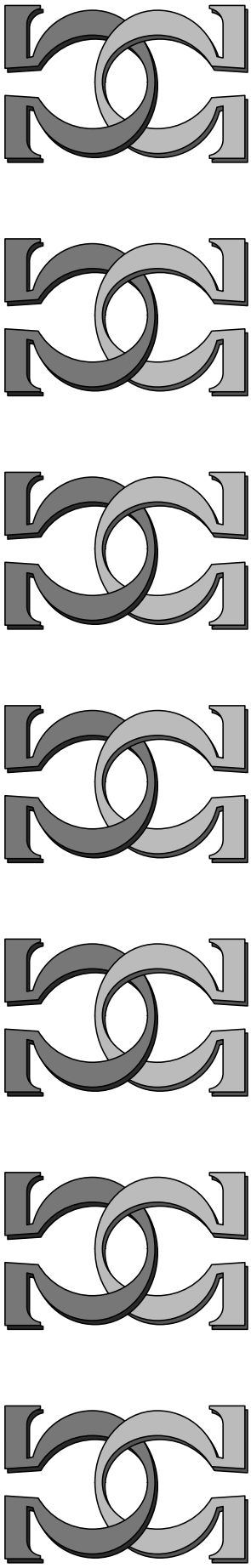

CDMTCS
Research
Report
Series

A Quantum Random Number Generator Certified by Value Indefiniteness

Alastair A. Abbott[1], Cristian S. Calude[1], Karl Svozil[2]

[1]University of Auckland, NZ
[2]Vienna University of Technology, Austria

CDMTCS-396
December 2010

Centre for Discrete Mathematics and
Theoretical Computer Science

Under consideration for publication in Math. Struct. in Comp. Science

A Quantum Random Number Generator Certified by Value Indefiniteness

ALASTAIR A. ABBOTT[1], CRISTIAN S. CALUDE[1] and KARL SVOZIL[2]

[1] *Department of Computer Science, University of Auckland,*
Private Bag 92019, Auckland, New Zealand
Email: aabb009@aucklanduni.ac.nz, cristian@cs.auckland.ac.nz
[2] *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) which utilises 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 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 produced can be classically computed (reproduced and validated), the mathematical form of bitwise physical unpredictability.
The effects of various experimental imperfections are discussed in detail, particularly those related to detector efficiencies, context alignment and temporal correlations between bits. The analysis is to a large extent relevant for the construction of any QRNG based on beam-splitters. By measuring the two entangled photons in maximally misaligned contexts and utilising the fact that two rather than one bitstring are obtained, more efficient and robust unbiasing techniques can be applied. A robust and efficient procedure based on XORing the bitstrings together—essentially using one as a one-time-pad for the other—is proposed 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. Some open problems are also discussed.

1. Introduction

Random numbers have been around for more than 4,000 years, but never have they been in such demand as in our time. People use random numbers everywhere. Thereby, randomness is understood through various "symptoms." Here are three of the largely accepted ones:

(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.
(iii)Typicalness: Random sequences pass every statistical test of randomness.

Can our intuition on randomness be cast in more rigorous terms? Randomness plays an essential role in probability theory, 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, not defined or deduced.

Algorithmic information theory (AIT) (Chaitin 1977), developed in the 1960s, defines and studies individual random objects, like 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 mathematically proved: one can never be sure a sequence is random, there are only forms and degrees of randomness.

Computers produce "random numbers" generated by algorithms. Computer scientists needed a long time to realize that randomness produced by software is far from being random. This form of randomness—known as pseudo-randomness—mimics well the human perception of randomness, but its quality is rather low because computability destroys many symptoms of randomness, e.g. unpredictability. It is not totally unreasonable to put forward that pseudo-randomness rather reflects its creators' subjective "understanding" and "projection" of randomness [†]. And although no computer or software manufacturer claims that their products can generate truly random numbers, recently such formally unfounded claims have re-appeared for randomness produced with physical experiments suggesting that "truly random numbers have been generated at last" (Haahr 2010; Merali 2010).

2. Quantum Randomness

2.1. *Theoretical claims to quantum randomness*

Quantum mechanics has a credible claim to be one of (if not) the best sources of randomness. There are many quantum phenomena which can be used for random number generation: nuclear decay radiation sources, the quantum mechanical noise in electronic circuits (known as shot noise), or photons traveling 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? Besides quantum complementarity (Pauli 1958) (i.e. 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: value definiteness (the fact that

[†] 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 too often for its own sake 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 are more chances that the coin will land on heads at the next flip.

there can, in general, be no co- or pre-existing definite values prescribable to certain sets of measurement outcomes (Calude and Svozil 2008; Svozil 2010)) and 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 (i.e., an experiment in which the Kochen-Specker theorem guarantees value indefiniteness) generates an *infinite (strongly) incomputable sequence of bits*: every Turing machine can reproduce exactly only finitely many scattered digits of such an infinite sequence, i.e. the sequence is bi-immune (Calude and Svozil 2008). Such certification, as has already previously been pointed out (Calude and Svozil 2008), is based on the assumptions that there are no contextual hidden variables and that the uniformity and symmetry of the Kochen-Specker construction allows us to conclude strong value indefiniteness—that all observables are, in fact, value indefinite (except those which the state is in an eigenstate of). Actually, a stronger statement is true: no Turing machine can be proved to reproduce exactly any digit of such an infinite sequence, i.e. it is Solovay bi-immune (Abbott et al. 2010). Indeed, if the value of a bit could be computed before measurement then we could assign a definite value to the observable, 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 which corresponds to the physical notion of indeterminism in quantum mechanics—the inability *even in principle* to predict the outcome of certain quantum measurements—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 the Zeilinger group in Innsbruck and Vienna (Jennewein et al. 2000) and applied for the sake of violation of Bell's inequality under strict Einstein locality conditions (two space-like separated events cannot influence each other in any way) (Weihs et al. 1998).

The Gisin group in Geneva (Stefanov et al. 2000), and in particular its spin-off *id Quantique*, produces and markets a commercial device called *Quantis* (ID Quantique SA 2010). In order to eliminate bias, the device employs von Neumann normalisation (actually a more efficient iterated version due to Peres (1992) is used) which requires the *independence* of individual events: bits are grouped into pairs, equal pairs (00 or 11) are discarded and we replace 01 with 0 and 10 with 1 (Von Neumann 1951).

A group in Shanghai and Beijing (Wang et al. 2006) has utilised a Fresnel multiple prism as polarising beam splitter. As a normalisation technique, previously generated experimental sequences have been used as 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), who utilised spontaneous parametric down-conversion to produce entangled pairs of photons. One of the photons has been used as trigger, mostly to allow a faster data production rate by eliminating double counts. Again, von Neumann normalisation has been applied in an attempt to eliminate bias.

A group from the Hewlett-Packard Laboratories in Palo Alto and Bristol (Fiorentino et al. 2007) 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 contains also V_1V_2 as well as 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 have been mapped into 0 and 1, respectively. Thereby, as the authors have 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 rendition of a QRNG (Pironio et al. 2010), although not based on photons and beamsplitters, utilises 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 strong value indefiniteness), but falls short of providing certification of strong incomputability *via* value indefiniteness (Calude and Svozil 2008; Svozil 2009). With regard to value indefiniteness, the difference between Boole-Bell-type inequalities *versus* Kochen-Specker-type theorems is this: In the Boole-Bell-type case, the breach of value indefiniteness needs not happen at every single particle, whereas in the Kochen-Specker-type case this must happen *for every particle* (Svozil 2010). Pointedly 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, one could potentially produce sequences containing infinite computable subsequences "protected" by Boole-Bell-type violations. Further, given that such criticisms seem also 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, preferably a strongly incomputable one. Do the current proposals of QRNGs generate "in principle" strongly incomputable sequences of quantum random bits? To answer this question one has to check whether the QRNG is "protected" by value indefiniteness, the only physical principle currently known to guarantee incomputability; in most cases the answer is either negative or cannot be verified because of lack of information about the mechanism of the QRNG.

In Calude et al. (2010) tests based on algorithmic information theory were used 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 (ID Quantique SA 2010) 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. No distribution was assumed for any of the sources, yet 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), although the converse is not true. Indeed, the tests found the quantum sources to be less normal than the pseudo-random ones. Is this a property of quantum randomness, or evidence of flaws in the tested QRNGs?

In Abbott and Calude (2010) the probability distribution for an ideal QRNG was discussed: not surprisingly, 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. Further, weaker evidence

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	$\mathbf{< 10^{-10}}$	$\mathbf{< 10^{-10}}$	$\mathbf{< 10^{-10}}$	$\mathbf{< 10^{-10}}$

suggests the pseudo-random sources of randomness—Mathematica and Maple—are, on the contrary, too normal. The results of the analysis are presented in Table 2.2.

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 has been achieved (perhaps through experimental feedback control) at the sacrifice of the performance at the $k \geq 2$ level, a property much harder to control without post-processing. The *Quantis* QRNG uses iterated 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 non-independence of successive bits (Abbott and Calude 2010).

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 remove bias, but to have the desired effect assumptions about independence and constancy of bias must be satisfied (Abbott and Calude 2010). While experiments will never realize the ideal QRNG, one needs to be aware of how much affect experimental imperfections have. Any credible QRNG should take these issues into account, as well as the need of explicit certification of randomness by some physical law, e.g. value indefiniteness.

3. The scheme under ideal conditions

In what follows, a proposal for a QRNG depicted in Fig. 1, previously put forward in Svozil (2009), will be discussed in detail. It utilises the singlet state of two two-state particles (e.g., photons of 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 more than one photons are rarely 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 nonlinear medium). The two resulting entangled photons are then analysed with respect to their linear polarisation state at some directions which are $\pi/4$ radians "apart," symbolised by "$\oplus$" and "$\otimes$," respectively.

Due to the required four-dimensional Hilbert space, this QRNG is "protected" by Bell- as well as Kochen-Specker- and Greenberger-Horne-Zeilinger-type value indefiniteness [‡]. The protocol

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

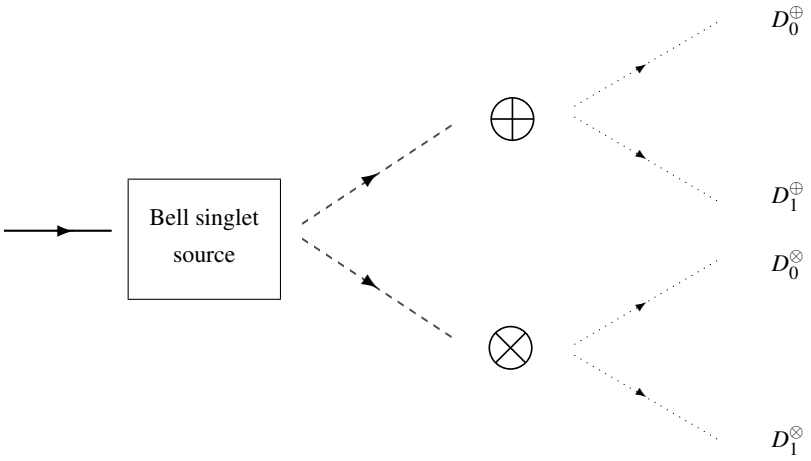

Fig. 1. Scheme of a quantum random number generator (Svozil 2009).

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

utilises all three principal types of quantum indeterminism: (i) the indeterminacy of individual outcomes of single events as proposed by Born and Dirac; (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 & Specker, and Greenberger, Horne & Zeilinger.

This, essentially, is the same experimental configuration as the one used for a measurement of the correlation function at the 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 via addition modulo 2.

Formally, 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 their parity, or to the addition modulo 2 according to Table 3 (in what follows, depending on the formal context, XOR refers to either a binary function of two binary observables, or to the logical operation). Stated differently, one outcome is used as a *one time pad* to "encrypt" the other outcome, and *vice versa*. As a result, one obtains a sequence $x = x_1 x_2 \ldots x_n$ with

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

For the XORd sequence to still be certifiably incomputable (via value indefiniteness), one must prove this certification is preserved under XORing—indeed 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 $n \geq 3$. 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 one cannot claim to produce truly indeterministic bits. In general incomputability itself is not preserved by f; however by consideration of the value indefiniteness of the source the certification can be seen to hold under `XOR` as well as when discarding bits (Abbott et al. 2010).

4. "Random" errors or systematic errors

In what follows we shall discuss possible "random" (no pun) or systematic errors in experimental realisations of this QRNG (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 (e.g. by value indefiniteness), take into account the nature of these errors and be carefully designed (along with any subsequent post-processing) so that the resultant distribution of bitstrings the QRNG samples from is as close as possible to the expected uniform distribution (Abbott and Calude 2010). 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 conceivable 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 seems to be no 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 last property is mathematically modelled by strong incomputability (Calude and Svozil 2008; Abbott et al. 2010)). If, however, events are not independent then more care is needed. However, correlation between events is an undesirable property in itself, and as long as care is made, 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 exactly a singlet. This may give rise to a systematic bias of the combined light source-analyser setup in a very similar way as for beam splitters.

4.3. *Non-alignment of polarisation measurement angles*

No experimental realisation will attain a "perfect anti-alignment" of the polarisation analysers at angles $\pi/4$ radians apart. Only in this ideal case are the bases conjugate and the correlation function will be exactly zero. Indeed, "tuning" the angle to obtain equi-balanced sequences of

zeroes and ones may be a method to properly anti-align the polarisers. However, one has to keep in mind that any such "tampering" with the raw sequence of data to achieve Borel normality (e.g. by readjustments of the experimental setup) may introduce unwanted (temporal) correlations or other bias (Calude et al. 2010).

Incidentally, the angle $\pi/4$ is one of the three points at angles 0, $\pi/4$ and $\pi/2$ in the interval $[0,\pi/2]$ in which the classical and quantum correlation functions coincide. For all other angles, there is a higher ratio of different or identical pairs than could 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 *i*th experiment, over a "large number" of experiments; i.e.,

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

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 $E^{\mathrm{cl}}_{\texttt{XOR}}(\theta) = 1 - 2\theta/\pi$, and the quantum expectation function $E_{\texttt{XOR}}(\theta) = (1/2)(1+\cos 2\theta)$.

Thus, for angles "far apart" 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,* as the entangled particles are more correlated and thus "less independent." Potentially, this could be utilised to ensure a $\pi/4$ mismatch more accurately than possible through classical means. This will be discussed in section 5 below.

In order to avoid this negative feature while generating bits, instead of XORing outcomes of *identical* partner pairs, one could XOR time-shifted outcomes; e.g., instead of the expression in Eq. (1) one may consider

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

One should make j large enough so that, taking in to account double counting, there is no chance of accidentally causing two offset but correlated outcomes to be XOR'd together. Theoretical analysis of the effects of experimental imperfections and the XOR operation are discussed later in the paper, and XORing shifted pairs is an efficient and effective procedure for reducing such errors.

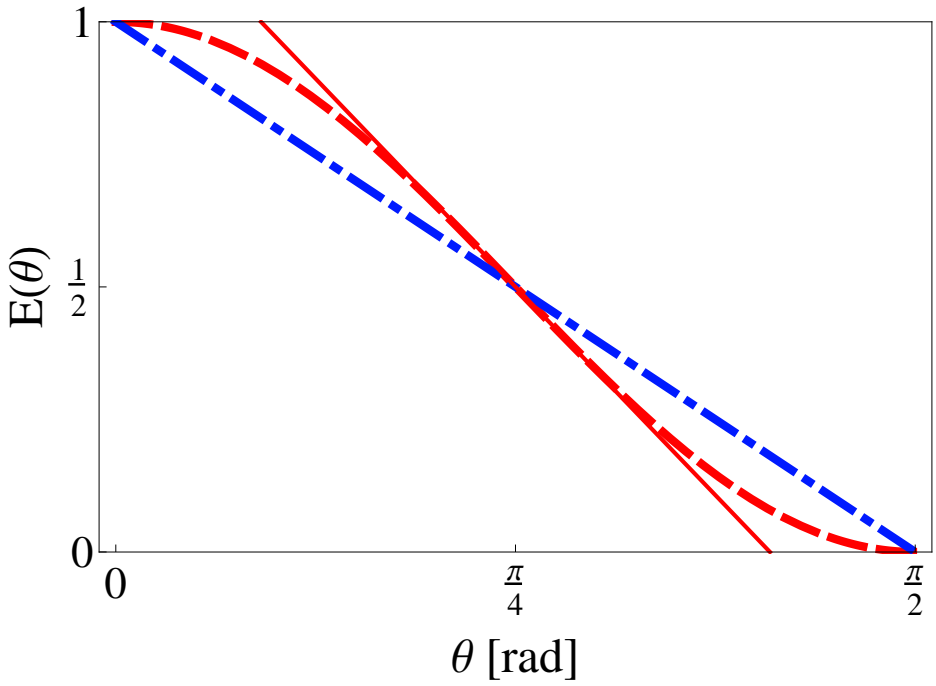

Fig. 2. (Color online) The classical and quantum expectation functions and the linear quantum approximation around $\pi/4$.

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 polarisation context. Suppose that 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 to find 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 $p_{H_2} \neq p_{V_2}$ then the resulting `XOR`'d sequence is biased. The two obtained sequences could be unbiased before or after `XOR`ing by the von Neumann method (Von Neumann 1951, p. 768), although any temporal correlations would violate the condition of independence required by this method. One should keep in mind, however, that the von Neumann normalisation procedure necessarily discards many bits (more efficient methods exist (Peres 1992)). The efficiency can be increased by utilising 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 but instead will simply be less biased (Abbott and Calude 2010). It is difficult to overcome this, as experimental instability is inevitable. However, bounds on the bias of the normalised sequence based on reasonable experi-

mental parameters (Abbott and Calude 2010) can be used to determine the length for which the source samples "closely enough" from the uniform distribution.

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 XOR'd bitstring is advantageous compared working with a single bitstring from a source of varying bias.

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

Due to the Hanbury-Brown-Twiss effect, the photons may be temporally correlated and thus arrive clustered or "bunched." Temporal correlations appear also at "double-slit analogous experiments" in the time domain (Lindner et al. 2005), in which the role of the slits is played by windows in time of attosecond duration. This can, to an extent, be avoided by ensuring 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 once is potentially of sufficient importance, this effect needs further careful consideration.

Another conceivable source of temporal correlations is due to the detector dead-time, T_d, during which the detector is inactive after 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, significantly increasing the chance of detecting a photon at the other detector during this time, obtaining a 1. This leads to higher than expected chances of 01 and 10 being measured. This is problematic as 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 from the previous measurement.

In view of conceivable temporal correlations, it would be interesting to test the quality of the random signal as j is varied in Eq. (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 then unbiasing techniques such as that proposed by Blum (1986) could be used instead of von Neumann's procedure. It seems desirable and simpler to avoid temporal correlations with carefully designed experimental methodology as opposed to post-processing where possible.

4.7. *Fair sampling*

As in 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 let us consider the extreme case that the detection efficiency is less that 50%; our supposed demon could reject all bits detected as 0 and 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 $(1/(1-\rho))$'th bit is a zero; this would introduce an infinite computable subsequence, a property violating 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 operationalization of spatial orthogonality

As has already been pointed out, for no temporal offset and in the regime of relative spatial angles around $\pi/4$ — i.e., at almost half orthogonal measurement directions — the classical linear expectation function $E^{\mathrm{cl}}_{\mathtt{XOR}}(\theta) = 1 - 2\theta/\pi$, for $0 < \theta < \pi/4$ is strictly *smaller*, and for $\pi/4 < \theta < \pi/2$ is 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 by 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 Fig. 2).

Phenomenologically this indicates less-than-classical numbers of equal pairs of outcomes "0–0" as well as "1–1," and more-than-classical non-equal pairs of outcomes "0–1" as well as "1–0," respectively, for the quantum case in the region $0 < \theta < \pi/4$; as well as the reverse behaviour in the region $\pi/4 < \theta < \pi/2$. This in turn results in "less zeroes" and "more ones" of the resulting sequence obtained by XORing the pairs of outcomes in the region $0 < \theta < \pi/4$, as well as in "more zeroes" and "less ones" in the region $\pi/4 < \theta < \pi/2$ as compared to 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 quickly quantum mechanically than classically.

This effect could in principle be used to operationalize 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.

6. Theoretical analysis on generated bitstrings

Here 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 Fig. 1 for the setup, we write the generated Bell singlet state with respect the top ("$\oplus$") 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 ("$\otimes$") polariser is at an angle of 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, i.e $e_x^{\oplus} = e_y^{\otimes}$, 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, 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, i.e 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 $X \subseteq B^n \times B^n$ as follows:

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

and the term

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

ensures normalisation.

We can check easily that this is indeed a valid probability space (i.e. that is 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

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

vary in each detector, this is not, in general, the case. For every bitstring $x \in B^n$ we have

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

We see that each bitstring taken separately appears to come from a constantly biased source where the probabilities that a bit is 0 or 1, p_0, p_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 alternatively be viewed as the distribution obtained if we were to discard one bitstring after measurement. Note that if either $e_0^{\otimes} = e_1^{\otimes}$ or we have perfect misalignment (i.e. $\theta = \pi/4$) then the probabilities have the simpler formulae:

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

In this case, if we further 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 $P_{n^2}(B^n \times \{y\})$ also holds.

6.2. *Independence of the QRNG probability space*

If we were to discard one bitstring it is clear 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 2010). However, we would like to extend our notion of independence defined Abbott and Calude (2010) 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 $1 \leq k \leq n$ and $x_1, \ldots, x_k, y_1, \ldots, y_k \in B$ we have

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

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

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

Indeed, using the additivity of the Hamming distance and the $\#_x$ functions, e.g.

$d(x_1 \dots x_k, y_1 \dots y_k) = d(x_1 \dots x_{k-1}, y_1 \dots y_{k-1}) + d(x_k, y_k)$, we have:

$$\begin{aligned} P_{n^2}(B^{n-k}xB^{n-k-|x|} \times B^{n-k}yB^{n-k-|x|}) &= \sum_{a_1,a_2 \in B^{n-k}} \sum_{b_1,b_2 \in B^{n-k-|x|}} P_{n^2}\left((a_1xb_1, a_2yb_2)\right) \\ &= P_{|x|^2}((x,y)) \sum_{a_1,a_2 \in B^{n-k}} \sum_{b_1,b_2 \in B^{n-k-|x|}} P_{(n-|x|)^2}\left((a_1b_1, a_2b_2)\right) \\ &= P_{|x|^2}((x,y)) P_{(n-|x|)^2}(B^{n-|x|} \times B^{n-|x|}) \\ &= P_{|x|^2}((x,y)). \end{aligned}$$

As a direct consequence we 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'd 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 only considering the effect of XORing paired (and potentially correlated) bits, we also consider XORing outcomes shifted by $j > 0$ bits as described in Section 4.3.

For $j \geq 0$ and $x, y \in B^{n+j}$ define the offset-XOR function $X_j : B^{n+j} \times B^{n+j} \to B^n$ as $X_j(x,y) = z$ where $z_i = x_i \oplus y_{i+j}$ for $i = 1, \dots, n$. For $z \in B^n$ the set of pairs (x,y) which produce z when XOR'd with offset j is

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

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 $X \subseteq B^n$ as:

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

We note that $|A_j(z)| = 2^{n+2j}$ and check this is a valid probability space. Indeed, $Q_{n,j}(\emptyset) = 0$, is trivially true,

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

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

$$|\bigcup_z A_j(z)| = 2^n 2^{n+2j} = (2^{n+j})^2, \text{ so } \bigcup_z A_j(z) = B^{n+j} \times B^{n+j},$$

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 XOR'd distribution $Q_{n,j}$ for $j = 0$ and $j > 0$.

Let $z \in B^n$ and $j \geq 0$. By $z[m,k]$ we denote the substring $z_m \dots z_k, 1 \leq m \leq k \leq n$. We have

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

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

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

We recognise this as a constantly biased source where

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

It is interesting to compare the form of $Q_{n,0}$ to the distribution of the constantly biased source Eq. (3) by discarding one output string—the former is more sensitive to misalignment, 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, while if we have equal detector efficiencies then we get the uniform distribution. We show this as follows (note that $Z_{n+j} = 2^{n+j}$ in this case):

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

However, in the more general case of non-equal detector efficiencies, the distribution is no longer independent, although in general is much closer to the uniform distribution than the $j = 0$ case. (Recall that independence is a sufficient but not necessary condition for uniform distribution (Abbott and Calude 2010).) It is indeed this "closeness"—the total variation distance given by $\Delta(U_n, Q_{n,j}) = \frac{1}{2}\sum_{x\in B^n} |2^{-n} - Q_{n,j}(x)|$—which 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

Table 3. *Empirical evidence for the quality of* XORing *with $j > 0$ compared to $j = 0$ 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 (further from the ideal case) that one would expect in an experimental setup. The (small) value of $n = 10$ has been used as, unfortunately, the distribution is very costly to calculate numerically. Here $bin(m)$ denotes the (10-bit zero-extended) binary representation of m. For example, $bin(1) = 0000000001$, $bin(2) = 0000000010$, etc.*

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 Table 6.3.*

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

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 operationalizations*

This given, one may ask why not simply discard one string to give the distribution in Eq. (3) and apply von Neumann normalisation to obtain uniformly distributed bitstrings. There are two primary answers to this question.

(i) As discussed previously the effect of drift in bias and temporal correlations will ensure 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 ($Q_{n,j}$ for example is less sensitive to detector bias than that in Eq. (3)). It is extremely plausible that $Q_{n,j}$ gives as good results as discarding one string in practice; it is indeed very close to the uniform distribution as can be seen from Table 6.3 and Fig. 3. To compare properly the distributions, the following *open question* must be answered: what is the bound ρ depending on $e_x^{\oplus}, e_y^{\otimes}$ and θ such that $\Delta(U_n, Q_{n,j}) \leq \rho$, and how does that compare to that given in (Abbott and Calude 2010) for normalisation of a source with varying bias?

Further, $Q_{n,j}$ 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 XORing process extremely appealing for a high bitrate, un-normalized QRNG. Even the $j = 0$ case with von Neumann applied after XORing would often be preferable

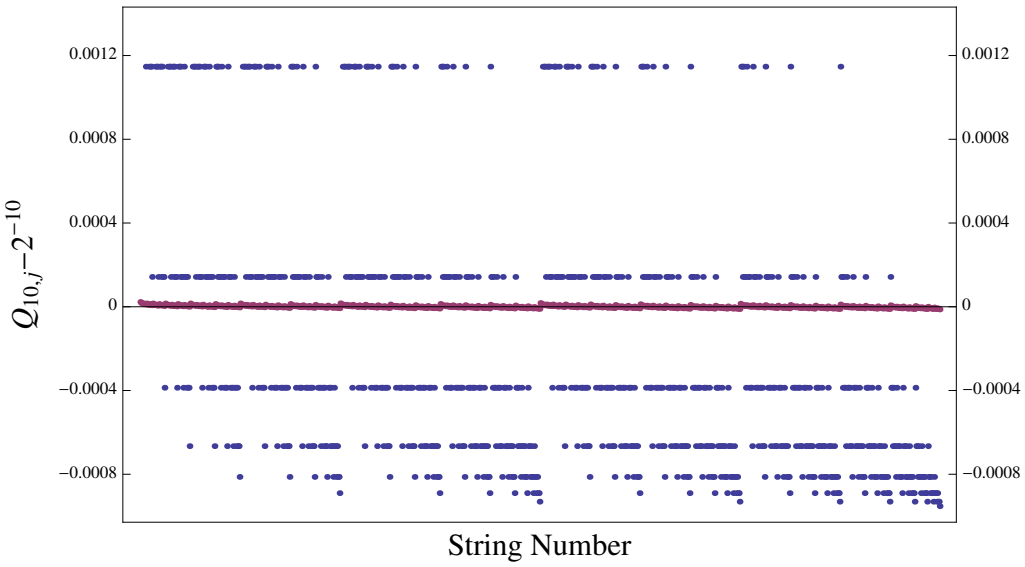

Fig. 3. (Color online) A plot of $Q_{10,j} - 2^{-10}$ for each of the 2^{10} strings of length 10. The two cases $j = 0$ (blue) and $j = 1$ (red) show how much closer the probabilities given by $Q_{10,1}$ are to that expected from the uniform distribution than for $Q_{10,0}$. The same experimental configuration as in Table 6.3 has been used.

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 one insists on a perfect theoretical distribution in the presence of non-ideal misalignment and unequal detector efficiencies, or perhaps the $Q_{n,j}$ distribution is not sufficient for particular requirements, then one can still operationalize 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 so, 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, those with $a_1b_1 > a_2b_2$ to 1, and discarding those with $a_1b_1 = a_2b_2$, one will obtain the uniform distribution as for von Neumann's procedure. The key advantage is that this will obtain 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 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 operationalize in more than one way: either by using shifted `XOR`ing of bits to sample from a distribution which is close to (equal to in the ideal limit) the uniform distribution and efficient and robust to various errors, or by utilising both produced bitstrings to allow a more efficient normalisation procedure giving (in absence of the aforementioned temporal effects) the uniform distribution. Many more operationalizations are undoubtedly possible.

7. Summary

Every QRNG claiming to produce a better form of randomness than pseudo-randomness must firstly be certified by some physical law implying the incomputability of the output bitstrings; value indefiniteness is one such example. Most existing proposals of QRNGs 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 holds only in a Hilbert space of dimension greater than 2). In this paper we have proposed a QRNG which, by utilising an entangled photon singlet-state in four-dimensional Hilbert space, is certified by value indefiniteness which implies strong incomputability, 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 exactly the theoretical uniform probability distribution, another essential symptom of randomness (independent of incomputability). The form and effects of these conceivable experimental errors have been discussed, and care has been taken 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 obtain better protection against experimental imperfections, particularly non-ideal misalignment and unequal detector efficiencies, and to utilise the benefit of these two strings over simply using one. Rather than XORing corresponding bits, bits x_i and y_{i+j} are XOR'd (for fixed $j > 0$) as this not only provides much better results, but also mitigates the effects of temporal correlations between adjacent bits. Further, we have proposed an alternative normalisation method based on von Neumann's procedure which uses both bitstrings. This procedure is significantly more efficient yet still guarantees uniformly distributed strings in the presence of non-ideal misalignment and unequal detector efficiencies. We leave it as an *open question* to improve upon the time-shifted XOR method and find a technique to extract bits which are provably uniformly distributed and is more efficient than the improved von Neumann method discussed.

Analyses of sequences generated by the proposed QRNG should be conducted, utilising the knowledge of the expected uniform distribution, as in Calude et al. (2010). In particular, the quality of both the individual strings produced should be compared with that of the XOR'd sequence, both with and without von Neumann normalisation applied, as well as the sequence produced by our improved von Neumann method.

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

The proposed QRNG produces bits which are certified via 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 experimentally test the quality of bits produced via this method against existing classical and quantum sources of randomness.

Acknowledgment

We thank A. Cabello, G. Longo and A. Zeilinger for many interesting discussions about quantum randomness.

References

Abbott, A. A. and Calude, C. S. (2010) Von Neumann normalisation of a quantum random number generator. Report CDMTCS-392, Centre for Discrete Mathematics and Theoretical Computer Science, University of Auckland, Auckland, New Zealand.

Abbott, A. A., Calude, C. S., and Svozil, K. (2010) Incomputability of quantum randomness. *in preparation*.

Bechmann-Pasquinucci, H. and Peres, A. (2000) Quantum cryptography with 3-state systems. *Phys. Rev. Lett.* **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. *Phys. Rev. A* **81** (1), 012109.

Billingsley, P. (1979) *Probability and Measure*. John Wiley & Sons, New York, Toronto, London.

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*. Springer, New York, second edition.

Cabello, A. (2008) Experimentally testable state-independent quantum contextuality. *Phys. Rev. Lett.* **101** (21), 210401.

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

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

Calude, C. S. and Svozil, K. (2008) Quantum randomness and value indefiniteness. *Adv. Sci. Lett.* **1** (2), 165–168.

Chaitin, G. J. (1977) Algorithmic information theory. *IBM J. Res. and Dev.*, **21**, 350–359, 496. Reprinted in Chaitin (1990).

Chaitin, G. J. (1990) *Information, Randomness and Incompleteness*. World Scientific, Singapore, second edition. This is a collection of G. Chaitin's early publications.

Clauser, J. F. and Shimony, A. (1978) Bell's theorem: experimental tests and implications. *Rep. Prog. Phys.* **41**, 1881–1926.

Ekert, A. K. (1991) Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **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. *Phys. Rev. A* **75** (3), 032334.

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

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

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

Haahr, M. (2010) True random number generator. http://www.random.org.

Hai-Qiang, M., Su-Mei, W., Da, Z., Jun-Tao, C., Ling-Ling, J., Yan-Xue, H., and Ling-An, W. (2004) A random number generator based on quantum entangled photon pairs. *Chin. Phys. Lett.* **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. *Phys. Rev. Lett.* **90** (25), 250401.

ID Quantique (2001-2010) *QUANTIS. Quantum number generator*. idQuantique, Geneva, Switzerland.

Jennewein, T. Private communication to authors, 18 February 2009.

Jennewein, T., Achleitner, U., Weihs, G., Weinfurter, H., and Zeilinger, A. (2000) A fast and compact quantum random number generator. *Rev. Sci. Instrum.* **71**, 1675–1680.

Kochen, S. and Specker, E. P. (1967) The problem of hidden variables in quantum mechanics. *J. Math. Mech. (now Indiana Univ. Math. J.)* **17** (1), 59–87. Reprinted in Specker (1990, pp. 235–263).

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

Lindner, F., Schätzel, M. G., Walther, H., Baltuška, A., Goulielmakis, E., Krausz, F., Milošević, D. B., Bauer, D., Becker, W., and Paulus, G. G. (2005) Attosecond double-slit experiment. *Phys. Rev. Lett.* **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., editor, *Handbuch der Physik. Band V, Teil 1. Prinzipien der Quantentheorie I*, 1–168. Springer, Berlin, Göttingen and Heidelberg.

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

Peres, A. (1978) Unperformed experiments have no results. *Am. J. Phys.* **46**, 745–747.

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

Pironio, S., Acín, A., Massar, S., Boyer de la Giroday, A., Matsukevich, D. N., Maunz, P., Olmschenk, S., Hayes, D., Luo, L., Manning, T. A., and Monroe, C. (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. *J. Mod. Opt.* **41**, 2435–2444.

Specker, E. (1990) *Selecta*. Birkhäuser Verlag, Basel.

Stefanov, A., Gisin, N., Guinnard, O., Guinnard, L., and Zbinden, H. (2000) Optical quantum random number generator. *J. Mod. Opt.* **47**, 595–598.

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

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

Svozil, K. (2010) Quantum value indefiniteness. *Nat. Comput.*, online first, 1–12.

Von Neumann, J. (1951) Various techniques used in connection with random digits. *National Bureau of Standards Appl. Math Ser.* **12**, 36–38. Reprinted in *John von Neumann, Collected Works, (Vol. V)*, A. H. Traub, editor, MacMillan, New York, 1963, p. 768–770.

Wang, P. X., Long, G. L., and Li, Y. S. (2006) Scheme for a quantum random number generator. *J. Appl. Phys.* **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. *Phys. Rev. Lett.* **81**, 5039–5043.