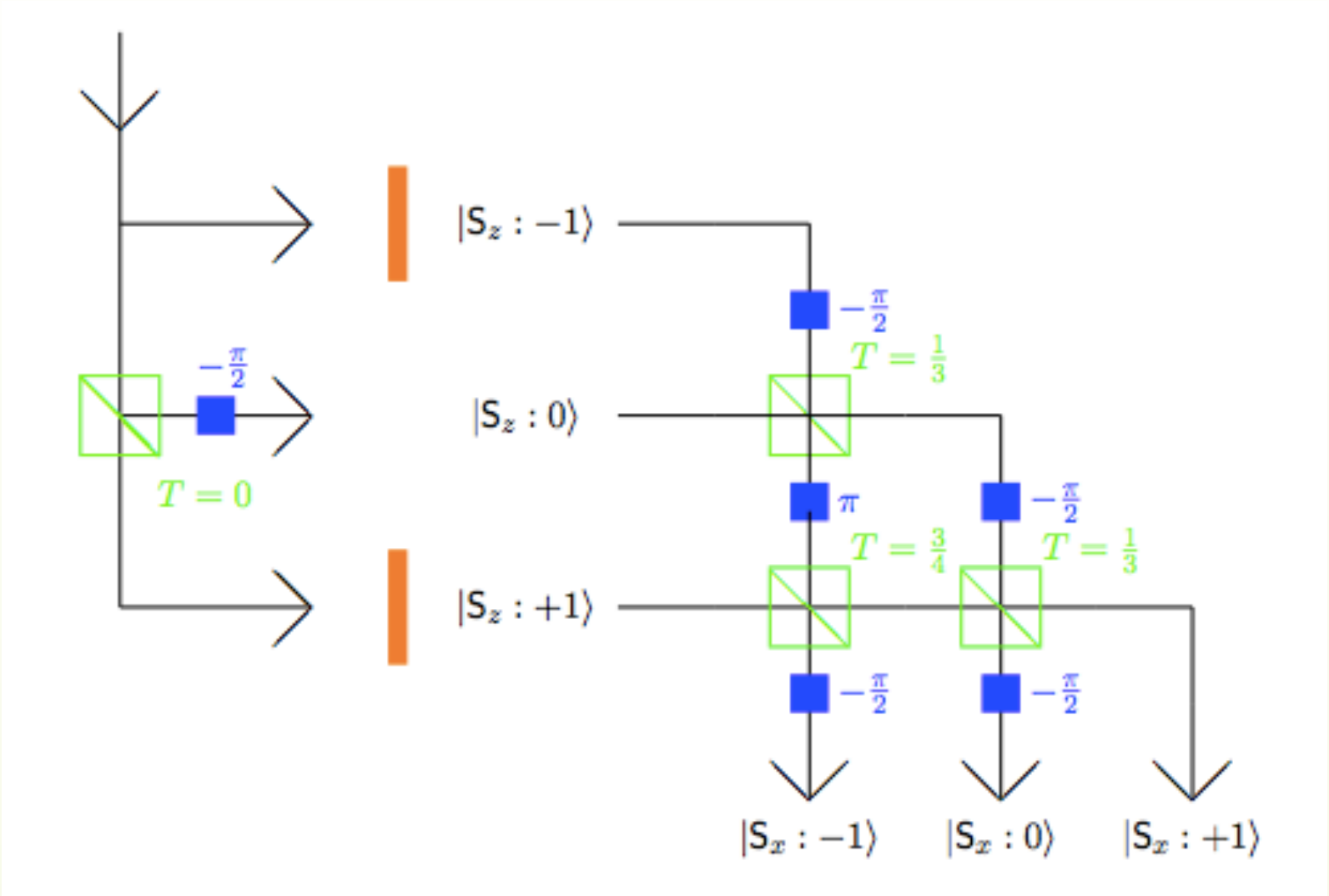


Spin-1 particles are prepared in the $S_z = 0$ state (this operator has a definite value), and then the S_x operator is measured. Since the preparation state is an eigenstate of the $S_x = 0$ projector with eigenvalue 0, this outcome has a definite value and cannot be obtained.

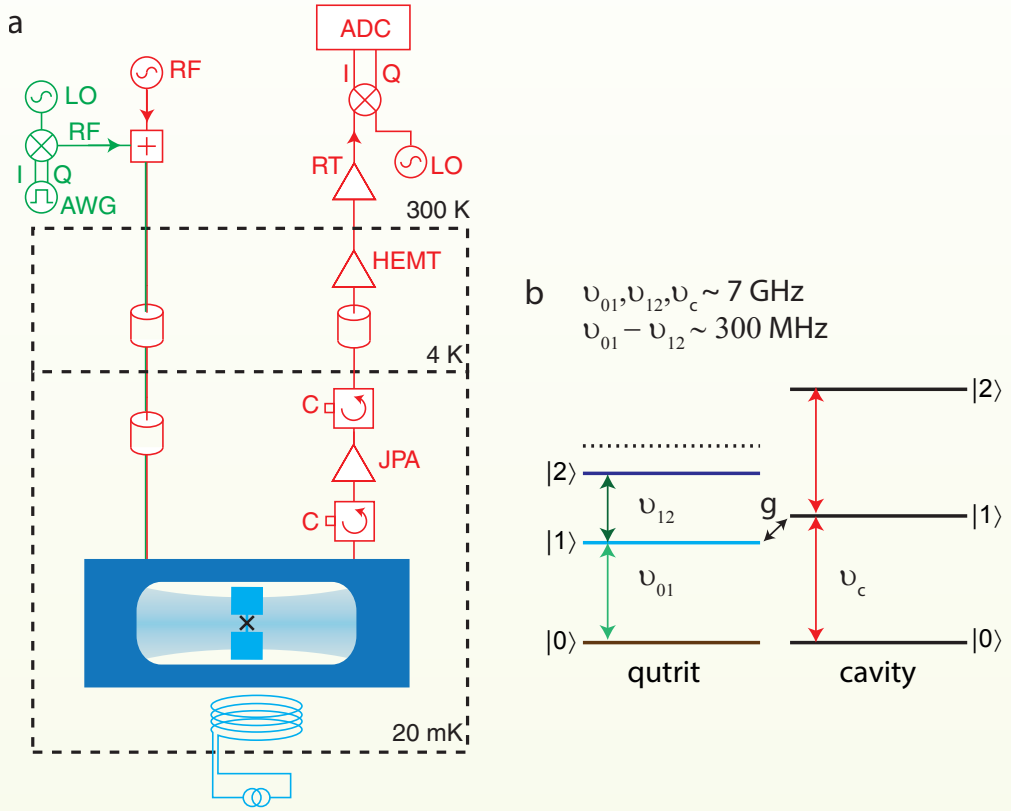
Thus, while the setup uses spin-1 particles, the outcomes are dichotomic and the $S_x = \pm 1$ outcomes can be assigned 0 and 1 respectively.

Furthermore, since $\langle S_z = 0 | S_x = \pm 1 \rangle = 1/\sqrt{2}$, neither of the $S_x = \pm 1$ outcomes can have pre-assigned definite value.

3D QRNG producing bi-immune sequences

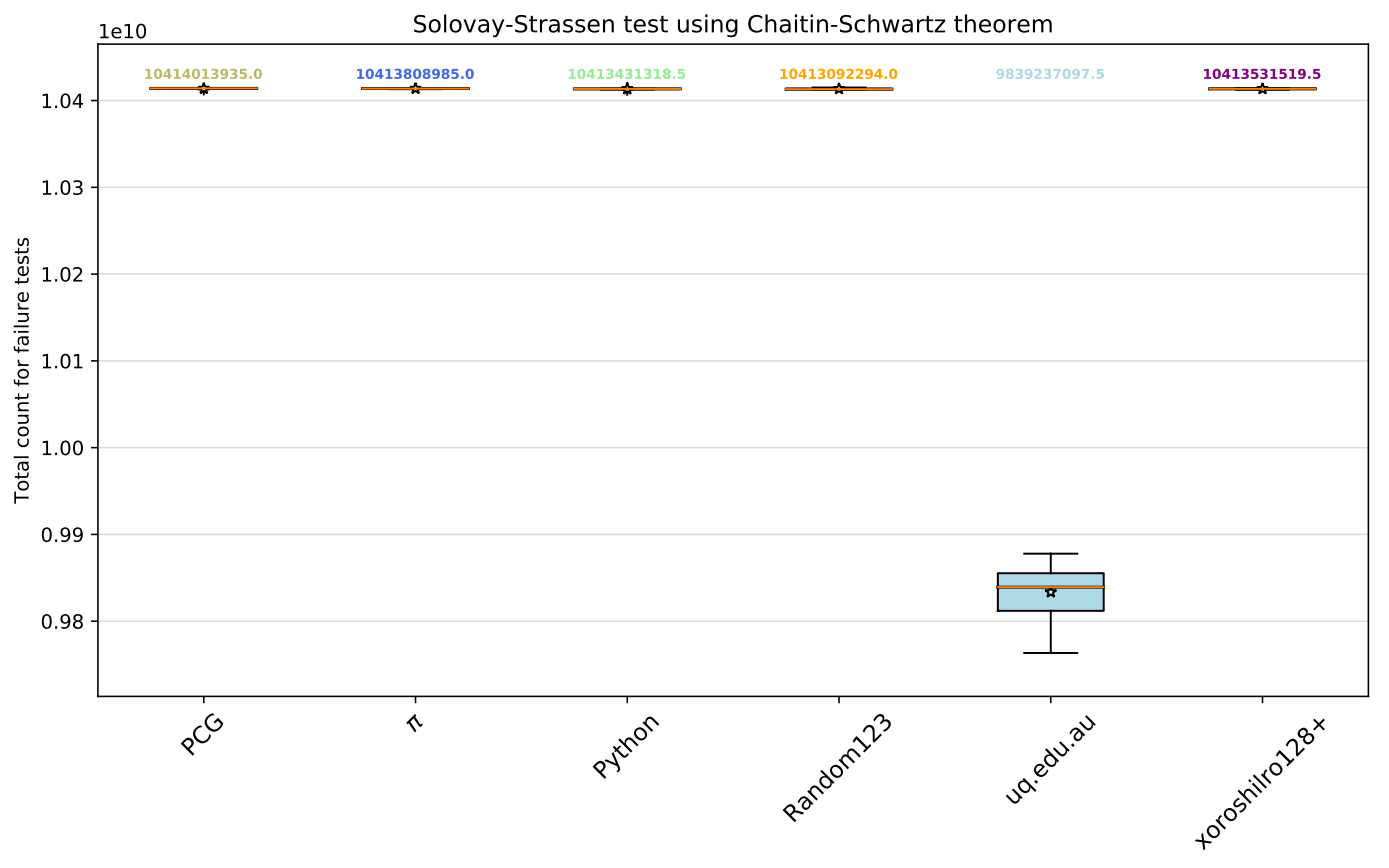


Realisation of a 3D QRNG



Transmon, super-conducting quantum system coupled to a microwave cavity. Kulikov, M. Jerger, A. Fedorov (2017)

Experimental evidence of incomputability of the 3D QRNG



A comparative analysis of 10 samples of strings length 2^{29} obtained with Transmon, π, and four of the best pseudo-random generators.

References

- A. Einstein, B. Podolsky and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review* 47, 10 (1935), 777–780.
- S. Kochen and E. Specker. The problem of hidden variables in quantum mechanics, *Journal of Mathematics and Mechanics* 17 (1967), 59–87.
- A. A. Abbott, C. S. Calude, J. Conder and K. Svozil. Strong Kochen-Specker theorem and incomputability of quantum randomness, *Physical Review A* 86, 6 (2012), PhysRevA.86.062109.
- A. A. Abbott, C. S. Calude and K. Svozil. Value-indefinite observables are almost everywhere, *Physical Review A*, 89, 3 (2014), 032109–032116, PhysRevA.89.032109.

References (cont.)

- A. A. Abbott, C. S. Calude and K. Svozil. On the unpredictability of individual quantum measurement outcomes, in L. D. Beklemishev, A. Blass, N. Dershowitz, B. Finkbeiner, W. Schulte (eds.). *Fields of Logic and Computation II*, LNCS 9300, Springer, 2015, 69–86.
- A. A. Abbott, C. S. Calude and K. Svozil. A variant of the Kochen-Specker theorem localising value indefiniteness, *Journal of Mathematical Physics* 56 (2015); JMP2015.
- A. Abbott, C. S. Calude, K. Svozil. A non-probabilistic model of relativised predictability in physics, *Information* 6, (2015), 773–789.
- A. Kulikov, M. Jerger, A. Fedorov. Realization of a quantum random generator certified with the Kochen-Specker theorem, 2017, `https://arxiv.org/pdf/1709.03687.pdf`.