IOP PUBLISHING EUROPEAN JOURNAL OF PHYSICS

Eur. J. Phys. **30** (2009) 1189–1200 doi:10.1088/0143-0807/30/5/026

Demonstrating quantum random with single photons

Patrick Bronner[1], Andreas Strunz[1], Christine Silberhorn[2] and Jan-Peter Meyn[1]

[1] Friedrich-Alexander-Universität Erlangen, Physikalisches Institut, Didaktik der Physik, Staudtstrasse 7, 91058 Erlangen, Germany
[2] Max Planck Junior Research Group, Guenther-Scharowsky-Strasse 1, 91058 Erlangen, Germany

E-mail: Jan-Peter.Meyn@physik.uni-erlangen.de and csilberhorn@physik.uni-erlangen.de

Received 26 June 2009
Published 14 August 2009
Online at stacks.iop.org/EJP/30/1189

Abstract

We present an experiment for education which demonstrates random transmission or reflection of heralded single photons on beam splitters. With our set-up, we can realize different quantum random experiments by appropriate settings of polarization rotators. The concept of entanglement is motivated by correlated randomness. The experiments are suitable for undergraduate education and are available as interactive screen experiments.

(Some figures in this article are in colour only in the electronic version)

1. Introduction

The random process is a unique feature of quantum physics. Contrary to classical physics, quantum physics does not definitely predict what will happen when an individual measurement is performed. Only probabilities for all possible measurement outcomes are determined. Quantum physics is the sole theory which contains intrinsic randomness. This fact has been very disturbing to many physicists, including Albert Einstein, who expressed his discomfort saying 'I, at any rate, am convinced that he does not throw dice' [1]. Since the first decades of the 20th century, quantum randomness has been confirmed by theoretical and experimental research. The discovery that individual events are absolutely random is one of the most significant findings of the last century. Quantum random should therefore play a substantial role in education. Didactic aspects of quantum randomness have been discussed in connection with quantum experiments [2], evaluated hands-on tutorial activities [3, 4], probability theories [5, 6] and philosophical aspects [7, 8].

Furthermore, random numbers are an essential tool for a wide range of applications: for computer simulations, for testing fundamental physical laws [9] and for lottery games. Many important applications for random numbers are in the new field of quantum information, such

as quantum cryptography. Quantum cryptography is based on the idea of generating a key sequence between two parties [10]. To produce the key sequence, a random number generator is needed for both communication parties. Random numbers used for cryptographic protocols have to fulfil stringent quality criteria, such as unpredictability and a bias-free statistical distribution. For sensitive applications, reliable random numbers are essential.

There are two approaches to producing random numbers: algorithmic and hardware-based implementations. Algorithmic random number generators apply a mathematical formula to produce random bits from a seed. The seed is obtained from data which are not easily accessible to an eavesdropper, such as computer clock reading or computer mouse path movement. If the seed is known, the random number could be predicted in principle, therefore these generators are typically called pseudorandom. Hardware-based systems can also use the unpredictable behaviour of a complex or chaotic physical system, where determinism is hidden behind complexity. The prediction of such a classical system is possible if sufficient knowledge of the initial conditions is available. Contrarily, a hardware-based system which employs a quantum mechanical process can produce true randomness, according to theory. The first quantum random number generators exploited the radiation of a single atom [11] or the decay of a radioactive nucleus [12]. Although it is a fact that the radioactive process produces random numbers of excellent quality [13] and the experiment is available for undergraduate labs [2], the use of radioactive material causes health and safety concerns. Recently, a hardware quantum random number generator [14] based on the unpredictable transmission or reflection of a single photon on a beam splitter has been demonstrated.

We have designed single photon experiments on quantum randomness for educational purposes in order to expand existing single photon demonstration experiments [15–17]. All our quantum random experiments are available as interactive screen experiments [18] on our website[3] and may be used in high school and undergraduate lessons. The quantum random generators are very similar to modern research experiments [14, 19] and yield comparable results.

In the following section, we recall the concept of quantum randomness. In section 3, the experimental setting is described. The randomness of a single photon on a beam splitter is presented in section 4. We extend the experiment in section 5 to a symmetric set-up with two beam splitters, both for separable and entangled photons. Finally, we test the random data with statistical tests in section 6.

2. Quantum random

2.1. Concept of quantum randomness

Quantum random occurs in the measurement of a system in a quantum superposition of basis states:

$$|\psi\rangle = \sum_{i=1}^{z} a_i \, |x_i\rangle \, .$$

The coefficients a_i with $i \in \mathrm{N}$ are probability amplitudes with $\sum_{i=1}^{z} |a_i|^2 = 1$. The elementary quantum superposition state is a linear superposition of two single states ($z = 2$):

$$|\psi\rangle = a_1 \, |x_1\rangle + a_2 \, |x_2\rangle \, .$$

A quantum superposition of a two-state system is called a quantum bit (qubit) [20]. In contrast to a classical bit, a qubit cannot only be found in one of the two basis states, but also in a

[3] Interactive screen experiments and random data are available through www.quantumlab.de.

superposition of both. Measurements of qubits yield a projection on one basis state with the probability given by the coefficients. In physical experiments, qubits can be realized easily, e.g., with single photons. A photonic qubit arises from a distinguishable path by transmission T or reflection R of a single photon state on a 50% beam splitter:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|T\rangle + |R\rangle\right). \tag{1}$$

Alternatively, a qubit can be realized by a diagonal polarized photon with horizontal (H) and vertical (V) polarization basis:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle + |V\rangle\right). \tag{2}$$

A polarization beam splitter transforms the polarization basis into a spatial basis.

Qubits can also be prepared with trapped ions [21], nuclear spin [22] and electron spin in quantum dots [23]. For a random number generator, the basis states of the qubit are associated with the binary values 0 and 1, respectively.

2.2. Quantum random generators

Any qubit would be useful for the generation of quantum random numbers. For commercial use, a quantum number generator should be small, fast, easy to use and safe. The best solution is to use photonic systems, because light is easy to handle and its intensity can be adjusted. The first light-based random number generators were established in 1994 [24–26]. These systems used attenuated light pulses with Poissonian photon number statistics. Theoretically, the light can be treated as a classical electromagnetic wave, which is detected behind a beam splitter by two binary quantum detectors. The quantum process takes place due to absorption of light in the detectors. There is no preparation of a single photon state required, thus the description with a quantum superposition state as discussed above appears not to be appropriate. Commercial quantum random systems with attenuated light are available as USB modules [27].

2.3. Photon-based quantum random generator

A quantum random number generator especially based on photonic qubits as discussed in section 2.1 relies on the superposition of single photon states. The single photon qubit can be realized on a 50% beam splitter (equation (1)) or on a polarizing beam splitter (equation (2)). The measurement takes place behind the beam splitter with sensitive detectors. The first quantum random number generator which used the superposition of a single photon state on a beam splitter was demonstrated in 2004 [14]. Subsequently, quantum random generators with two photons have been realized with entangled photons [19, 28] and Hong–Ou–Mandel states [29].

3. Experiment

3.1. Single photon preparation

For the preparation of single photons, we use photon pairs which are generated by parametric down conversion (PDC) in a nonlinear crystal with a spread of different arrival times. One photon is detected as a gate to specify the time event of the other photon within a coincidence window of 2 ns. The coincidence method (figure 1) is used in all experiments.

The quality of the heralded single photon source can be demonstrated with the second-order correlation function $g^{(2)}(0)$ [30]. In an ideal single photon case, the second-order

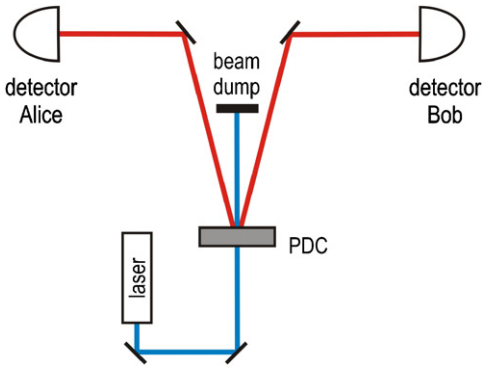

Figure 1. Sketch of the set-up to measure coincidences.

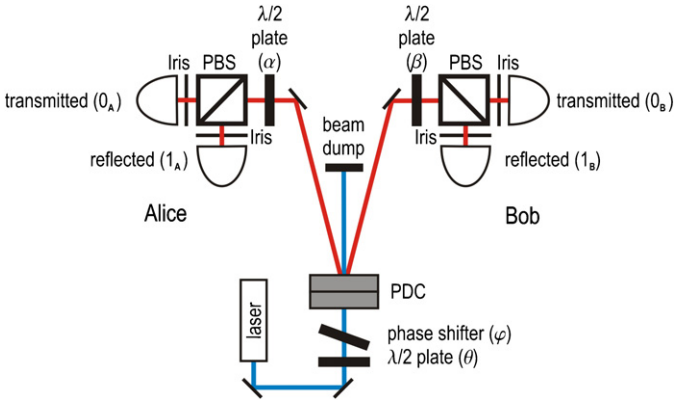

Figure 2. Sketch of the complete demonstration experiment.

correlation function should be $g^{(2)}(0) = 0$. We measure a second-order correlation function of $g^{(2)}(0) = 0.0059 \pm 0.0006$, which is over 1600 standard deviations beyond the classical limit with $g^{(2)}(0) = 1$.

3.2. Experimental set-up

For demonstrating quantum random on beam splitters, we set up an experiment where different types of photon random experiments can be realized. The set-up of the experiment is sketched in figure 2.

Photon pairs are generated by the PDC process under energy and momentum conversation in two 0.5 mm long barium beta borate crystals. The crystals have orthogonal orientation and are stacked together [31]. The first (second) crystal converts a vertically (horizontally) polarized 405 nm laser photon in two horizontally (vertically) polarized downconversion photons, each around 810 nm with an efficiency of 10^{-11}. Due to momentum conservation, the photons are emitted diagonally to each other on a cone. The opening angles of the cones can be independently adjusted. The laser (CrystaLaser BCL-405-S) has a power of 24 mW, a wavelength of 405 nm and is vertically polarized. The polarization of the laser light is adjusted

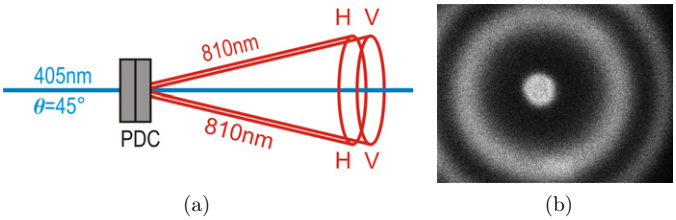

Figure 3. Crystal combination as an entanglement source. (a) Sketch of the set-up. (b) Photograph of two separated cones.

with a $\lambda/2$-plate (angle θ) in front of the crystal combination. With $\theta = 0^\circ$, only the first crystal produces photon pairs in the $|H\rangle\,|H\rangle$ state[4].

For $\theta = 45^\circ$, the photon pairs are generated in both sections of the composite device (figure 3). Both crystals emit a single cone which are aligned to overlap with a cone opening of $\pm 3^\circ$. The experimental configuration ensures that the generation of photon pairs from the two crystals becomes indistinguishable, which yields a polarization-entangled state

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle\,|H\rangle + \mathrm{e}^{\mathrm{i}\varphi}\,|V\rangle\,|V\rangle\right).$$

The phase φ of the entangled state can be adjusted with a phase shifter [32] before the crystal combination. With the phase $\varphi = 0$, we produce a Bell state, which is necessary for the random experiment in section 5.2. To enhance entanglement visibility, we use irises before every detector to detect only photons from the total overlap area of the two cones.

For polarization measurement, we place a combination of a $\lambda/2$-plate (angles α and β) and a polarizing beam splitter (PBS) on each side of the symmetric set-up. The photons are detected with fibre-coupled avalanche photo diodes (PerkinElmer SPCM AQ4C), which are protected by bandpass filters (780–820 nm) against diffuse visible light. The detection arrangements are commonly referred to as Alice and Bob. For data acquisition, we use a time-digital converter module (Acam TDC-GPX). The allocation between binary numbers and the transmitted or reflected detector after the beam splitter is not consistent in the literature [26, 33]; we use the allocation transmitted = 0, reflected =1 according to [26].

3.3. Different random experiments with one set-up

Different types of photon random experiments can be realized by turning one to three $\lambda/2$-plates (angles α, β, θ) between two positions. To rotate the polarization of the light by an angle, the corresponding $\lambda/2$-plate is physically rotated by half that angle. The polarization of the photons on Alice's and Bobs's side (α, β) can be set to 0° or 45°. With laser polarization $\theta = 0^\circ$, separable photon pairs are prepared; with $\theta = 45^\circ$, the photon pairs are entangled.

With the angles $\alpha = \beta = \theta = 0^\circ$, all photon pairs are generated in the first crystal and are detected in the transmitted detectors on Alice's and Bob's side. The experiment is reduced to the source and two detectors (figure 1), and the coincidence method can be discussed. The generated quantum state is

$$|\psi\rangle = |H\rangle_A\,|H\rangle_B\,. \tag{3}$$

[4] Analogue experiments would be possible with $\theta = 90^\circ$, preparing the $|V\rangle\,|V\rangle$ state. In the following, we do not discuss these redundant cases.

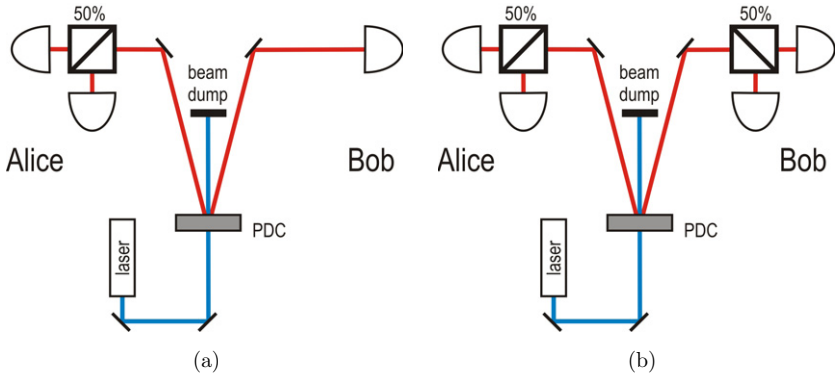

Figure 4. Reduction of the experimental set-up. (a) One beam splitter random experiment. (b) Two beam splitter random experiment.

With the angles $\alpha = 45^\circ$ and $\beta = \theta = 0^\circ$, the experiment is expanded by a beam splitter combination on Alice's side (figure 4(a)). The original quantum state (equation (3)) is turned into

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}\left(|H\rangle_A + |V\rangle_A\right)\right)|H\rangle_B\,. \tag{4}$$

With this setting, a quantum random number generator is realized on Alice's side according to equation (2). The combination of a $\lambda/2$-plate with a polarization rotation of 45° and a polarizing beam splitter is equatable to a 50% beam splitter.

With the angles $\alpha = \beta = 45^\circ$ and $\theta = 0^\circ$, the experiment is expanded on Bob's side to a symmetric set-up (figure 4(b)). Now the quantum state is

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}\left(|H\rangle_A + |V\rangle_A\right)\right)\left(\frac{1}{\sqrt{2}}\left(|H\rangle_B + |V\rangle_B\right)\right). \tag{5}$$

With this setting, a quantum random number generator is realized on Alice's and Bob's side.

With the angles $\alpha = \beta = \theta = 45^\circ$, a quantum random number generator on Alice's and Bob's side with entangled photons is realized (figure 2). The corresponding quantum state (equation (3)) is turned into

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle_A\,|H\rangle_B + |V\rangle_A\,|V\rangle_B\right). \tag{6}$$

This state is a maximally entangled state of two polarization qubits and is commonly called an entangled bit (ebit) [34].

3.4. Focus on the education experiment

For our demonstration experiment, we emphasize a clear geometry, where the beam path can be followed easily, and individual optical elements can be recognized (see figure 7). The lab is illuminated by white LED modules (420–750 nm). The LED light is blocked by bandpass filters (780–820 nm) in front of the detectors. The running experiment can be explained to students in a bright lab.

Quantum random bits can be recorded continuously up to 22 kBit s^{-1}. Parallel to the data acquisition, single measurement events can be picked out from the data stream at the push of button. The single measurement results are visualized with LED lamps on the detector boxes

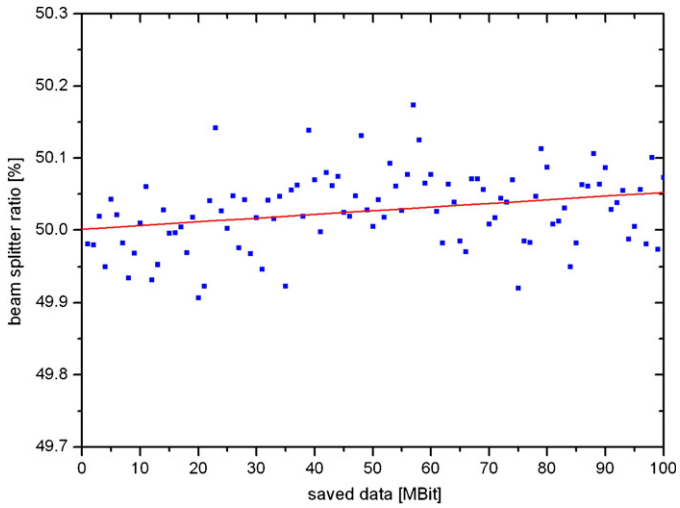

Figure 5. Beam splitter ratio of the 100 MBit random bit stream with line of best fit.

(see figure 7). All random experiments are available with single events as interactive screen experiments (ISE). For visualizing the measurement results, every ISE uses a 100 kBit dataset from the original experiment.

The quantum random experiments can be introduced in a physics course at different levels. For simplification of the basic experiment with a single beam splitter (figure 4(a)), we separate the heralded photon source from the actual beam splitter experiment with a polarization-maintaining fibre. With this two-part experiment, it is possible to discuss the quantum random process without the PDC-process.

To illustrate applications of quantum random, we provide everyday examples, such as a quantum dice. The quantum dice are applied to the musical dice game by Mozart [35].

4. Single beam splitter random experiment

For the single beam splitter random experiment on Alice's side, we set the angles to $\alpha = 45^\circ$ and $\beta = \theta = 0^\circ$ (figure 4(a)). The photon on the beam splitter is heralded by the detection on Bob's side with the coincidence method. Due to different detector and coupling efficiencies, it is not possible, with a 50% beam splitter, to achieve an exact 50% balance of 0 and 1 bits. A common solution for removing the bias is to apply an algorithm to the collected random bits [36, 37]. The simple von Neumann algorithm groups two successive bits together. The probability of 00 and 11 is biased and discarded. The groups of 01 and 10 are unbiased, the bit group 01 is converted into 0, and the bit group 10 is converted into 1. The algorithm reduces the generated data to approximately 25%. To dispose of the bias directly in the experiment, we utilize the combination of a $\lambda/2$-plate and a PBS. The polarization of the photon can be rotated with a micrometer-driven waveplate holder by 0.06° per 0.1% variation around 50.0%. 100 MBit quantum random numbers are gathered within 2.6 h at 10.5 kBit s^{-1}. The beam splitter ratio within the dataset of a sequence of 1 MBit is $50.02 \pm 0.05\%$ (figure 5).

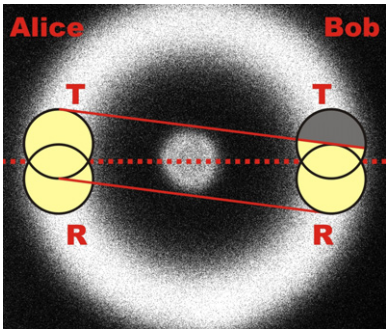

Figure 6. Detector views on the cone. Coincidence regions between Alice's transmitted and Bob's detectors.

5. Two beam splitter random experiments

5.1. Separable quantum random

At this point, we transform the single beam splitter experiment into the symmetric set-up ($\alpha = \beta = 45^\circ, \theta = 0^\circ$) (figure 4(b)). The photon on one beam splitter is heralded with the coincidence method by the detection in the transmitted or reflected detector on the other beam splitter, and vice versa. Again, on each side in one experimental run, we record 100 MBit random data. On Alice's (Bob's) side, there is a beam splitter ratio of $50.01 \pm 0.05\%$ ($49.98 \pm 0.05\%$).

The independence of both quantum random number generators is tested with the correlation function C:

$$C = \frac{N_{0_A 0_B} + N_{1_A 1_B} - N_{0_A 1_B} - N_{1_A 0_B}}{N_{0_A 0_B} + N_{1_A 1_B} + N_{0_A 1_B} + N_{1_A 0_B}}.$$

The factor $N_{0_A 0_B}$ is the number of recorded simultaneous events with the binary value 0 in Alice's and Bob's data. In theory, the probability P for measuring simultaneous events between Alice and Bob is $P_{0_A 0_B} = P_{1_A 1_B} = P_{0_A 1_B} = P_{1_A 0_B} = 0.25$, which yields a correlation factor of $C = 0$. If the random data are perfectly correlated, the factor is $C = \pm 1$. We measure a correlation factor ranging from $C = -0.1$ to $C = 0.1$. This deviation is caused by different detector views on the cone for diagonally emitted photon pairs. In an ideal case, the transmitted and reflected detector view of Alice's or Bob's side overlaps at exactly the same cone location. A different overlap of Alice's and Bob's detectors on the cone (figure 6) causes different probabilities for coincidence counts between the four detectors. This imbalance changes the value of the correlation function, which can be investigated numerically[5]. With detector alignment, we measure a correlation function of $C = -5 \times 10^{-4} \pm 9 \times 10^{-4}$ between the recorded 100 MBit random data on Alice's and Bob's side. The random numbers are independent within the limits of error. The experiment illustrates the meaning of the term *separable state*, which is identified with a product state (equation (5)).

[5] Program for investigating the correlation coefficient with variable detector views on the fluorescence cone, available through www.quantumlab.de.

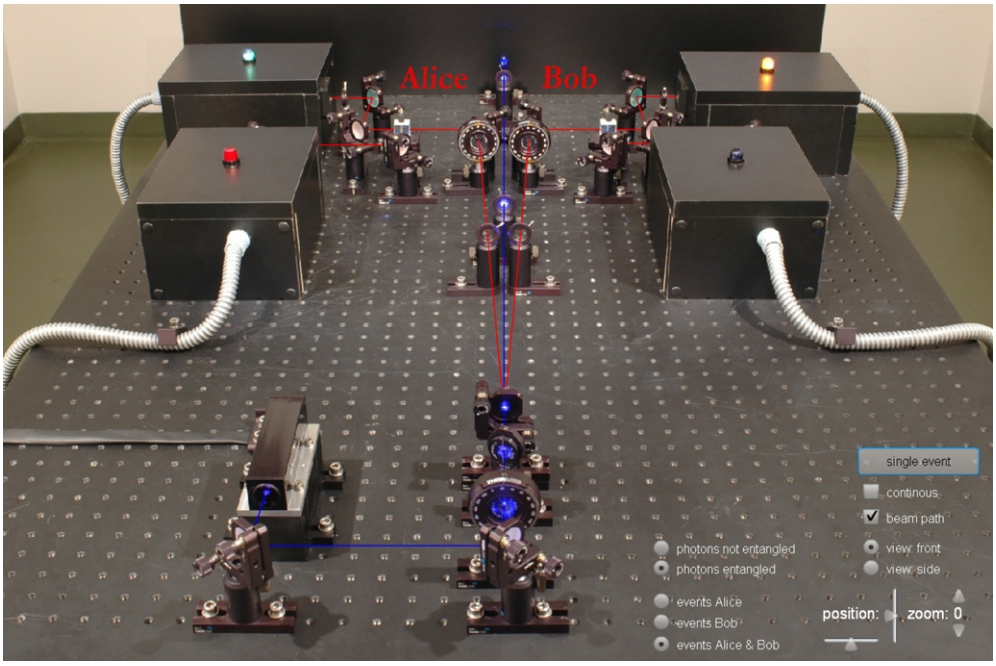

Figure 7. Screenshot of the interactive screen experiment to quantum random.

5.2. Entangled quantum random

In the symmetric set-up, we entangle photons with the laser polarization of $\theta = 45°$. Again, we take random data of 100 MBit separately on each side. The data rate of each side is reduced by the use of irises to 630 Bit s^{-1}. On Alice's (Bob's) side, there is a beam splitter ratio of $49.99 \pm 0.36\%$ ($50.22 \pm 0.35\%$). The correlation coefficient between the two data files is $C = 0.9705 \pm 0.0002$, which shows that the separated random processes are highly correlated. The random numbers are almost identical on each side. The probability P for simultaneous events between Alice and Bob depends on the measurement angles α and β according to $P_{0_A 0_B} = P_{1_A 1_B} = 1/2 \cos^2(\alpha - \beta)$ and $P_{0_A 1_B} = P_{1_A 0_B} = 1/2 \sin^2(\alpha - \beta)$. If $\alpha = \beta$ as in our experiment with $\alpha = \beta = 45°$, the photons show random behaviour at individual beam splitters, but yield identical results when comparing of Alice's and Bob's events. The principle of correlated random can be used to distribute the secret key in entangled quantum cryptography systems [38].

In the associated interactive screen experiment (figure 7), the random process on two beam splitters can be investigated by capping the detector results (lamps) on each side and switching between separable and entangled photon pairs.

5.3. Nonlocality

With the experiment of section 5.1, students are convinced about the quantum random process at Alice's beam splitter. Equivalently, they are convinced about the quantum random process at Bob's beam splitter. With entangled states, Bob's and Alice's results for individual measurements are identical in all cases, not only accidentally. This is a striking observation. Obviously, the photons are no longer independent. The entangled state cannot be regarded as two separable single photon states. After this observation, one might start to wonder about

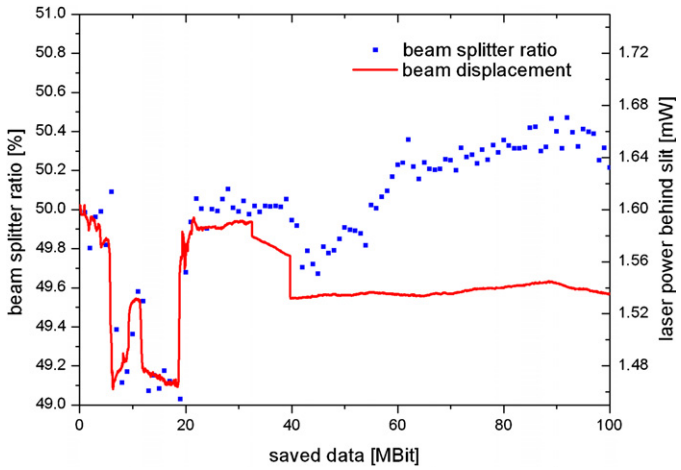

Figure 8. Beam splitter ratio over 44 h on Alice's side with laser beam displacement.

hidden local parameters, like whether the photons could agree on reflection or transmission on either side in advance. For a stringent proof of nonlocality, the CHSH [39], Wigner [40] and Hardy [41] schemes are used. By implementing these with our set-up, local theories are excluded by more than 100 standard deviations of measurement error.

6. Test of randomness

There are no statistical tests which can prove absolute randomness, due to no-go theorems based on Gödel's incompleteness theorems [42]. A generally accepted definition of absolute random is missing [43].

The National Institute for Standards and Technology (NIST) has recently put forward a statistical test suite for random and pseudorandom number generators for cryptography applications [44]. The test is designed as an industry standard for testing pseudo-random number generators. It consists of 15 individual statistical tests, such as entropy, longest run of ones in a block, and so on. Each test evaluates a probability value P and a proportion value $\hat{p}$ to quantify the randomness of the sequence. If the value P is in the interval $P \in [0.0001; 1)$ and the value $\hat{p}$ is within another interval, the test concludes that the sequence is absolutely random. The interval of $\hat{p}$ depends on the significance level S, which should be in the order of $S = 0.01$–0.001. We chose a significance level of $S = 0.001$ for all tests, which resulted in $\hat{p} \in [0.9895; 1.0084]$.

The 100 MBit random data from the single beam splitter experiment (section 4) pass the NIST tests with $P \in [0.0005; 0.9878]$ and $\hat{p} \in [0.9900; 1.0000]$. Similar results are achieved with Alice's and Bob's data from the two beam splitter experiment (section 5.1). To show the independence of both quantum random numbers, we add each bit of the data from Alice's and Bob's binarily modulo two. The sum passes the NIST test as well, so the two datasets are indeed independent.

With the two beam splitter experiment with entangled photons (section 5.2), we pass 8 out of 15 statistical tests on each side ($P_A \in [0.0000; 0.9642]$, $\hat{p}_A \in [0.190; 1.000]$). The reason for failure in some of the tests is a varying beam splitter ratio on Alice's and Bob's side between 49.0 and 50.6%, with a pattern of over 44 h measurement time (figure 8). The beam splitter ratio is caused by uncontrollable beam displacement of the pump laser over time

(figure 8), which was measured by a slit in front of a power meter. The exact overlap of the two cones and its limitation to irises behaves sensitively to beam displacement. Despite this technical limitation, the number of tests passed with entangled photons is comparable to recent research results [19].

7. Summary

We provide a demonstration experiment which highlights the quantum random process of single photons in different experimental settings. We give a qualitative introduction to entanglement by correlated quantum randomness. Our experiments are very similar to modern research experiments and yield comparable results. The quantum random demonstration experiment is available in the form of various interactive screen experiments.

Acknowledgments

We would like to thank Gesine Murphy for language consultation. One of us (PB) acknowledges a scholarship from Cusanus Stiftung.

References

[1] Einstein A 1971 Letter to Max Born *The Born–Einstein Letters* (translated by Irene Born) 1916–1955 (New York: Walker and Company) ISBN-0-8027-0326-7
[2] Aguayo R, Simms G and Siegel P B 1996 Throwing nature's dice *Am. J. Phys.* **64** 752–8
[3] Bao L and Redish E 2002 Understanding probabilistic interpretations of physical systems: a prerequisite to learning quantum physics *Am. J. Phys.* **70** 210–7
[4] Wittmann M, Morgan J and Feeley R 2006 Laboratory-tutorial activities for teaching probability *Phys. Rev. Special Top.–Phys. Educ. Res.* **2** 020104
[5] Chow C and Cohen T 2000 Quantum coins, dice, and children: probability and quantum statistics **68** *Am. J. Phys.* 829–34
[6] de la Torre A 2008 On randomness in quantum mechanics *Eur. J. Phys.* **29** 567–75
[7] Howson C 1995 Theories of probability **46** *Br. J. Phil. Sci.* **1** 1–32
[8] Zeilinger A 2005 The message of the quantum *Nature* **438** 743
[9] 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** 5039–43
[10] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–95
[11] Erber T and Putterman S 1985 Randomness in quantum mechanics—nature's ultimate cryptogram? *Nature* **318** 41–3
[12] Inoue H, Kumahora H, Yoshizawa Y, Ichimura M and Miyatake O 1983 Random numbers generated by a physical device *Appl. Stat.* **32** 115–20
[13] HotBits 2006 Genuine random numbers, generated by radioactive decay with statistical tests http://www.fourmilab.ch/hotbits
[14] Hai-Qiang M *et al* 2004 A random number generator based on quantum entangled photon pairs *Chin. Phys. Lett.* 1961–4
[15] Thorn J, Neel M, Donato V, Bergreen G, Davies R and Beck M 2004 Observing the quantum behavior of light in an undergraduate laboratory *Am. J. Phys.* **72** 1210–9
[16] Galvez E *et al* 2005 Interference with correlated photons: five quantum mechanics experiments for undergraduates *Am. J. Phys.* **73** 127–40
[17] Carlson J A, Olmstead M D and Beck M 2006 Quantum mysteries tested: an experiment implementing Hardy's test of local realism *Am. J. Phys.* **74** 180–6
[18] Bronner P, Strunz A, Silberhorn C and Meyn J P 2009 Interactive screen experiments with single photons *Eur. J. Phys.* **30** 345–53
[19] Owens I J, Hughes R J and Nordholt J E 2008 Entangled quantum-key-distribution randomness *Phys. Rev.* **78** 022307
[20] Schumacher B 1995 Quantum coding *Phys. Rev.* A **51** 2738–47
[21] Blinov B, Leibfried D, Monroe C and Wineland D 2005 Quantum computing with trapped ion hyperfine qubits *Quantum. Inform. Process.* **3** 45–59
[22] Vandersypen L, Steffen M, Breyta G, Yannoni C, Sherwood M and Chuang I 2001 Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance *Nature* **414** 883–7

[23] van der Wiel W, Stopa M, Kodera T, Hatano T and Tarucha S 2006 Semiconductor quantum dots for electron spin qubits *New J. Phys.* **8** 28
[24] Rarity J G, Owens P C M and Tapster P R 1994 Quantum random-number generation and key sharing *J. Mod. Opt.* **41** 2435–44
[25] Stefanov A, Gisin N, Guinnard O, Guinnard L and Zbinden H 2000 Optical quantum random number generator *J. Mod. Opt.* **47** 595–8
[26] Jennewein T, Zeilinger A, Achleitner U, Weihs G and Weinfurter H 2000 A fast and compact quantum random number generator *Rev. Sci. Instrum.* **71** 1675–80
[27] id Quantique 2008 Quantis—quantum random number generator, Chemin de la Marbrerie 3, 1227 Carouge/Geneva, Switzerland http://www.idquantique.com/
[28] Fiorentino M, Santori C, Spillane S M, Beausoleil R G and Munro W J 2007 Secure self-calibrating quantum random-bit generator *Phys. Rev.* **75** 032334–5
[29] Kwon O, Cho Y and Kim Y 2009 Quantum random number generator using photon-number path entanglement *Appl. Opt.* **48** 1774–8
[30] Fox M 2006 *Quantum Optics* (Oxford: Oxford University Press)
[31] Kwiat P, Waks E, White A, Appelbaum I and Eberhard P 1999 Ultrabright source of polarization-entangled photons *Phys. Rev.* A **60** 773–6
[32] Hale P and Day G 1988 Stability of birefringent linear retarders (waveplates) *Appl. Opt.* **27** 5146–53
[33] Stipcevic M and Medved-Rogina B 2007 Quantum random number generator based on photonic emission in semiconductors *Rev. Sci. Instrum.* **78** 045104
[34] Bennett C, DiVincenzo D, Smolin J and Wootters W 1996 Mixed-state entanglement and quantum error correction *Phys. Rev.* A **54** 3824–51
[35] Mozart W 1793 Musikalisches Wuerfelspiel (Walzer), Adagio KV 294d/516f
[36] von Neumann J 1951 Various techniques used in connection with random digits *Appl. Math. Ser.* **12** 36–8
[37] Peres Y 1992 Iterating von Neumann's procedure for extracting random bits *Ann. Stat.* **20** 590–7
[38] Ekert A 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3
[39] Clauser J F, Horne M, Shimony A and Holt R 1969 Proposed experiment to test local hidden-variable theories *Phys. Rev. Lett.* **23** 880–4
[40] Wigner E 1970 On hidden variables and quantum mechanical probabilities *Am. J. Phys.* **38** 1005–9
[41] Hardy L 1993 Nonlocality for two particles without inequalities for almost all entangled states *Phys. Rev. Lett.* **71** 1665–8
[42] Gödel K 1931 Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme *Monats. Math. Phys.* **38** 173–98
[43] Compagner A 1991 Definitions of randomness *Am. J. Phys.* **59** 700–5
[44] NIST 2008 Statistical Test Suite version 2.0b (Gaithersburg, MD: National Institute of Standards and Technology) http://csrc.nist.gov/rng/