CDMTCS
Research
Report
Series

Quantum Randomness: From Practice to Theory and Back

C. S. Calude
University of Auckland, NZ

CDMTCS-442
September 2013

Centre for Discrete Mathematics and
Theoretical Computer Science

Quantum Randomness: From Practice to Theory and Back

Cristian S. Calude
Department of Computer Science, University of Auckland,
Private Bag 92019, Auckland, New Zealand
www.cs.auckland.ac.nz/~cristian

> *Phenomena that we cannot predict must be judged random.*
> P. Suppes

1 "Babylon is nothing but an infinite game of chance"

A mythical Babylon in which everything is dictated by an *universal lottery* is sketched in *The Lottery in Babylon* [4], a short story published in 1941 (first English translation in 1962) by Jorge Luis Borges. A normally operated lottery—with tickets, winners, losers, and money rewards—starts adding punishments to rewards and finally evolves into an all-encompassing "Company" whose decisions are mandatory for all but a small elite. The Company acts at random and in secrecy. Most Babylonians have two only options: to accept the all-knowing, all-powerful, but mysterious Company, or to deny its very existence (no such Company). While various possible philosophical interpretations of the story have been discussed, there is a large consensus that the Company symbolises the power and pervasiveness of *randomness.* Indeed, randomness is the very stuff of life, impinging on everything, fortunes and misfortunes, from the beginning to end. It causes fear and anxiety, but also fun and, most interestingly, it provides efficient tools used since Ancient Athens.

2 A case study: security

It is difficult to deny that security is one of the key issue of our time. Here is an example related to NSA scandal (June 2013)[1] presented in [13]. The CNN report, significantly sub-titled "Tapping the strange science of quantum mechanics, physicists are creating new data security protocols that even the NSA can't crack", starts with ... Snowden.

[1] Borges names "Qaphqa", an obvious code for Kafka, the "sacred latrine" allowing access to the Company.

> The news out of Moscow of late has been dominated by Edward Snowden, the American leaker of secret state documents who is currently seeking temporary asylum in Russia. Meanwhile, across town and to much less fanfare, Dr. Nicolas Gisin found himself explaining last week the solution to the very problems of data security and privacy intrusion Snowden brought to light in exposing the vast reach of the National Security Agency's data collection tools: *data encryption that is unbreakable now and will remain unbreakable in the future.*[2]

According to Wikipedia, "Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries)". A cryptosystem is a suite of algorithms used to implement a particular form of encryption and decryption. Modern cryptography is dominated by three main approaches: (a) the information theoretical approach in which the adversary should have not enough information to break a cryptosystem, (b) the complexity theoretical approach in which the adversary should have not enough computational power to break a cryptosystem and (c) the quantum physics approach in which the adversary would need to break some physical laws to break a cryptosystem. The third approach is called quantum cryptography; by contrast, the first two approaches are referred to as classical cryptography.

Cryptographic algorithms require a method of generating a secret key from "random" bits. The encryption algorithm uses the key to encrypt and decrypt messages, which are sent over unsecured communication channels. The strength of the system ultimately depends on the strength of the key used, i.e. on the difficulty for an eavesdropper to guess or calculate it. Vulnerabilities of classical cryptography are well documented, but quantum cryptography was (and, as we will see below, continues to be) believed to be unbreakable: Heisenberg's Uncertainty Principle guarantees that an adversary cannot look into the series photons which transmit the key without either changing or destroying them. The difference between classical and quantum cryptography rests on keys: classical keys are vulnerable, but keys formed with quantum random bits have been claimed to be unbreakable because *quantum randomness is true randomness* (see [25]). In the words from [13]:

> "It sounds like there's some quantum magic in this new technology, but of course it's not magic, it's just very modern science", Gisin says. But next to classical communication and encryption methods, it might as well be magic. Classical cryptography generally relies on algorithms to randomly generate encryption and decryption keys enabling the sender to essentially scramble a message and a receiver to unscramble it at the other end. If a third-party ... obtains a copy of the key, that person can make a copy of the transmission and decipher it, or—with enough time and computing power—use powerful algorithms to break the decryption key. (This is what the NSA and other agencies around

[2] My Italics.

> the world are allegedly up to.) But Gisin's quantum magic taps some of the stranger known phenomena of the quantum world to transmit encryption keys that cannot be copied, stolen, or broken without rendering the key useless.
>
> The primary quantum tool at work in ID Quantique's quantum communication scheme is known as "entanglement", a phenomena in which two particles—in this case individual photons—are placed in a correlated state. Under the rules of quantum mechanics, these two entangled photons are inextricably linked; a change to the state of one photon will affect the state of the other, regardless of whether they are right next to each other, in different rooms, or on opposite sides of the planet. One of these entangled photons is sent from sender to receiver, so each possesses a photon. These photons are not encoded with any useful information—that information is encoded using normal classical encryption methods—but with a decryption key created by a random number generator. (*True random number*[3] generators represent another technology enabled by quantum physics—more on that in a moment.)

The above quote contains errors and misleading statements, but we reproduce it here as it is illustrative of the way quantum cryptography is presented to the public. Really, how good is this technology?

Gruska [20] offers a cautious answer from a theoretical point of view:

> Goals of quantum cryptography have been very ambitious. Indeed, some protocols of quantum cryptography provably achieve so-called unconditional secrecy, a synonym for absolute secrecy, also in the presence of eavesdroppers endowed with unlimited computational power and limited only by the laws of nature, or even only by foreseeable laws of nature not contradicting the non-signaling principle of relativity.

An answer from a practical point of view appears in [13]:

> "Security experts didn't learn anything from this Snowden story, it was already obvious that it is so easy to monitor all the information passing through the Internet", Gisin says. "No security expert can pretend to be surprised by his revelation. And I'm not a national security expert, but I don't think the Americans are the only ones who are doing this—the Russians are doing it, the Chinese are doing it, everybody is spying on the others and that's always been the case and it always will be. One way to be a step ahead of the others is to use quantum cryptography, because *for sure the programs that the Americans and others are using will not be able to crack it.*[4]

[3] My Italics.

[4] My Italics.

3 True randomness

The "magic" of the quantum technology capable of producing unbreakable security depends on the possibility of producing *true random* bits. What does it mean "true randomness"[5]? The concept is not formally defined, but a common meaning is the *lack of any possible correlations.* Is this indeed theoretically possible? The answer is *negative*: *there is no true randomness, irrespective of the method used to produce it.* The British mathematician and logician Frank P. Ramsey was the first to demonstrate it in his study of *conditions under which order must appear* (see [19, 26]); other proofs have been given in the framework of algorithmic information theory [5].

We will illustrate Ramsey's theory later in this section. For now, let's ask a more pragmatical question: Are these mathematical results relevant for the theory or practice of quantum cryptography? Poor quality randomness is, among other issues, the cause of various failures of quantum cryptographic systems. After a natural euphoria period when quantum cryptography was genuinely considered to be "unbreakable" scientists started to exercise one of the most important attitudes in science: skepticism. And, indeed, weaknesses of quantum cryptography have been discovered; they are not new and they are not a few in number. Issues have been found as early as 2008 [9], even earlier. In 2010, V. Makarov and his colleagues published the details of a traceless attack against a class of quantum cryptographic systems [23] which includes the products commercialised by ID Quantique[6] (Geneva) [28] and MagiQ Technologies (Boston) [29]: both companies claim to produce *true randomness.* Recent critical weaknesses of a new class of quantum cryptographic schemes called "device-independent" protocols—that rely on public communication between secure laboratories—are described in [3].

Geneva is only 280 kms from Zurich, but the views on quantum cryptography of ID Quantique and physicist R. Renner, from the Institute of Theoretical Physics in Zurich, are quite different. Recognising the weaknesses of quantum cryptography, R. Renner has embarked in a program to evaluate the failure rate of different quantum cryptography systems. He was quoted in [30]:

> *The security of Quantum Key Distribution systems is never absolute.*

Renner's work was presented at the "2013 Conference on Lasers and Electro-Optics" (San Jose, California, USA, [27]). Not surprisingly, even before presenting his invited lecture on June 11, Renner's main findings made the news: [12, 24] are two examples. Commenting on "timeslicing" BB84 protocol, K. Svozil, cited in [21], said: "The newly proposed [quantum] protocol is 'breakable' by middlemen attacks" in the same way as BB84: "complete secrecy" is an illusion.

[5] Also called perfect randomness.

[6] Featured in Section 2.

Why would some physicists claim that quantum randomness is *true randomness*? According to ID Quantique website [28]

> Existing randomness sources can be grouped in two classes: software solutions, which can only generate pseudo-random bit streams, and physical sources. In the latter, most random generators rely on classical physics to produce what looks like a random stream of bits. In reality, determinism is hidden behind complexity. Contrary to classical physics, quantum physics is fundamentally random. It is the only theory within the fabric of modern physics that integrates randomness.

Certainly, this statement is not a proper scientific justification. Randomness in quantum mechanics comes from measurement, which is part of the interpretation of quantum mechanics. To start with we need to assume that measurement yields a physically meaningful and unique result. This may seem rather self-evident, but it is not true of interpretations of quantum mechanics such as the many-worlds, where measurement is just a process by which the apparatus or experimenter becomes entangled with the state being "measured"; in such an interpretation it does not make sense to talk about the unique "result" of a measurement.

If the only basis for claiming that quantum randomness is better than pseudo-randomness is the fact that the first is true randomness, then the claim is very weak. After all, experimentally, both types of randomness are far from being perfect [7].

Our short analysis shows that we need much more understanding of randomness to be able to say something non-trivial about quantum randomness. Interestingly, Ramsey theory provides arguments for the impossibility of true randomness resting on the sole fact that any model of randomness has to satisfy the common intuition that "randomness means no correlations, no patterns". The question becomes:

> *Are there binary (finite) strings or (infinite) sequences with* no *patterns/correlations?*

Ramsey theory answers in the negative the above question; measure-theoretical arguments have been also found in algorithmic information theory [5]. Here is an illustration of the Ramsey-type argument.

Let $s_1 \cdots s_n$ be a binary string. A monochromatic arithmetic progression of length k is a substring $s_i s_{i+t} s_{i+2t} \cdots s_{i+(k-1)t}, 1 \leq i \leq i + (k-1)t \leq n$ with all characters equal (0 or 1) for some $t > 0$. The theorem below states that *all* sufficiently long binary strings have "long enough" monochromatic arithmetic progressions. The importance of the theorem lies in the fact that *all* strings display one of the simplest type of correlation:

> **Van der Waerden finite theorem.** *For every natural k there is a natural $n > k$ such that every string of length n contains a monochromatic arithmetic progression of length k.*

The Van der Waerden number $W(k)$ is smallest n such that every string of length n contains a monochromatic arithmetic progression of length k. For example, $W(3)$=9. The string 01100110 contains no arithmetic progression of length 3 because the positions 1,4,5,8 (for 0) and 2,3,6,7 (for 1) do not contain three terms of an arithmetic progression, hence $W(3) > 8$. However, both strings 011001100, 011001101 do: 1,5,9 for 0 and 3,6,9 for 1, and a brute force test shows that every string of length 9 contains three terms of a monochromatic arithmetic progression, so $W(3)$=9.

How long should be a string to display a monochromatic arithmetic progression, i.e. how big is $W(k)$? In [17] it was proved that $W(k) < 2^{2^{2^{2^{2^{k+9}}}}}$, but conjectured to be much smaller in [18]: $W(k) < 2^{k^2}$.

Van der Waerden result is true for infinite binary sequences as well:

> **Van der Waerden infinite theorem.** *Every infinite binary sequence contains arbitrarily long monochromatic arithmetic progressions.*

This is one of the many results in Ramsey theory [26]. Graham and Spencer, well-known experts in this field, subtitled their *Scientific American* presentation of Ramsey Theory [19] with a sentence similar in spirit to Renner's one (quoted above):

> *Complete disorder is an impossibility. Every large set of numbers, points or objects necessarily contains a highly regular pattern.*

The adjective "large" applies to both finite and infinite sets.[7] The simplest finite example is *the pigeonhole principle*: A set of N objects is partitioned into n classes. Here "large" means $N > n$. Conclusion: a class contains at least two objects. Example: "Of three ordinary people, two must have the same sex" (D. J. Kleitmen). *The infinite pigeonhole principle*: A set of objects is partitioned into finitely many classes. Here "large" means that the set is infinite while the number of classes which finite. Conclusion: a class is infinite.

Randomness comes from different sources and means different things in various fields. Algorithmic information theory [5, 14] is a mathematical theory in which, in contrast to probability theory, the randomness of individual objects is studied. Given the impossibility of true randomness, the effort is directed towards studying degrees of randomness. The main point of algorithmic information theory (a point emphasied from a philosophical point of view in [15]) is:

> *Randomness means unpredictability with respect to some fixed theory.*

[7] We identify a binary finite string and an infinite sequence with sets of positive integers.

The quality of a particular type of randomness depends on the power of the theory to detect correlations, which determines how difficult is predictability. For example, finite automata detect less correlations than Turing machines. Consequently, finite automata based unpredictability is weaker than Turing machine based unpredictability: there are (many) sequences computable by Turing machines (hence, predictable, not random) that are unpredictable, random, for finite automata.

In analogy with the notion of incomputability, see [10], one can prove that there is a never ending hierarchy of stronger (better quality) and stronger forms of randomness.

4 Is quantum randomness "better" than pseudo-randomness?

The intuition confirmed by experimental results reported in [7] suggests that the quality of quantum randomness is *better* than that of pseudo-randomness. Is there any solid basis to compare quantum randomness and pseudo-randomness?

Although in practice only finitely many bits are necessary, to be able to evaluate and compare the quality of randomness we need to consider infinite sequences of bits. In [6, 8, 2, 1] the first steps in this direction have been made.

Pseudo-random sequences are obviously Turing computable (i.e. they are produced by an algorithm); they are easily predictable once we know the seed and the algorithm generating the sequence, so, not surprisingly, their quality of randomness is low. Is quantum randomness Turing computable?

How can one prove such a result? As we have already observed in the previous section, we need to make some physical assumptions to base our mathematical reasoning on. To present these assumptions we need a few notions specific to quantum mechanics; we will adopt them in the form presented in [1].

In what follows we only consider pure quantum states. Projection operators—projecting on to the linear subspace spanned by a non-zero vector $|\psi\rangle$—will be denoted by $P_\psi = \frac{|\psi\rangle\langle\psi|}{\langle\psi|\psi\rangle}$.

We fix a positive integer n. Let $\mathcal{O} \subseteq \{P_\psi \mid |\psi\rangle \in \mathbb{C}^n\}$ be a non-empty set of *projection observables* in the Hilbert space $\mathbb{C}^n$ and $\mathcal{C} \subseteq \{\{P_1, P_2, \ldots P_n\} \mid P_i \in \mathcal{O}$ and $\langle i|j\rangle = 0$ for $i \neq j\}$ a set of measurement contexts over $\mathcal{O}$. A *context* $C \in \mathcal{C}$ is thus a maximal set of compatible (i.e. they can be simultaneous measured) projection observables. Let $v : \{(o, C) \mid o \in \mathcal{O}, C \in \mathcal{C}$ and $o \in C\} \overset{o}{\to} B$ be a partial function (i.e., it may be undefined for some values in its domain) called *assignment function*. For some $o, o' \in \mathcal{O}$ and $C, C' \in \mathcal{C}$ we say $v(o, C) = v(o', C')$ if $v(o, C), v(o', C')$ are both defined and have equal values.

Value definiteness corresponds to the notion of predictability in classical determinism: an observable is value definite if v assigns it a definite value—i.e. is able to predict in advance, independently of measurement, the value obtained via measurement. Here is the formal definition: an observable $o \in C$ is *value definite* in the context C under v if $v(o, C)$

is defined; otherwise o is *value indefinite* in C. If o is value definite in all contexts $C \in \mathcal{C}$ for which $o \in C$ then we simply say that o is value definite under v. The set $\mathcal{O}$ is *value definite* under v if every observable $o \in \mathcal{O}$ is value definite under v.

Non-contextuality corresponds to the classical notion that the value obtained via measurement is independent of other compatible observables measured alongside it. Formally, an observable $o \in \mathcal{O}$ is *non-contextual* under v if for all contexts $C, C' \in \mathcal{C}$ with $o \in C, C'$ we have $v(o, C) = v(o, C')$; otherwise, v is *contextual.* The set of observables $\mathcal{O}$ is *non-contextual* under v if every observable $o \in \mathcal{O}$ which is not value indefinite (i.e. value definite in *some* context) is non-contextual under v; otherwise, the set of observables $\mathcal{O}$ is *contextual.*

To be in agreement with quantum mechanics we restrict the assignment functions to admissible ones: v is *admissible* if the following hold for all $C \in \mathcal{C}$: a) if there exists an $o \in C$ with $v(o, C) = 1$, then $v(o', C) = 0$ for all $o' \in C \setminus \{o\}$, b) if there exists an $o \in C$ such that $v(o', C) = 0$ for all $o' \in C \setminus \{o\}$, then $v(o, C) = 1$.

We are now ready to list the physical assumptions. A *value indefinite quantum experiment* is an experiment in which a particular value indefinite observable in a standard (von Neumann type) quantum mechanics is measured, subject to the following assumptions **(A1)**–**(A5)** (for a detailed motivation we refer to [1]).

We exclude interpretations of quantum mechanics, such as the many-worlds interpretation, where there is no unique "result" of a measurement.

> **(A1) Measurement assumption.** *Measurement yields a physically meaningful and unique result.*

We restrict the set of assignments to those which agree with quantum mechanics.

> **(A2) Assignment assumption.** *The assignment function v is a* faithful *representation of a realisation r_ψ of a state $|\psi\rangle$, that is, the measurement of observable o in the context C on the physical state r_ψ yields the result $v(o, C)$ whenever o has a definite value under v.*

We assume a classical-like behaviour of measurement: the values of variables are intrinsic and independent of the device used to measure them.

> **(A3) Non-contextuality assumption.** *The set of observables $\mathcal{O}$ is non-contextual.*

The following assumption reflects another agreement with quantum mechanics.

> **(A4) Eigenstate assumption.** *For every (normalised) quantum state $|\psi\rangle$ and faithful assignment function v, we have $v(P_\psi, C) = 1$ and $v(P_\phi, C) = 0$, for any context $C \in \mathcal{C}$, with $P_\psi, P_\phi \in C$.*

The motivation for the next assumption comes from the notion of “element of physical reality” described by Einstein, Podolsky and Rosen in [16, p. 777]:

> *If, without in any way disturbing a system, we can predict with certainty (i.e., with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality* [8] [(*e.p.r.*)] *corresponding to this physical quantity.*

The last assumption is a weak form of e.p.r. in which *prediction is certain* (not only with probability one) and, *given by some function which can be proved to be computable.*

> **(A5) Elements of physical reality (e.p.r.) assumption.** *If there exists a computable function* $f : \mathbf{N} \times \mathcal{O} \times \mathcal{C} \to B$ *such that for infinitely many* $i \geq 1$, $f(i, o_i, C_i) = x_i$, *then there is a definite value associated with* o_i *at each step* [i.e., $v_i(o_i, C_i) = f(i, o_i, C_i)$].

To use the e.p.r. assumption we need *to prove* the existence of a computable function f such that for infinitely many $i \geq 1$, $f(i, o_i, C_i) = x_i$.

Can projection observables be value definite and non-contextual? The following theorem answers this question in the negative.

> **Kochen-Specker theorem**. *In a Hilbert space of dimension* $n > 2$ *there exists a set of projection observables* $\mathcal{O}$ *on* $\mathbb{C}^n$ *and a set of contexts over* $\mathcal{O}$ *such that there is no admissible assignment function* v *under which* $\mathcal{O}$ *is both non-contextual and value definite.*

Kochen-Specker theorem [22]—proved 46 years ago—is a famous result showing a contradiction between two basic assumptions of a hypothetical hidden variable theory intended to reproduce the results of quantum mechanics: a) all hidden variables corresponding to quantum mechanical observables have definite values at any given time, and b) the values of those variables are intrinsic and independent of the device used to measure them. The result is important in the debate on the (in)completeness of quantum mechanics creating by the EPR paradox [16].

Interestingly, the theorem, that is considered a topic in the foundations of quantum mechanics, with more philosophical flavour and little presence in main stream quantum mechanical textbooks, has actually an *operational*importance. Indeed, using the assumption **(A3)**, the Kochen-Specker theorem states that some projection observables have to be value indefinite.

Why should we care about a value indefinite observable? Because a way “to see” the randomness in quantum mechanics is by measuring such an observable. Of course, we need

[8] An element of physical reality corresponds to the notion of a definite value, possibly contextual.

to be able to *certify* that a given observable is value indefinite. Unfortunately the theorem gives no indication which observables are value indefinite. We know that not all projection observables are value indefinite [1], but can we be sure that a specific observable is value indefinite observable? The following result from [1] answers this question in the affirmative:

> **Strong Kochen-Specker theorem**. *Let $|a\rangle, |b\rangle \in \mathbb{C}^3$ be unit vectors such that $0 < |\langle a|b\rangle| \leq \frac{3}{\sqrt{14}}$. Then there exists a set of projection observables $\mathcal{O}$ containing P_a and P_b, and a set of contexts $\mathcal{C}$ over $\mathcal{O}$, such that there is no admissible assignment function under which $\mathcal{O}$ is non-contextual and P_a, P_b have the value 1.*

An operational form of the strong Kochen-Specker theorem capable of identifying a value indefinite observable is given by

> **Operational Kochen-Specker theorem**. *Let $|\psi\rangle \in \mathbb{C}^3$ be a quantum state describing a system. Also let $|\phi\rangle \in \mathbb{C}^3$ be any other state which satisfies $\sqrt{\frac{5}{14}} \leq |\langle\psi|\phi\rangle| \leq \frac{3}{\sqrt{14}}$. Then, assuming* **(A3)***, P_ϕ cannot be assigned a definite value by a faithful assignment function.*

The operational Kochen-Specker theorem allows us to identify and then measure a value indefinite observable, a crucial point in what follows. Consider a system in which a value indefinite quantum experiment is prepared, measured, rinsed and repeated ad infinitum. The infinite sequence $\mathbf{x} = x_1x_2\dots$ obtained by concatenating the outputs of these measurements is called *value indefinite quantum random sequence*, shortly, *quantum random sequence*. We are now able to give a mathematical argument showing that a quantum randomness produced by a specific type of experiment is better than pseudo-randomness [8, 1]:

> **Incomputability theorem**. *Assume* **(A1)**–**(A5)** *for $\mathbb{C}^3$. Then, every quantum random sequence is Turing incomputable.*

In fact, a stronger result is true [8, 1]:

> **Strong incomputability theorem**. *Assume* **(A1)**–**(A5)** *for $\mathbb{C}^3$. Then, every quantum random sequence is bi-immune, that is, every Turing machine cannot compute exactly more than finitely many bits of the sequence.*

Bi-immunity assures that any adversary can be sure of no more than finitely many exact values—guessed or computed—of any given quantum random sequence. This is indeed a good certificate of quality for this type of quantum randomness.

5 A quantum random number generator

The theoretical results discussed in the previous section have practical value only if one can design a quantum random number generator in which a value indefinite observable is measured, a guarantee for its strong incomputability. In particular, a quantum random number generator has to act in $\mathbb{C}^n$ with $n > 2$.

A quantum random number generator [1] designed in terms of generalised beam splitters satisfies these requirements; its blueprint is presented in Figure 1. The configuration indicates the preparation and the measurement stage, including filters blocking $|\mathsf{S}_z : -1\rangle$ and $|\mathsf{S}_z : +1\rangle$. (For ideal beam splitters, these filters would not be required.) The measurement stage (right array) realises a unitary quantum gate U_x, corresponding to the projectors onto the S_x state observables for spin state measurements along the x-axis, in terms of generalised beam splitters. More details about its implementation and practical issues are presented in [1].

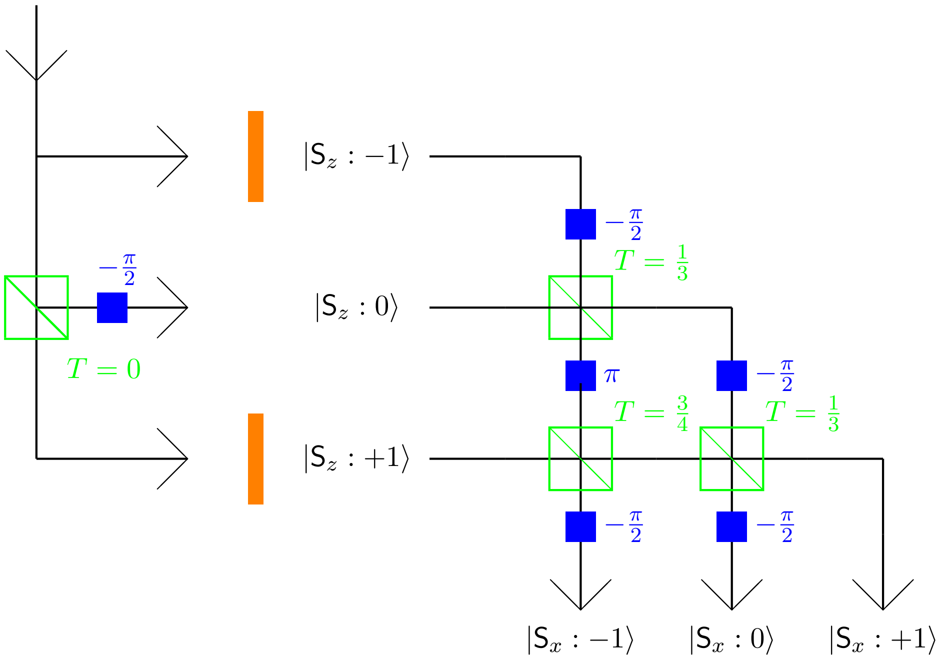
$|\mathsf{S}_z : -1\rangle$
$|\mathsf{S}_z : 0\rangle$
$|\mathsf{S}_z : +1\rangle$
$-\frac{\pi}{2}$
$T = 0$
$-\frac{\pi}{2}$
$T = \frac{1}{3}$
π
$-\frac{\pi}{2}$
$T = \frac{3}{4}$
$T = \frac{1}{3}$
$-\frac{\pi}{2}$
$-\frac{\pi}{2}$
$|\mathsf{S}_x : -1\rangle$
$|\mathsf{S}_x : 0\rangle$
$|\mathsf{S}_x : +1\rangle$

Figure 1: QRNG in $\mathbb{C}^3$

6 Conclusion and open questions

The practice of generating and commercialising quantum random bits raises many question marks about the quality of randomness it produces. Based on certain natural physical hypotheses, we have described a procedure to generate quantum random bits that *provably* are not reproducible by any Turing machine, an example of incomputability in nature (see [11]). In particular, this proves that this type quantum randomness is superior in quality to pseudo-randomness. A quantum random generator which produces bi-immune sequences has been described.

This is just the start of a program for better understanding and producing quantum randomness. Many problems remain open, and here are some of them. Does a variant of the operational Kochen-Specker theorem hold true in $\mathbb{C}^2$, possibly with additional physical assumptions? Does Quantis, the quantum random generator produced by ID Quantique which operates in $\mathbb{C}^2$, produce sequences bi-immune sequences? Are other physical assumptions sufficient for proving an analogue of the operational Kochen-Specker theorem? Can other physical assumptions lead to different types of quantum random generators producing bi-immune sequences? How random is a sequence produced by an experiment certified by the operational Kochen-Specker theorem? Can results on quantum randomness of sequences be transferred to randomness of single events? Is quantum randomness unique or of different forms and qualities?

7 Acknowledgement

The author has been supported in part by Marie Curie FP7-PEOPLE-2010-IRSES Grant RANPHYS and has benefitted from discussions and collaboration with A. Abbott, J. Conder, B. Cooper, M. Dinneen, M. Dumitrescu, J. Gruska, G. Longo, K. Svozil and K. Tadaki. I thank them all.

References

[1] A. A. Abbott, C. S. Calude, J. Conder, K. Svozil. Strong Kochen-Specker theorem and incomputability of quantum randomness, *Physical Review A* 86, 6 (2012), DOI: 10.1103/PhysRevA.00.002100.

[2] A. Abbott, C. S. Calude, K. Svozil. A quantum random number generator certified by value indefiniteness, *Mathematical Structures in Computer Science*, 2013, to appear.

[3] J. Barrett, R. Colbeck, A. Kent. Memory Attacks on Device-Independent Quantum Cryptography, arXiv:1201.4407v6 [quant-ph] 6 Aug 2013.

[4] J. L. Borges. *The Lottery in Babylon*, in D. A. Yates, J. E. Irby, J. M. Fein, E. Weinberger (ed. & transl.). *Everything and Nothing*, New Directions, New York, 1999, 31–38.

[5] C. S. Calude. *Information and Randomness: An Algorithmic Perspective*, Springer-Verlag, Berlin, 2002 (2nd Edition).

[6] C. S. Calude. Algorithmic randomness, quantum physics, and incompleteness, in M. Margenstern (ed.). *Proc. Conf. "Machines, Computations and Universality" (MCU'2004)*, Lectures Notes in Comput. Sci. 3354, Springer, Berlin, 2005, 1–17.

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

[8] C. S. Calude, K. Svozil. Quantum randomness and value indefiniteness, *Advanced Science Letters* 1 (2008), 165–168.

[9] J. Cederlof, J.-A. Larsson. Security aspects of the authentication used in quantum cryptography, *IEEE Transactions on Information Theory*, 54, 4, (2008), 1735–1741.

[10] S. B. Cooper. *Computability Theory*, Chapman & Hall/CRC London, 2004.

[11] S. B. Cooper, P. Odifreddi. Incomputability in nature, in S. B. Cooper and S. S. Goncharov (eds.). *Computability and Models: Perspectives East and West*, Plenum Publishers, New York, 2003, 137–160.

[12] B. Day. Just how secure is quantum cryptography? *Optical Society* `http://www.osa.org/en-us/about_osa/newsroom/newsreleases/2013/just_how_secure_is_quantum_cryptography/`, 28 May 2013. gives more details.

[13] C. Dillow. Zeroing in on unbreakable computer security, `http://tech.fortune.cnn.com/2013/07/29/from-russia-unbreakable-computer-code/`, July 29, 2013.

[14] R. Downey, D. Hirschfeldt. *Algorithmic Randomness and Complexity*, Springer, Heidelberg, 2010.

[15] A. Eagle. Randomness is unpredictability, *British Journal for the Philosophy of Science* 56 (2005), 749–90.

[16] A. Einstein, B. Podolsky, N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* 47 (1935), 777–780.

[17] T. Gowers. A new proof of Szemerédi's theorem, *Geom. Funct. Anal.* 11, 3 (2001), 465–588.

[18] R. Graham. Some of my favorite problems in Ramsey Theory, *INTEGERS, The Electronic Journal of Combinatorial Number Theory* 7, 2 (2007), #A2.

[19] R. Graham, J. H. Spencer. Ramsey theory, *Scientific American* 262, 7 (1990), 112–117.

[20] J. Gruska. From classical cryptography to quantum physics through quantum cryptography, *Journal of the Indian Institute of Science* 89,3 (2009), 271–282.

[21] M. Hogenboom. 'Uncrackable' codes set for step up, *BBC News* 4 September 2013, `http://www.bbc.co.uk/news/science-environment-23946488`.

[22] S. Kochen, E. P. Specker. The problem of hidden variables in quantum mechanics, *Journal of Mathematics and Mechanics* 17 (1967), 59–87.

[23] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photon* 4, 10 (2010), 686–689. Supplementary information `http://www.nature.com/nphoton/journal/v4/n10/abs/nphoton.2010.214.html`.

[24] A. Mann. The laws of physics say quantum cryptography is unhackable. It's not! *Wired Science*, `http://www.wired.com/wiredscience/2013/06/quantum-cryptography-hack/`, 21 March 2013.

[25] True randomness demonstrated, `http://www.nature.com/nature/journal/v464/n7291/edsumm/e100415-06.html.`

[26] A. Soifer. Ramsey theory before Ramsey, prehistory and early history: An essay, in A. Soifer (ed.), *Ramsey Theory: Yesterday, Today, and Tomorrow*, Springer, Progress in Mathematics 285, Berlin, 2011, 1–26.

[27] Conference on Lasers and Electro-Optic 2013, `http://www.cleoconference.org/home/news-and-press/cleo-press-releases/cleo-2013-the-premier-international-laser-and-elec/`.

[28] `www.idquantique.com`.

[29] `http://www.magiqtech.com`.

[30] `http://www.sciencedaily.com/releases/2013/05/130528122435.htm`.