Math. Struct. in Comp. Science (2014), vol. 24, iss. 3, e240303, 23 pages. © Cambridge University Press 2014
doi:10.1017/S0960129512000692

A quantum random number generator certified by value indefiniteness

ALASTAIR A. ABBOTT[†], CRISTIAN S. CALUDE[†] and KARL SVOZIL[‡]

[†]*Department of Computer Science, University of Auckland, Private Bag 92019, Auckland, New Zealand*
Email: a.abbott@auckland.ac.nz;cristian@cs.auckland.ac.nz
[‡]*Institut für Theoretische Physik, Vienna University of Technology, Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria*
Email: svozil@tuwien.ac.at

Received 13 December 2010; revised 5 May 2011

In this paper we propose a quantum random number generator (QRNG) that uses an entangled photon pair in a Bell singlet state and is certified explicitly by value indefiniteness. While 'true randomness' is a mathematical impossibility, the certification by value indefiniteness ensures that the quantum random bits are incomputable in the strongest sense. This is the first QRNG setup in which a physical principle (Kochen–Specker value indefiniteness) guarantees that no single quantum bit that is produced can be classically computed (reproduced and validated), which is the mathematical form of bitwise physical unpredictability.
We discuss the effects of various experimental imperfections in detail: in particular, those related to detector efficiencies, context alignment and temporal correlations between bits. The analysis is very relevant for the construction of any QRNG based on beam-splitters. By measuring the two entangled photons in maximally misaligned contexts and using the fact that two bitstrings, rather than just one, are obtained, more efficient and robust unbiasing techniques can be applied. We propose a robust and efficient procedure based on XORing the bitstrings together – essentially using one as a one-time-pad for the other – to extract random bits in the presence of experimental imperfections, as well as a more efficient modification of the von Neumann procedure for the same task. We also discuss some open problems.

1. Introduction

Random numbers have been around for more than 4,000 years, but they have never been in such demand as in our time – people now use random numbers everywhere. Randomness is understood through various 'symptoms', of which, three widely accepted ones are:

(i) *Unpredictability:*
It is impossible to win against a random sequence in a fair betting game.
(ii) *Incompressibility:*
It is impossible to compress a random sequence.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

(iii) *Typicalness:*

Random sequences pass every statistical test of randomness.

We are led to ask whether our intuitions with regard to randomness can be cast in more rigorous terms. Randomness plays an essential role in probability theory, which is the mathematical calculus of random events. Kolmogorov axiomatic probability theory assigns probabilities to sets of outcomes, and shows how to calculate with such probabilities; it assumes randomness, but does not distinguish between individually random and non-random elements.

For example, under a uniform distribution, the outcome of n zeros,

$$\underbrace{000\cdots0}_{n \text{ times}},$$

has the same probability as any other outcome of length n, namely 2^{-n}. A similar situation appears in quantum mechanics: quantum randomness is postulated, rather than defined or deduced.

Algorithmic information theory (AIT) (Chaitin 1977), which was developed in the 1960s, defines and studies individual random objects, such as finite bitstrings or infinite sequences. AIT shows that 'pure randomness' or 'true randomness' does not exist from a mathematical point of view. For example, there is no infinite sequence passing all tests of randomness. Randomness cannot be proved mathematically: one can never be sure a sequence is random; there are only forms and degrees of randomness.

Computers produce 'random numbers' generated by algorithms. It took a long time for computer scientists to realise that randomness produced by software is far from being random. This form of randomness, which is known as pseudo-randomness, is good at mimicking the human perception of randomness, but its quality is rather low because computability destroys many symptoms of randomness, such as unpredictability. It is not totally unreasonable to suggest that pseudo-randomness is a reflection of its creators' subjective 'understanding' and 'projection' of randomness[†]. Although no computer or software manufacturer claims that their products can generate truly random numbers, such formally unfounded claims have recently reappeared for randomness produced in physical experiments, with suggestions that 'truly random numbers have been generated at last'[‡].

2. Quantum randomness

2.1. *Theoretical claims for quantum randomness*

Quantum mechanics has a credible claim to be one of the best (if not the best) sources of randomness. Many quantum phenomena can be used for random number generation,

[†] Psychologists have known for a long time that people tend to distrust streaks in a series of random bits, hence they imagine a coin flipping sequence alternates between heads and tails much more often than in the case of 'randomness'. A simple illustration of this phenomenon, called the gambler's fallacy, is the belief that after a coin has landed on tails ten consecutive times, there is a greater chance that the coin will land on heads at the next flip.

[‡] See the RANDOM.ORG website (`http://www.random.org/`) and Merali (2010).

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

including nuclear decay radiation sources, the quantum mechanical noise in electronic circuits (known as shot noise) or photons travelling through a semi-transparent mirror.

What is the rationale for the claim that quantum randomness is indeed a better form of randomness than, say, pseudo-randomness? In addition to quantum complementarity (Pauli 1958) (that is, the impossibility of simultaneous measurements of certain complementary observables, resulting in a randomisation of one observable if the other observable is determined) and the randomness of certain individual measurement outcomes (Born 1969), the Kochen–Specker Theorem (Kochen and Specker 1967) tells us that in a quantum mechanical system represented by a Hilbert space of dimension greater than two, for any hidden variable theory fulfilling the predictions of quantum mechanics, the following two conditions are contradictory:

(1) value definiteness – the fact that, in general, there can be no co- or pre-existing definite values prescribable to certain sets of measurement outcomes (Calude and Svozil 2008; Svozil 2011); and
(2) non-contextuality – the value corresponding to the outcome of a measurement of an observable is independent of the other compatible observables measured alongside it.

A quantum random experiment certified by value indefiniteness via the Kochen–Specker Theorem (that is, an experiment in which the Kochen–Specker theorem guarantees value indefiniteness) generates an *infinite (strongly) incomputable sequence of bits*: every Turing machine can only exactly reproduce finitely many scattered digits of such an infinite sequence, that is, the sequence is bi-immune (Calude and Svozil 2008). Such certification, as has already been pointed out previously (Calude and Svozil 2008), is based on the assumption that there are no contextual hidden variables. Indeed, if the value of a bit could be computed before its measurement, we could assign a definite value to the observable, which would be a contradiction. The tricky part is that we need to look at infinite sequences to prove the incomputability of individual bits. It is this formal incomputability that corresponds to the physical notion of indeterminism in quantum mechanics[†] rather than the mathematically vacuous notion of 'true randomness'.

Quantum random number generators (QRNGs) based on beam splitters (Svozil 1990; Rarity *et al.* 1994) have been realised by Zeilinger's group in Innsbruck and Vienna (Jennewein *et al.* 2000) and applied to show violation of Bell's inequality under strict Einstein locality conditions[‡].

Gisin's group in Geneva (Stefanov *et al.* 2000), and, in particular, its *IDQ* spin-off, produces and markets a commercial device called *Quantis*[§]. In order to eliminate bias, the device employs von Neumann normalisation (in fact, a more efficient iterated version due to Peres (1992) is used), which requires the *independence* of individual events: bits are grouped into pairs, and then equal pairs (00 or 11) are discarded and we replace 01 with 0 and 10 with 1 (Von Neumann 1951).

[†] That is, the inability, *even in principle*, to predict the outcome of certain quantum measurements.
[‡] That is, two space-like separated events cannot influence each other in any way (Weihs *et al.* 1998).
[§] See the IDQ website `http://www.idquantique.com/` and the technical whitepaper `http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-whitepaper.pdf` for further details.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

A group in Shanghai and Beijing (Wang *et al.* 2006) has used a Fresnel multiple prism as a polarising beam splitter, and as a normalisation technique they used previously generated experimental sequences as a one-time pad to 'encrypt' random sequences.

QRNGs based on entangled photon pairs have been realised by a second Chinese group in Beijing and Ji'nan (Hai-Qiang *et al.* 2004). They used spontaneous parametric down-conversion to produce entangled pairs of photons. One of the photons was used as a trigger, mostly to allow a faster data production rate by eliminating double counts. Again, von Neumann normalisation was applied in an attempt to eliminate bias.

A group (Fiorentino *et al.* 2007) from the Hewlett-Packard Laboratories in Palo Alto and Bristol has used entangled photon pairs in the Bell basis state $|H_1V_2\rangle + |V_1H_2\rangle$ (note that this is not a singlet state and attains this form only for one polarisation direction; in all the other directions, the state also contains V_1V_2 and H_1H_2 contributions), where the outcomes H_1, V_1 and H_2, V_2 refer to observables associated with unspecified (presumably identical for both particles) directions. In analogy to von Neumann normalisation, the coincidence events H_1V_2 and V_1H_2 were mapped into 0 and 1, respectively. In this way, as the authors argued, the 2-qubit space of the photon pair is effectively restricted to a two-dimensional Hilbert subspace described by an effective-qubit state.

A more recent version of a QRNG (Pironio *et al.* 2010), although not based on photons and beamsplitters, uses Boole–Bell-type setups 'secured by' Boole–Bell-type inequality violations in the spirit of quantum cryptographic protocols (Ekert 1991; Bechmann-Pasquinucci and Peres 2000). This provides some indirect 'statistical verification' of value indefiniteness (again under the assumption of non-contextuality), but falls short of providing certification of strong incomputability through value indefiniteness (Calude and Svozil 2008; Svozil 2009). With regard to value indefiniteness, the difference between Boole–Bell-type inequalities and Kochen–Specker-type theorems is that in the Boole–Bell-type case, the breach of value indefiniteness does not need to happen at every single particle, but it must do so *for every particle* in the Kochen–Specker-type case (Svozil 2011). Briefly stated, the Boole–Bell-type violation is statistical, but *not necessarily* on every quantum separately. Hence, because a Boole–Bell-type violation does not guarantee that every bit is certified by value indefiniteness, we could potentially produce sequences containing infinite computable subsequences 'protected' by Boole–Bell-type violations. Furthermore, given that such criticisms also seem to hold for the statistical verification of value indefiniteness (Pan *et al.* 2000; Huang *et al.* 2003; Cabello 2008), it seems unlikely that statistical tests of the measurement outcomes alone can fully certify such a QRNG.

2.2. *Shortcomings of current QRNGs*

It is clear that any QRNG claiming a better quality of randomness has to produce at least an infinite incomputable sequence of outputs, and preferably a strongly incomputable one. We now need to consider whether current proposals for QRNGs generate 'in principle' strongly incomputable sequences of quantum random bits. To answer this question, we have to check whether the QRNG is 'protected' by value indefiniteness, which is the only

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

Table 1. *p-values for the χ^2 test that the bitstring is sampled from the uniform distribution. Bold values indicate statistically significant evidence that the strings are not sampled from the uniform distribution.*

QRNG	$k = 1$	$k = 2$	$k = 3$	$k = 4$	$k = 5$
Maple	0.79	0.15	0.83	0.47	0.97
Mathematica	0.18	0.38	0.35	0.45	0.99
π	0.38	0.27	0.05	0.62	0.21
Quantis	$\mathbf{<10^{-10}}$	$\mathbf{<10^{-10}}$	$\mathbf{<10^{-10}}$	$\mathbf{<10^{-10}}$	$\mathbf{<10^{-10}}$
Vienna	0.12	$\mathbf{<10^{-10}}$	$\mathbf{<10^{-10}}$	$\mathbf{<10^{-10}}$	$\mathbf{<10^{-10}}$

physical principle currently known to guarantee incomputability; in most cases, the answer is either no or cannot be given because of a lack of information about the mechanism of the QRNG.

Calude *et al.* (2010) used tests based on algorithmic information theory to analyse and compare quantum and non-quantum bitstrings. Ten strings of length 2^{32} bits each from two quantum sources (the commercial *Quantis* device and the Vienna Institute for Quantum Optics and Quantum Information group (Jennewein 2009)) and three classical sources (Mathematica, Maple and the binary expansion of π) were analysed. Even though no distribution was assumed for any of the sources, a test based on Borel-normality was able to distinguish between the quantum and non-quantum sources of random numbers. It is known that almost all algorithmically random strings are Borel-normal (Calude 2002), though the converse is not true. Indeed, the tests found the quantum sources to be less normal than the pseudo-random ones. So the question arises as to whether this is a property of quantum randomness or evidence of flaws in the tested QRNGs.

Abbott and Calude (2012) discussed the probability distribution for an ideal QRNG: it is no surprise that such devices are seen to sample from the uniform distribution. Testing the same strings as in Calude *et al.* (2010) against this expected distribution, strong evidence was found that the QRNGs tested are *not* sampling from the correct distribution. On the other hand, weaker evidence suggests the pseudo-random sources of randomness (Mathematica and Maple) are too normal. The results of the analysis are presented in Table 1.

The notable exception to these findings are the Vienna bits, which, when viewed at the single-bit level, appear unbiased. It appears that the good performance at the 1-bit level was achieved (perhaps through experimental feedback control) at the cost of the performance at the $k \geqslant 2$ level, which is much harder to control without post-processing. The *Quantis* QRNG uses von Neumann normalisation in an attempt to unbias the output; the fact that this is not completely successful indicates either a significant variation in bias over time, or some non-independence of successive bits (Abbott and Calude 2012).

These results highlight the need to pay extra attention in the design process to the distribution produced by a QRNG. Normalisation techniques are an effective way to

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

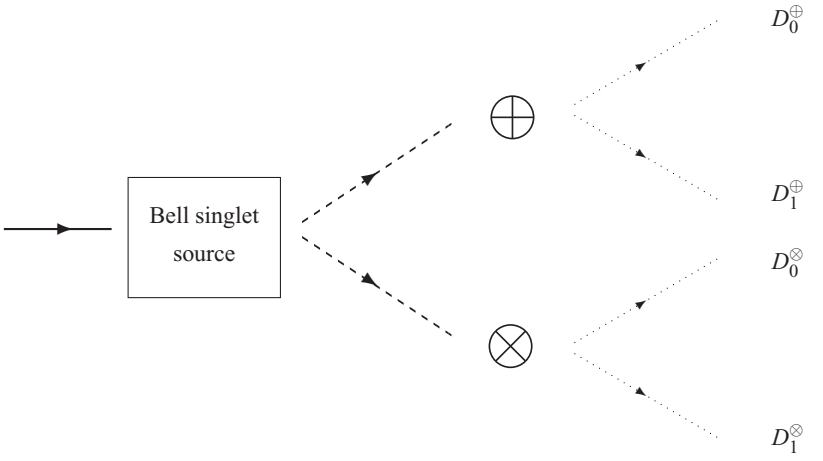


Fig. 1. Scheme of a quantum random number generator (Svozil 2009).

remove bias, but to achieve the desired effect, some assumptions about independence and constancy of bias must be satisfied (Abbott and Calude 2012). While the ideal QRNG will never be realised in practice, we need to be aware of how much the experimental imperfections affect the results. Any credible QRNG should take these issues into account, in addition to providing explicit certification of randomness by some physical law, such as value indefiniteness.

3. The scheme under ideal conditions

In this section, we will discuss in detail a QRNG proposal put forward in Svozil (2009) and illustrated in Figure 1. It uses the singlet state of two two-state particles (for example, photons with linear polarisation) proportional to $|H_1V_2\rangle - |V_1H_2\rangle$, which is form invariant in all measurement directions.

A single photon light source (presumably an LED) is attenuated so that it is rare for more than one photon to be in the beam path at the same time. These photons impinge on a source of singlet states of photons (presumably by spontaneous parametric down-conversion in a non-linear medium). The two resulting entangled photons are then analysed with respect to their linear polarisation state in two directions that are $\pi/4$ radians 'apart', which will be denoted by '$\oplus$' and '$\otimes$'.

Because a four-dimensional Hilbert space is required, this QRNG is 'protected' by Bell-type value indefiniteness in addition to Kochen–Specker- and Greenberger-Horne-Zeilinger-type value indefiniteness[†]. The protocol uses all three of the principal types of quantum indeterminism:

(i) the indeterminacy of individual outcomes of single events as proposed by Born and Dirac;

[†] Note that this is not the case for current QRNGs based on beam-splitters, which operate in a Hilbert space of dimension two.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

Table 2. *The logical exclusive or operation.*

$O_i^{\oplus}$	$O_i^{\otimes}$	$O_i^{\oplus}$ XOR $O_i^{\otimes}$
0	0	0
0	1	1
1	0	1
1	1	0

(ii)quantum complementarity (due to the use of conjugate variables), as put forward by Heisenberg, Pauli and Bohr; and

(iii)value indefiniteness due to Bell, Kochen and Specker, and Greenberger, Horne and Zeilinger.

This is essentially the same experimental configuration as that used to measure the correlation function at an angle of $\pi/4$ radians (45°). Whereas the correlation function averages over 'a large number' of single contributions, a random sequence can be obtained by concatenating these single pairs of outcomes through addition modulo 2.

Formally, we suppose that for the ith experimental run, the two outcomes are $O_i^{\oplus} \in \{0,1\}$ (corresponding to $D_0^{\oplus}$ or $D_1^{\oplus}$) and $O_i^{\otimes} \in \{0,1\}$ (corresponding to $D_0^{\otimes}$ or $D_1^{\otimes}$). These two outcomes $O_i^{\oplus}$ and $O_i^{\otimes}$, which themselves form two sequences of random bits, are subsequently combined by the XOR operation, which amounts to determining their parity, or to addition modulo 2 according to Table 2 (in the following, XOR refers to either a binary function of two binary observables or to the logical operation, depending on the formal context). In other words, one outcome is used as a *one-time pad* to 'encrypt' the other outcome, and *vice versa*. As a result, we obtain a sequence $x = x_1 x_2 \ldots x_n$ with

$$x_i = O_i^{\oplus} + O_i^{\otimes} \bmod 2. \tag{1}$$

In order for the XORed sequence to be certifiably incomputable (via value indefiniteness), we must prove that the certification is preserved under XORing – in fact, strong incomputability itself is *not* necessarily preserved. By necessity, any QRNG certified by value indefiniteness must operate non-trivially in a Hilbert space of dimension $n \geqslant 3$. To transform the n-ary (incomputable) sequence into a binary one, a function $f : \{0,1,\ldots,n-1\} \to \{0,1,\lambda\}$ must be used (λ is the empty string); to claim certification, the strong incomputability of the bits must still be guaranteed after the application of f. This is a fundamental issue, which has to be checked for existing QRNGs such as that in Pironio *et al.* (2010); without it, we cannot claim to produce truly indeterministic bits. In general, incomputability itself is not preserved by f, but by considering the value indefiniteness of the source, the certification can be seen to hold under XOR as well as when discarding bits (Abbott *et al.* 2012).

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

4. 'Random' errors or systematic errors

In this section we shall discuss possible 'random' (no pun) or systematic errors in experimental realisations of the QRNG described in the previous section (many of these errors may appear in other types of photon-based QRNGs). Our aim is to draw attention to the specific nature of such errors and how they affect the resulting bitstrings. A good QRNG must, in addition to the necessary certification (for example, by value indefiniteness), take into account the nature of these errors and be carefully designed (including any subsequent post-processing) so that the resultant distribution of bitstrings that the QRNG samples from is as close as possible to the expected uniform distribution (Abbott and Calude 2012). Both the uniformity of the source and incomputability are 'independent symptoms' of randomness, and care must be taken to obtain both properties.

4.1. *Double counting*

One possible problem is that the detectors analysing the different polarisation directions do not respond to photons of the same pair, but to two photons belonging to different pairs. This does not seem to be a drawback for the application of the XOR operation since (at least in the absence of temporal correlations between bits) the postulates of quantum mechanics state that the individual outcomes occur independently and indeterministically (the latter property is mathematically modelled by strong incomputability (Calude and Svozil 2008; Abbott *et al.* 2012)). On the other hand, more care is needed if the events are not independent. However, correlation between events is an undesirable property in itself, and provided care is taken, it is unlikely to be made worse by double counting.

4.2. *Non-singlet states*

The state produced by the spontaneous parametric down-conversion may not be an exact singlet. This may give rise to a systematic bias of the combined light source/analyser setup in a very similar way to the way it does for beam splitters.

4.3. *Non-alignment of polarisation measurement angles*

No experimental realisation can attain a 'perfect anti-alignment' of the polarisation analysers at angles $\pi/4$ radians apart, and it is only in this ideal case that the bases are conjugate and the correlation function is exactly zero. Indeed, 'tuning' the angle to obtain equi-balanced sequences of zeroes and ones may provide a method of anti-aligning the polarisers properly. However, we need to bear in mind that any such 'tampering' with the raw sequence of data to achieve Borel normality (for example, by readjustments of the experimental setup) may introduce unwanted (temporal) correlations or other bias (Calude *et al.* 2010).

Incidentally, the $\pi/4$ angle is one of the three points, at angles 0, $\pi/4$ and $\pi/2$, in the interval $[0, \pi/2]$ at which the classical and quantum correlation functions coincide. For all other angles, there is a higher ratio of different or identical pairs than would

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

be expected classically. Thus, ideally, the QRNG could be said to operate in the 'quasi classical' regime, albeit fully certified by quantum value indefiniteness.

Quantitatively, the expectation function of the sum of the two outcomes modulus 2 can be defined by averaging over the sum modulo 2 of the outcomes $O_i^0, O_i^\theta \in \{0,1\}$ at angle θ 'apart' in the ith experiment and over a 'large number' of experiments: that is,

$$E_{\texttt{XOR}}(\theta) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} \left(O_i^0 + O_i^\theta \bmod 2\right).$$

This is related to the standard correlation function

$$C(\theta) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} O_i^0 \cdot O_i^\theta$$

by

$$E_{\texttt{XOR}}(\theta) = \frac{|C(\theta) - 1|}{2},$$

where

$$O_i^0 \cdot O_i^\theta = \begin{cases} 1 & \text{if } O_i^0 = O_i^\theta \\ -1 & \text{if } O_i^0 \neq O_i^\theta. \end{cases}$$

A detailed calculation yields the classical linear expectation function

$$E_{\texttt{XOR}}^{\text{cl}}(\theta) = 1 - 2\theta/\pi,$$

and the quantum expectation function

$$E_{\texttt{XOR}}(\theta) = (1/2)(1 + \cos 2\theta).$$

Thus, for angles 'a long way' from $\pi/4$, the XOR operation actually *deteriorates* the two random signals taken from the two analysers *separately*. The deterioration is even *greater quantum mechanically than classically* since the entangled particles are more correlated and thus 'less independent'. Potentially, this could be used to ensure a $\pi/4$ mismatch more accurately than possible through classical means. This will be discussed further in Section 5.

In order to avoid this negative feature while generating bits, instead of XORing outcomes of *identical* partner pairs, we could XOR time-shifted outcomes: for example, instead of the expression in Equation (1), we could consider

$$x_i = O_i^0 + O_{i+j}^\theta \bmod 2, \text{ with } j > 0. \tag{2}$$

We should make j large enough to ensure that, taking into account double counting, there is no chance of accidentally causing two offset but correlated outcomes to be XORed together. We discuss a theoretical analysis of the effects of experimental imperfections and the XOR operation later in this paper, and XORing shifted pairs is an efficient and effective procedure for reducing such errors.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

4.4. *Different detector efficiencies*

Differences in detector efficiencies result in a bias of the sequence. This complicating effect is separate from non-perfect misalignment of the polarisation context. Suppose the probabilities of detection are denoted by p_{H_1}, p_{H_2}, p_{V_1}, p_{V_2}. Since

$$p_{H_1} + p_{V_1} = p_{H_2} + p_{V_2} = 1,$$

the probability of finding pairs adding up to 0 and 1 modulo 2 are

$$p_{H_1}p_{H_2} + p_{V_1}p_{V_2} = 1 - (p_{H_1} + p_{H_2}) + 2p_{H_1}p_{H_2}$$

and

$$p_{H_1}p_{V_2} + p_{V_1}p_{H_2} = p_{H_1} + p_{H_2} - 2p_{H_1}p_{H_2},$$

respectively (adding up to 1). If both $p_{H_1} \neq p_{V_1}$ and $p_{H_2} \neq p_{V_2}$, the resulting XORed sequence is biased. The two resulting sequences could be unbiased before or after XORing by the von Neuman method (Von Neumann 1951, page 768), although any temporal correlations would violate the condition of independence required by this method. However, it should be borne in mind that the von Neumann normalisation procedure necessarily discards many bits, though there are more efficient methods (Peres 1992). The efficiency can be increased by using both strings more carefully, and such a method is discussed in Section 6.4.

4.5. *Unstable detector bias*

Von Neumann type normalisation procedures will only remove bias due to detector efficiencies if the bias remains constant over time. If the bias drifts over time due to instability in the detectors, the resulting normalised sequence will not be unbiased, just less biased (Abbott and Calude 2012). It is difficult to overcome this since some experimental instability is inevitable. However, bounds on the bias of the normalised sequence based on reasonable experimental parameters (Abbott and Calude 2012) can be used to determine the length for which the source samples from the uniform distribution is 'close enough'.

If the bias varies independently between detectors, the XORing process should serve to reduce the impact of varying detector efficiencies, and applying von Neumann normalisation to the XORed bitstring is advantageous compared with working with a single bitstring from a source of varying bias.

4.6. *Temporal correlations, photon clustering and 'bunching'*

The Hanbury–Brown–Twiss effect means that the photons may be temporally correlated and thus arrive clustered or 'bunched'. Temporal correlations also appear in 'double-slit analogous experiments' in the time domain (Lindner *et al.* 2005), where the role of the slits is played by windows in time of attosecond duration. This can, to an extent, be avoided by ensuring that successive photons are sufficiently separated, although this poses a limit on the bitrate of such a device. However, since the case where two or more singlet pairs are in the beam path at the same time is potentially of sufficient importance, this effect needs further careful consideration.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

Another possible source of temporal correlations arises from the detector dead-time, T_d, during which the detector is inactive after making a measurement (Stefanov *et al.* 2000). If we measure $O_i^{\oplus} = 0$, the detector $D_0^{\oplus}$ corresponding to 0 is unable to detect another photon for a small amount of time, which significantly increases the chance of detecting a photon at the other detector during this time, producing a 1. This leads to higher than expected chances of 01 and 10 being measured. This is problematic since such a correlation will not be removed by `XORing`, even with an offset of j. However, this can be avoided by discarding any measurements within time T_d of the previous measurement.

In view of possible temporal correlations, it would be interesting to test the quality of the random signal as j is varied in Equation (2). As previously mentioned, any temporal correlations will violate the condition of independence needed for von Neumann normalisation, making it difficult to remove any bias in the output; if the dependence can be bounded, unbiasing techniques such as that proposed in Blum (1986) could be used instead of von Neumann's procedure. Where possible, it seems more desirable and simpler to avoid temporal correlations by using a carefully designed experimental methodology rather than by post-processing.

4.7. *Fair sampling*

In the same way as with most optical tests of Bell's inequalities (Clauser and Shimony 1978; Garrison and Chiao 2008), the inefficiency of photon detection requires us to make the *fair sampling assumption* (Garg and Mermin 1987; Larsson 1998; Pearle 1970; Berry *et al.* 2010): the loss is independent of the measurement settings, so the ensemble of detected systems provides a fair statistical sample of the total ensemble. In other words, we must exclude the possibility of a 'demon' in the measuring device conspiring against us in choosing which bits to reject.

The strength of the proposed QRNG relies crucially on value indefiniteness, so without this fair sampling assumption, we would forfeit the assurance of bitwise incomputability of the generated sequence. As an example, consider the extreme case in which the detection efficiency is less than 50%; our supposed demon could reject all bits detected as 0 and still be within the bounds given by this efficiency, while the produced sequence would be computable. In the more general case for any efficiency $\rho < 1$, the demon could reject bits to ensure every $\big(1/(1-\rho)\big)$th bit is a zero; this would introduce an infinite computable subsequence, which would violate the strong incomputability of the output bitstring produced by our QRNG, and still be consistent with the detection efficiency.

Note that this condition is stronger than the fair sampling assumption required in tests for violation of Bell-type inequalities because, without this assumption, *any* inefficiency can lead to a loss of randomness.

5. Better-than-classical operationalisation of spatial orthogonality

As has already been pointed out, for no temporal offset and in the regime of relative spatial angles around $\pi/4$ (that is, at almost half orthogonal measurement directions), the

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

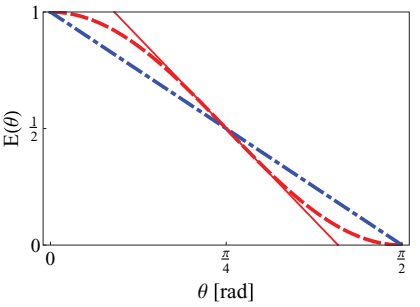


Fig. 2. (Colour online) The classical and quantum expectation functions and the linear quantum approximation around $\pi/4$.

classical linear expectation function

$$E^{\mathrm{cl}}_{\mathtt{XOR}}(\theta) = 1 - 2\theta/\pi$$

for $0 < \theta < \pi/4$ is strictly *smaller* than and for $\pi/4 < \theta < \pi/2$ strictly *greater* than the quantum expectation function

$$E_{\mathtt{XOR}}(\theta) = (1/2)(1 + \cos 2\theta).$$

This can be demonstrated by rewriting $\theta = \pi/4 \pm \Delta\theta$ and considering a Taylor series expansion around $\pi/4$ for small $\Delta\theta \ll 1$, which yields

$$E_{\mathtt{XOR}}(\pi/4 \pm \Delta\theta) \approx (1/2) \mp \Delta\theta,$$

whereas

$$E^{\mathrm{cl}}_{\mathtt{XOR}}(\pi/4 \pm \Delta\theta) = (1/2) \mp (2/\pi)\Delta\theta$$

(see Figure 2).

Phenomenologically, this indicates less-than-classical numbers of equal pairs of outcomes '0–0' and '1–1', and more-than-classical non-equal pairs of outcomes '0–1' and '1–0', respectively, for the quantum case in the region $0 < \theta < \pi/4$; and the converse behaviour in the region $\pi/4 < \theta < \pi/2$. This in turn gives 'fewer zeroes' and 'more ones' in the sequence obtained by XORing the pairs of outcomes in the region $0 < \theta < \pi/4$, and 'more zeroes' and 'fewer ones' in the region $\pi/4 < \theta < \pi/2$ when compared with classical non-entangled systems (Peres 1978). Hence, with increasing aberration from misalignment $\Delta\theta$, the quantum device 'drifts off' into biasedness of the output 'faster' than any classical device. As a result, Borel normality is expected to be broken more strongly and more quickly in the quantum mechanical case than in the classical case.

This effect could in principle be used to operationalise spatial orthogonality through the fine-tuning of angular directions yielding Borel normality. In the resulting protocols, quantum mechanics outperforms any classical scheme due to the differences in the correlation functions.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

6. Theoretical analysis of generated bitstrings

In this section we analyse the output distribution of the proposed QRNG and the ability to extract uniformly distributed bits from the two generated bitstrings in the presence of experimental imperfections.

6.1. *Probability space construction*

With reference to Figure 1 for the setup, we write the generated Bell singlet state with respect to the top ('⊕') measurement context (this is arbitrary as the singlet is form invariant in all measurement directions) as

$$\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle).$$

The lower ('⊗') polariser is at an angle θ to the top one. After beam splitters, we have the state

$$\frac{1}{\sqrt{2}}\left[\cos\theta(|00\rangle - |11\rangle) - \sin\theta(|01\rangle + |10\rangle)\right],$$

so we measure the same outcome in both contexts with probability $\cos^2\theta$, and different outcomes with probability $\sin^2\theta$.

More formally, the QRNG generates two strings simultaneously, so the probability space contains pairs of strings of length n. Let $e_x^{\oplus}, e_y^{\otimes}$ for $x, y = 0, 1$ be the detector efficiencies of the $D_x^{\oplus}$ and $D_y^{\otimes}$ detectors, respectively. For perfect detectors, that is, $e_x^{\oplus} = e_y^{\otimes}$, we would expect a pair of bits (a, b) to be measured with probability

$$2^{-1}(\sin^2\theta)^{a\oplus b}(\cos^2\theta)^{1-a\oplus b};$$

non-perfect detectors alter this probability depending on the values of a and b.

Let $B = \{0, 1\}$, and for $x, y \in B^n$, let $d(x, y)$ be the Hamming distance between the strings x and y, that is, the number of positions at which x and y differ, and let $\#_b(x)$ be the number of bs in x.

The probability space[†] of bitstrings produced by the QRNG is

$$(B^n \times B^n, 2^{B^n \times B^n}, P_{n^2}),$$

where the probability

$$P_{n^2} : 2^{B^n \times B^n} \to [0, 1]$$

is defined for all $X \subseteq B^n \times B^n$ by

$$P_{n^2}(X) = \frac{1}{Z_n} \sum_{(x,y)\in X} (\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)}(e_0^{\oplus})^{\#_0(x)}(e_1^{\oplus})^{\#_1(x)}(e_0^{\otimes})^{\#_0(y)}(e_1^{\otimes})^{\#_1(y)},$$

[†] B^n is the set of bitstrings x of length $|x| = n$, and 2^X is the set of all subsets of the set X.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

and the term

$$Z_n = \sum_{(x,y)\in B^n\times B^n} (\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)}(e_0^{\oplus})^{\#_0(x)}(e_1^{\oplus})^{\#_1(x)}(e_0^{\otimes})^{\#_0(y)}(e_1^{\otimes})^{\#_1(y)}$$
$$= \left[(\sin^2\theta(e_0^{\oplus}e_1^{\otimes} + e_1^{\oplus}e_0^{\otimes}) + \cos^2\theta(e_0^{\oplus}e_0^{\otimes} + e_1^{\oplus}e_1^{\otimes})\right]^n$$

ensures normalisation.

It is easy to check that this is indeed a valid probability space (that is, that it satisfies the Kolmogorov axioms (Billingsley 1979)). Note that for equal detector efficiencies, we have

$$Z_n = (e^{\oplus})^n(e^{\otimes})^n \sum_{(x,y)\in B^n\times B^n} (\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)} = 2^n(e^{\oplus})^n(e^{\otimes})^n,$$

hence the probability has the simplified form

$$P_{n^2}(X) = \sum_{(x,y)\in X} 2^{-n}(\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)}.$$

Given that the proposed QRNG produces two (potentially correlated) strings, it is worth considering the distribution of each string taken separately. Given the rotational invariance of the singlet state, this should be uniformly distributed. However, because the detector efficiencies may vary in each detector, this is not the case in general. For every bitstring $x \in B^n$, we have

$$P_{n^2}(\{x\}\times B^n) = \frac{1}{Z_n}\sum_{y\in B^n}(\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)}(e_0^{\oplus})^{\#_0(x)}(e_1^{\oplus})^{\#_1(x)}(e_0^{\otimes})^{\#_0(y)}(e_1^{\otimes})^{\#_1(y)}$$
$$= \frac{(e_0^{\oplus})^{\#_0(x)}(e_1^{\oplus})^{\#_1(x)}}{Z_n}\sum_{y\in B^n}(\sin^2\theta)^{d(x,y)}(\cos^2\theta)^{n-d(x,y)}(e_0^{\otimes})^{\#_0(y)}(e_1^{\otimes})^{\#_1(y)}$$
$$= \frac{1}{Z_n}\left(e_0^{\oplus}(e_1^{\otimes}\sin^2\theta + e_0^{\otimes}\cos^2\theta)\right)^{\#_0(x)}\left(e_1^{\oplus}(e_0^{\otimes}\sin^2\theta + e_1^{\otimes}\cos^2\theta)\right)^{\#_1(x)}. \quad (3)$$

We can see that each bitstring taken separately appears to come from a constantly biased source, where the probabilities p_0, p_1 that a bit is 0 or 1 are given by the formulae

$$p_0 = e_0^{\oplus}(e_1^{\otimes}\sin^2\theta + e_0^{\otimes}\cos^2\theta)/Z_1$$
$$p_1 = e_1^{\oplus}(e_0^{\otimes}\sin^2\theta + e_1^{\otimes}\cos^2\theta)/Z_1.$$

This can also be viewed as the distribution obtained if we discarded one bitstring after measurement. Note that if either $e_0^{\otimes} = e_1^{\otimes}$ or we have perfect misalignment (that is, $\theta = \pi/4$), the probabilities are given by the simpler formula

$$p_x = e_x^{\oplus}/(e_0^{\oplus} + e_1^{\oplus}), x \in \{0,1\}.$$

In this case, if we also have that $e_0^{\oplus} = e_1^{\oplus}$, we obtain the uniform distribution by discarding one string after measurement.

The analogous result for the symmetrical case $P_{n^2}\left(B^n\times\{y\}\right)$ also holds.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

6.2. *Independence of the QRNG probability space*

If we were to discard one bitstring, it is clear that the other bitstring is generated independently in a statistical sense since the probability distribution source producing it is constantly biased and independent (Abbott and Calude 2012). However, we would like to extend our notion of independence defined in Abbott and Calude (2012) to this 2-bitstring probability space.

We say the probability space $(B^n \times B^n, 2^{B^n \times B^n}, R_{n^2})$ is *independent* if for all $1 \leqslant k \leqslant n$ and $x_1, \ldots, x_k, y_1, \ldots, y_k \in B$, we have

$$\begin{aligned} R_{n^2}(x_1 \ldots x_k B^{n-k} \times y_1 \ldots y_k B^{n-k}) = {} & R_{n^2}\left(x_1 \ldots x_{k-1} B^{n-k+1} \times y_1 \ldots y_{k-1} B^{n-k+1}\right) \\ & \times R_{n^2}\left(B^{k-1} x_k B^{n-k} \times B^{k-1} y_k B^{n-k}\right). \end{aligned}$$

For all $x, y \in B^{|x|}$ and $0 \leqslant k + |x| \leqslant n$, we have

$$P_{n^2}\left(B^{n-k} x B^{n-k-|x|} \times B^{n-k} y B^{n-k-|x|}\right) = P_{|x|^2}((x, y)).$$

Indeed, using the additivity of the Hamming distance and the $\#_x$ functions, for example,

$$d(x_1 \ldots x_k, y_1 \ldots y_k) = d(x_1 \ldots x_{k-1}, y_1 \ldots y_{k-1}) + d(x_k, y_k),$$

we have

$$\begin{aligned} P_{n^2}(B^{n-k} x B^{n-k-|x|} \times B^{n-k} y B^{n-k-|x|}) &= \sum_{a_1, a_2 \in B^{n-k}} \sum_{b_1, b_2 \in B^{n-k-|x|}} P_{n^2}((a_1 x b_1, a_2 y b_2)) \\ &= P_{|x|^2}((x, y)) \sum_{a_1, a_2 \in B^{n-k}} \sum_{b_1, b_2 \in B^{n-k-|x|}} P_{(n-|x|)^2}((a_1 b_1, a_2 b_2)) \\ &= P_{|x|^2}((x, y)) P_{(n-|x|)^2}\left(B^{n-|x|} \times B^{n-|x|}\right) \\ &= P_{|x|^2}((x, y)). \end{aligned}$$

As a direct consequence, we can deduce that the probability space P_{n^2} defined above is independent.

6.3. *XOR application*

We now consider the situation where the two output bitstrings x and y are `XOR`ed against each other (effectively using one as a one-time pad for the other) to produce a single bitstring, and we investigate the distribution of the resulting bitstring. Rather than just considering the effect of `XOR`ing paired (and potentially correlated) bits, we also consider `XOR`ing outcomes shifted by $j > 0$ bits, as described in Section 4.3.

For $j \geqslant 0$ and $x, y \in B^{n+j}$, we define the offset-`XOR` function

$$X_j : B^{n+j} \times B^{n+j} \to B^n$$

as

$$X_j(x, y) = z$$

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

where $z_i = x_i \oplus y_{i+j}$ for $i = 1, \ldots, n$. For $z \in B^n$, the set of pairs (x, y) that produce z when XORed with offset j is

$$\begin{aligned} A_j(z) &= \{(x, y) \mid x, y \in B^{n+j}, X_j(x, y) = z\} \\ &= \{(ua, b(u \text{ XOR } z) \mid u \in B^n, a, b \in B^j\}. \end{aligned}$$

The probability space of the output produced by the QRNG is $(B^n, 2^{B^n}, Q_{n,j})$, where

$$Q_{n,j} : 2^{B^n} \to [0, 1]$$

is defined for all $X \subseteq B^n$ by

$$Q_{n,j}(X) = \sum_{z \in X} P_{(n+j)^2}(A_j(z)). \tag{4}$$

We now note that $|A_j(z)| = 2^{n+2j}$ and check that this is a valid probability space. First,

$$Q_{n,j}(\varnothing) = 0,$$

is trivially true. Then, we have

$$\begin{aligned} Q_{n,j}(B^n) &= \sum_{z \in B^n} P_{(n+j)^2}(A_j(z)) \\ &= P_{(n+j)^2}\left(\bigcup_z A_j(z)\right) \\ &= P_{(n+j)^2}\left(B^{n+j} \times B^{n+j}\right) \\ &= 1 \end{aligned}$$

because all $A_j(z)$ are disjoint and thus

$$\left|\bigcup_z A_j(z)\right| = 2^n 2^{n+2j} = (2^{n+j})^2,$$

so

$$\bigcup_z A_j(z) = B^{n+j} \times B^{n+j},$$

and for disjoint $X, Y \subseteq B^n$, we have

$$Q_{n,j}(X \cup Y) = Q_{n,j}(X) + Q_{n,j}(Y).$$

We now explore the form of the XORed distribution $Q_{n,j}$ for $j = 0$ and $j > 0$.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

Let $z \in B^n$ and $j \geqslant 0$. We use $z[m,k]$ to denote the substring $z_m \ldots z_k, 1 \leqslant m \leqslant k \leqslant n$. We have

$$\begin{aligned} Q_{n,j}(z) &= P_{(n+j)^2}(A_j(z))) \\ &= \sum_{a,b\in 2^j} \sum_{u\in 2^n} P_{(n+j)^2}((ua, b(u \texttt{ XOR } z)) \\ &= \sum_{u\in 2^n} P_{(n-j)^2}\left((u[j+1,n], (u \texttt{ XOR } z)[1,n-j])\right) \\ &\quad \cdot \sum_{a\in 2^j} P_{j^2}\left((a, (u \texttt{ XOR } z)[n-j+1,n])\right) \sum_{b\in 2^j} P_{j^2}\left((u[1,j], b)\right). \end{aligned}$$

Note that for $j = 0$, we have $d(u, u \texttt{ XOR } z) = \#_1(z)$, and thus

$$\begin{aligned} Q_{n,0}(z) &= \sum_{u\in 2^n} P_{n^2}\left((u, (u \texttt{ XOR } z))\right) \\ &= \frac{1}{Z_n}(\sin^2\theta)^{\#_1(z)}(\cos^2\theta)^{\#_0(z)} \sum_{u\in B^n} (e_0^{\oplus})^{\#_0(u)}(e_1^{\oplus})^{\#_1(u)}(e_0^{\otimes})^{\#_0(u \texttt{ XOR } z)}(e_1^{\otimes})^{\#_1(u \texttt{ XOR } z)} \\ &= \frac{1}{Z_n}\left(\sin^2\theta(e_0^{\oplus}e_1^{\otimes} + e_1^{\oplus}e_0^{\otimes})\right)^{\#_1(z)} \left(\cos^2\theta\left(e_0^{\oplus}e_0^{\otimes} + e_1^{\oplus}e_1^{\otimes}\right)\right)^{\#_0(z)}. \end{aligned}$$

We can recognise this as a constantly biased source where

$$\begin{aligned} p_0 &= \cos^2\theta\left(e_0^{\oplus}e_0^{\otimes} + e_1^{\oplus}e_1^{\otimes}\right)/Z_1 \\ p_1 &= \sin^2\theta\left(e_0^{\oplus}e_1^{\otimes} + e_1^{\oplus}e_0^{\otimes}\right)/Z_1. \end{aligned}$$

It is interesting to compare the form of $Q_{n,0}$ with the distribution of the constantly biased source Equation (3) by discarding one output string – the former is more sensitive to misalignment and the latter to differences in detection efficiencies. In the case of perfect/equal detector efficiencies (but non-perfect misalignment), discarding one string produces uniformly distributed bitstrings, whereas XORing does not.

We now look at the case where $j > 0$. For the ideal situation of $\theta = \pi/4$, we have the same result as for the $j = 0$ case, and if we have equal detector efficiencies, we get the uniform distribution. We can show this as follows (note that $Z_{n+j} = 2^{n+j}$ in this case):

$$\begin{aligned} Q_{n,j}(z) &= 2^{-n-j} \sum_{u_n\in B} \cdots \sum_{u_{n-j}\in B} (\sin^2\theta)^{u_n\oplus z_{n-j}\oplus u_{n-j}}(\cos^2\theta)^{1-u_n\oplus z_{n-j}\oplus u_{n-j}} \cdots \\ &\quad \times \sum_{u_1\in B} (\sin^2\theta)^{u_j+1\oplus z_1\oplus u_1}(\cos^2\theta)^{1-u_j+1\oplus z_1\oplus u_1} \\ &= 2^{-n-j} \sum_{u_n\in B} \cdots \sum_{u_{n-j}\in B} (\sin^2\theta + \cos^2\theta) \cdot \sum_{u_1\in B} (\sin^2\theta + \cos^2\theta) \\ &= 2^{-n-j} \sum_{u_{n-j+1}\ldots u_n\in B^j} 1 \\ &= 2^{-n}. \end{aligned}$$

However, in the more general case of non-equal detector efficiencies, the distribution is no longer independent, although, in general, it is much closer to the uniform distribution than

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

Table 3. *Empirical evidence for the quality of* XORing *with* $j > 0$ *compared with* $j = 0$ *and configuration settings of* $\theta = \pi/5$, $e_0^{\oplus} = 0.30$, $e_1^{\oplus} = 0.33$, $e_0^{\otimes} = 0.29$, $e_1^{\otimes} = 0.30$ – *this is probably much worse (that is, further from the ideal case) than one would expect in an experimental setup. The (small) value of* $n = 10$ *has been used since, unfortunately, the distribution is very costly to calculate numerically. Here* $bin(m)$ *denotes the (10-bit zero-extended) binary representation of m. For example,* $bin(1) = 0000000001$, $bin(2) = 0000000010$, *and so on.*

x	bin(174)	bin(487)	bin(973)
$Q_{10,0}(x)$	5.90×10^{-4}	9.70×10^{-4}	1.64×10^{-4}
$Q_{10,1}(x)$	9.75×10^{-4}	9.71×10^{-4}	9.71×10^{-4}
$Q_{10,2}(x)$	9.78×10^{-4}	9.70×10^{-4}	9.70×10^{-4}
$U_{10}(x)$	9.77×10^{-4}	9.77×10^{-4}	9.77×10^{-4}

Table 4. *The variation from the uniform distribution of the distributions* $Q_{10,j}$ *using the same parameters as in Table 3.*

$\Delta(Q_{10,0}, U_{10})$	0.770271
$\Delta(Q_{10,1}, U_{10})$	0.00441399
$\Delta(Q_{10,1}, U_{10})$	0.00440061

the $j = 0$ case. (Recall that independence is a sufficient but not necessary condition for a uniform distribution (Abbott and Calude 2012).) It is indeed this 'closeness' (the total variation distance given by $\Delta(U_n, Q_{n,j}) = \frac{1}{2}\sum_{x \in B^n} |2^{-n} - Q_{n,j}(x)|$) that is the important quantity (U_n is the uniform distribution on n-bit strings). However, since $Q_{n,j}$ for $j > 0$ is not independent, von Neumann normalisation cannot be applied to guarantee the uniform distribution; indeed, the dependence is not even bounded to a fixed number of preceding bits.

6.4. *Criticisms and alternative operationalisations*

Given the analysis above, we could ask why we should not simply discard one string to give the distribution in Equation (3), and then apply von Neumann normalisation to obtain uniformly distributed bitstrings. There are two main reasons for giving the answer no to this question:

(i) As discussed above, the effect of drift in bias and temporal correlations will ensure that this method will not produce the uniform distribution anyway. Indeed, the distribution $Q_{n,j}$ for $j > 0$ should be more robust to those effects: for example, $Q_{n,j}$ is less sensitive to detector bias than the distribution in Equation (3). It is extremely plausible that, in practice, $Q_{n,j}$ would give as good results as discarding one string; indeed, it is very close to the uniform distribution, as can be seen from Table 4 and Figure 3. To compare the distributions properly, the following *open question* must be answered: what is the bound ρ depending on $e_x^{\oplus}, e_y^{\otimes}$ and θ such that $\Delta(U_n, Q_{n,j}) \leqslant \rho$, and how

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

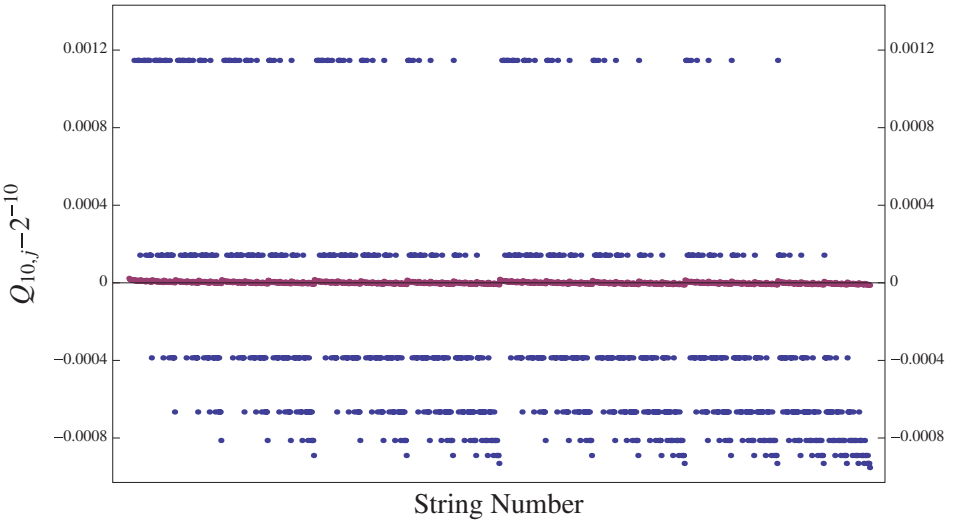


Fig. 3. (Colour online) A plot of $Q_{10,j} - 2^{-10}$ for each of the 2^{10} strings of length 10. The two cases $j = 0$ (blue) and $j = 1$ (red) show how much closer the probabilities given by $Q_{10,1}$ are to that expected from the uniform distribution than for $Q_{10,0}$. The same experimental configuration as in Table 4 has been used.

does that compare to that given in Abbott and Calude (2012) for normalisation of a source with varying bias?

Furthermore, $Q_{n,j}$ produces bitstrings of length n, whereas applying von Neumann to a single string produces a string with expected length at most $n/4$ bits. This is a significant increase in efficiency, making the shifted `XOR`ing process extremely appealing for a high bitrate, un-normalised QRNG. Even the $j = 0$ case with von Neumann applied after `XOR`ing would often be preferable to discarding one string since it is less sensitive to detector efficiency (the hardware limit) and more sensitive to to misalignment (which is controlled by the experimenter).

(ii) If we insist on a perfect theoretical distribution in the presence of non-ideal misalignment and unequal detector efficiencies, or perhaps, if the $Q_{n,j}$ distribution is not sufficient for particular requirements, we can still operationalise both strings to improve the efficiency of the QRNG over discarding a single string by a simple modification of von Neumann's procedure. To do this, note that the pair of pairs (a_1a_2, b_1b_2) have the same probability as the pairs (a_2a_1, b_2b_1). By mapping those with $a_1b_1 < a_2b_2$ (lexicographically) to 0 and those with $a_1b_1 > a_2b_2$ to 1, and discarding those with $a_1b_1 = a_2b_2$, we will obtain the uniform distribution in the same way as for von Neumann's procedure. The key advantage is that this will produce strings of expected length up to $3n/8$ while maintaining the desired property of sampling from the uniform distribution.

The problem of determining how best to obtain the maximum amount of information from the QRNG is largely a problem of randomness extractors (Gabizon 2010), and is a trade off between the number of uniformly distributed bits obtained and the processing

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

cost – a suitable extractor needs to operate in real-time for most purposes. As we have seen, the fact that two (potentially correlated) bitstrings are obtained allows more efficient operation than a QRNG using single-photons. We have shown how the proposed QRNG can be operationalised in more than one way: either by using shifted XORing of bits to sample from a distribution that is close to (in the ideal limit, equal to) the uniform distribution, and efficient and robust to various errors, or by using both produced bitstrings to allow a more efficient normalisation procedure giving (in the absence of the aforementioned temporal effects) the uniform distribution. Undoubtedly, many other operationalisations are possible.

7. Summary

Every QRNG claiming to produce a better form of randomness than pseudo-randomness must first be certified by some physical law implying the incomputability of the output bitstrings; value indefiniteness is one example. Most existing QRNG proposals are based on single beam splitters and work in a dimension-two Hilbert space, so they cannot be certified by value indefiniteness given by the Kochen–Specker theorem (which only holds in a Hilbert space of dimension greater than 2). In this paper, we have proposed a QRNG that uses an entangled photon singlet-state in four-dimensional Hilbert space and is certified by value indefiniteness, which implies strong incomputability, which is the mathematical property corresponding to physical indeterminism. While this is an ingredient of fundamental importance in any reasonable QRNG, we have recognised that experimental imperfections will always prevent the QRNG from producing the theoretical uniform probability distribution exactly, which is another essential symptom of randomness (independent of incomputability). We have discussed the form and effects of the possible experimental errors, and taken care to make the proposed QRNG robust to these effects.

Since this QRNG produces two bitstrings, we have proposed XORing the bitstrings produced, using one as a one-time pad for the other, to get better protection against experimental imperfections (in particuar, non-ideal misalignment and unequal detector efficiencies), and to use the advantages provided by two strings compared with just using one. Rather than XORing corresponding bits, bits x_i and y_{i+j} are XORed (for fixed $j > 0$) since this not only provides much better results but also mitigates the effects of temporal correlations between adjacent bits. Furthermore, we have proposed an alternative normalisation method based on von Neumann's procedure that uses both bitstrings. This procedure is significantly more efficient, but still guarantees uniformly distributed strings in the presence of non-ideal misalignment and unequal detector efficiencies. We leave as an *open question* the problem of improving on the time-shifted XOR method and finding a technique for extracting bits that are provably uniformly distributed and is more efficient than the improved von Neumann method discussed in this paper.

An analysis of the sequences generated by the proposed QRNG should be carried out using the knowledge of the expected uniform distribution, as in Calude *et al.* (2010). In particular, the quality of both of the individual strings produced should be compared with

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

that of the XORed sequence, both with and without von Neumann normalisation applied, as well as with the sequence produced by our improved von Neumann method.

Furthermore, in view of the possible temporal correlations between bits, the quality of the random bits should be tested as j is varied in Equation (4). Since this has little effect on the bias of the resulting string (and normalisation can subsequently remove this), it would allow investigation of the effect and significance of the possible temporal correlations.

The proposed QRNG produces bits that are certified through value indefiniteness and, based on our theoretical analysis, should be distributed more uniformly than those produced by existing QRNGs based on beam splitters. It will be interesting to carry out experimental tests of the quality of bits produced using this method compared with existing classical and quantum sources of randomness.

Note added in proof

It has recently come to our attention that the Quantis device '[does not] use the Von Neumann unbiasing technique' (email sent to Abbott on 19 July 2013 by Grégoire Ribordy on behalf of id Quantique).

Although Quantis uses normalisation, we have been unable to determine the normalisation technique. However, our results are unaffected by this fact.

Acknowledgments

We are grateful to A. Cabello, G. Longo and A. Zeilinger for many interesting discussions on the subject of quantum randomness.

References

Abbott, A. A. and Calude, C. S. (2012) Von Neumann normalisation of a quantum random number generator. *Computability* **1** 59–83.

Abbott, A. A., Calude, C. S., Conder, J. and Svozil, K. (2012) Strong Kochen–Specker theorem and incomputability of quantum randomness. *Physical Review A* **86** (6) 062109.

Bechmann-Pasquinucci, H. and Peres, A. (2000) Quantum cryptography with 3-state systems. *Physical Review Letters* **85** (15) 3313–3316.

Berry, D. W., Jeong, H., Stobińska, M. and Ralph, T. C. (2010) Fair-sampling assumption is not necessary for testing local realism. *Physical Review A* **81** (1) 012109.

Billingsley, P. (1979) *Probability and Measure*, John Wiley and Sons.

Blum, M. (1986) Independent unbiased coin flips from a correlated biased source: a finite state Markov chain. *Combinatorica* **6** (2) 97–108.

Born, M. (1969) *Physics in My Generation*, second edition, Springer.

Cabello, A. (2008) Experimentally testable state-independent quantum contextuality. *Physical Review Letters* **101** (21) 210401.

Calude, C. S. (2002) *Information and Randomness – An Algorithmic Perspective*, second edition, Springer.

Calude, C. S., Dinneen, M. J., Dumitrescu, M. and Svozil, K. (2010) Experimental evidence of quantum randomness incomputability. *Physical Review A* **82** (2) 022102.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

Calude, C. S. and Svozil, K. (2008) Quantum randomness and value indefiniteness. *Advanced Science Letters* **1** (2) 165–168.

Chaitin, G. J. (1977) Algorithmic information theory. *IBM Journal of Research and Development* **21** 350–359, 496. (Reprinted in Chaitin, G. J. (1990) *Information, Randomness and Incompleteness*, second edition, World Scientific.)

Clauser, J. F. and Shimony, A. (1978) Bell's theorem: experimental tests and implications. *Reports on Progress in Physics* **41** 1881–1926.

Ekert, A. K. (1991) Quantum cryptography based on Bell's theorem. *Physical Review Letters* **67** 661–663.

Fiorentino, M., Santori, C., Spillane, S. M., Beausoleil, R. G. and Munro, W. J. (2007) Secure self-calibrating quantum random-bit generator. *Physical Review A* **75** (3) 032334.

Gabizon, A. (2010) *Deterministic Extraction from Weak Random Sources*, Springer.

Garg, A. and Mermin, D. N. (1987) Detector inefficiencies in the Einstein–Podolsky–Rosen experiment. *Physical Review D* **35** (12) 3831–3835.

Garrison, J. C. and Chiao, R. Y. (2008) *Quantum Optics*, Oxford University Press.

Hai-Qiang, M. *et al.* (2004) A random number generator based on quantum entangled photon pairs. *Chinese Physics Letters* **21** (10) 1961–1964.

Huang, Y.-F., Li, C.-F., Zhang, Y.-S., Pan, J.-W. and Guo, G.-C. (2003) Experimental test of the Kochen–Specker theorem with single photons. *Physical Review Letters* **90** (25) 250401.

Jennewein, T. (2009) Private communication to authors.

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

Kochen, S. and Specker, E. P. (1967) The problem of hidden variables in quantum mechanics. *Journal of Mathematics and Mechanics* (now *Indiana University Mathematics Journal*) **17** (1) 59–87. (Reprinted in Specker, E. P. (1970) *Selecta*, Birkhäuser 235–263.)

Larsson, J.-A. (1998) Bell's inequality and detector inefficiency. *Physical Review A* **57** (5) 3304–3308.

Lindner, F. *et al.* (2005) Attosecond double-slit experiment. *Physical Review Letters* **95** (4) 040401.

Merali, Z. (2010) A truth test for randomness. *Nature News* (Published online 14 April 2010 – Nature – doi:10.1038/news.2010.181.)

Pan, J.-W., Bouwmeester, D., Daniell, M., Weinfurter, H. and Zeilinger, A. (2000) Experimental test of quantum nonlocality in three-photon Greenberger–Horne–Zeilinger entanglement. *Nature* **403** 515–519.

Pauli, W. (1958) Die allgemeinen Prinzipien der Wellenmechanik. In: Flügge, S. (ed.) *Handbuch der Physik. Band V, Teil 1. Prinzipien der Quantentheorie I*, Springer 1–168.

Pearle, P. M. (1970) Hidden-variable example based upon data rejection. *Physical Review D* **2** (8) 1418–1425.

Peres, A. (1978) Unperformed experiments have no results. *American Journal of Physics* **46** 745–747.

Peres, Y. (1992) Iterating von Neumann's procedure for extracting random bits. *Annals of Statistics* **20** (1) 590–597.

Pironio, S. *et al.* (2010) Random numbers certified by Bell's theorem. *Nature* **464** 1021–1024.

Rarity, J. G., Owens, M. P. C. and Tapster, P. R. (1994) Quantum random-number generation and key sharing. *Journal of Modern Optics* **41** 2435–2444.

Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L. and Zbinden, H. (2000) Optical quantum random number generator. *Journal of Modern Optics* **47** 595–598.

Svozil, K. (1990) The quantum coin toss – testing microphysical undecidability. *Physics Letters A* **143** 433–437.

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press

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

Svozil, K. (2011) Quantum value indefiniteness. *Natural Computing* **10** (4) pp 1371–1382.

Von Neumann, J. (1951) Various techniques used in connection with random digits. *National Bureau of Standards Applied Math Series* **12** 36–38. (Reprinted in Traub, A. H. (ed.) *John von Neumann, Collected Works, (Vol. V)*, MacMillan 768–770.)

Wang, P. X., Long, G. L. and Li, Y. S. (2006) Scheme for a quantum random number generator. *Journal of Applied Physics* **100** (5) 056107.

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

https://doi.org/10.1017/S0960129512000692 Published online by Cambridge University Press