# Quantum random number generator using photon-number path entanglement

Osung Kwon, Young-Wook Cho, and Yoon-Ho Kim*

Department of Physics, Pohang University of Science and Technology , Pohang 790-784, South Korea

*Corresponding author: yoonho@postech.ac.kr

Received 21 January 2009; accepted 18 February 2009;
posted 4 March 2009 (Doc. ID 106049); published 19 March 2009

We report a quantum random number generator based on the photon-number–path entangled state that is prepared by means of two-photon quantum interference at a beam splitter. The randomness in our scheme is truly quantum mechanical in origin since it results from the projection measurement of the entangled two-photon state. The generated bit sequences satisfy the standard randomness test. 

*OCIS codes:* 270.5585, 030.5260, 190.7110.

## 1. Introduction

The need to generate random numbers arises in many scientific and engineering disciplines. For example, in quantum cryptography, the initial choices of the basis and the polarization state for the photon must be truly random for a secure system. Although mathematical algorithms can be used to obtain pseudorandom numbers that exhibit some statistical random behavior, they are not truly random in the sense that the algorithmic method is deterministic in nature. Since randomness is inherent in quantum physics, a physical random number generator built upon a quantum mechanical process would offer true randomness. For example, consider a single-photon, $|1\rangle$, entering a lossless 50/50 beam splitter by way of one of two input ports. The state at the output ports of the beam splitter is easily calculated to be in quantum superposition, $|\psi\rangle = (|1\rangle_t + |1\rangle_r)/\sqrt{2}$, where the subscripts $t$ and $r$ refer to the two output modes of the beam splitter. The single-photon detectors placed at the output ports perform the projection measurement on the quantum state $|\psi\rangle$: when the $t$ ($r$) detector clicks, we know that the quantum state has collapsed to $|1\rangle_t$ ($|1\rangle_r$). It can easily be seen that each detector has 50% probability of registering the photon but, within the framework of quantum physics, it is not possible to predict which of the two detectors will click. Since the final outcome is inherently nondeterministic and quantum mechanically random, this process can then be used to build a quantum random number generator (QRNG). Hence, this discussion allows us to identify the key elements that give rise to quantum mechanical randomness as the projection measurement and the quantum superposition state. In other words, quantum mechanical randomness arises from the projection measurement on a quantum superposition state.

Obviously, the single-photon beam-splitting scheme discussed above would make the ideal QRNG if properly implemented. Unfortunately, an efficient single-photon source that is essential for the beam-splitter-based QRNG does not yet exist and the scheme, in practice, is implemented with attenuated optical pulses [1–3]. Thus, practical implementations of the beam-splitter-based QRNG scheme do not properly realize the key elements, which are quantum superposition and projection measurement, for the QRNG. These implementations should therefore be considered as classical physical random number generators inspired by the ideal quantum scheme.

Recently, a number of alternative QRNG schemes were reported in the literature [4–8]. Some of these schemes make use of Poissonian statistics inherent in the photon emission and detection processes to

0003-6935/09/091774-05$15.00/0

extract random bit sequences [4–6]. The key elements of QRNG, i.e., projection measurement and quantum superposition, however, have not been invoked in these schemes. Implementations of QRNG that do in fact realize the projection measurement and the quantum superposition state are reported in Refs. [7,8]. In Ref. [7], the beam-splitter-based QRNG scheme was implemented with the heralded single-photon state from spontaneous parametric downconversion (SPDC). This implementation, however, is based on postselection of the detected events, requiring two detectors and a coincidence circuit for coincidence-based postselection [9]. In Ref. [8], a QRNG scheme involving a two-photon polarization entangled state is reported [10–12]. While this scheme could, in principle, achieve the projection measurement on a quantum superposition state, preparing and maintaining a pure polarization entangled state are difficult experimental tasks and often require quantum state tomography.

We report a novel QRNG based on the photon-number–path entangled state that is prepared by means of two-photon Hong–Ou–Mandel quantum interference at a beam splitter. Since the randomness in our scheme comes from the projection measurement of the two-photon photon-number–path entangled state, the quantum mechanical origin of randomness can be guaranteed for the generated bit sequences. Furthermore, the use of photon-number–path entanglement not only makes the pure state preparation easier but also removes the lengthy quantum state tomography process from state characterization as the visibility of the Hong–Ou–Mandel interference is a good measure of the prepared quantum state.

### 2. Quantum Random Number Generator Based on Photon-Number Path Entanglement

A schematic of the QRNG using the photon-number–path entanglement is shown in Fig. 1. A pair of 816 nm photons is generated in a 1 mm thick type-II BBO crystal by means of the SPDC process pumped by a 408 nm diode laser. The type-II BBO crystal is phase matched so that the signal–idler photon pairs emerge from the crystal in a beamlike configuration at a $\pm 3.2°$ angle with respect to the pump laser [13,14]. The 40 mW pump laser was focused at the BBO crystal by use of an $f = 300$ mm lens. A pair of 10 nm full width at half-maximum (FWHM) interference filters (IFs) was used to cut the unwanted pump wavelength noise and the signal–idler photons were coupled to a single-mode optical fiber by use of a ×10 objective lens. The signal–idler photons were then brought together at a 3 dB (or 50/50) fiber beam splitter (FBS). The fiber polarization controllers (FPCs) were used to ensure that the arriving photons have the same polarization state and the adjustable air gaps (AGs) allow us to control the arrival time difference between the photons at the FBS.

The input quantum state to the FBS is written as $|\psi\rangle_i = |1\rangle_1 \otimes |1\rangle_2$, referring to the two-photon state where each photon of the SPDC photon pair occupies one of the two input modes of the FBS. It is well known that, when a pair of identical photons arrive simultaneously at a 50/50 beam splitter by way of different input ports, two-photon quantum interference takes places and, as a result, the two photons always exit the beam splitter through the same output port [15–19]. The quantum state that occupies the two output modes of the FBS is then calculated to be

$$|\psi\rangle = \frac{|2\rangle_3 \otimes |0\rangle_4 + |0\rangle_3 \otimes |2\rangle_4}{\sqrt{2}}, \tag{1}$$

where, for example, $|2\rangle_3 \otimes |0\rangle_4$ refers to the probability amplitude of finding two photons (zero photons) in the lower (upper) output mode of the FBS.

Since the preparation of the photon-number–path entangled state in Eq. (1) is at the heart of the current QRNG scheme, it is of utmost importance to experimentally prepare a high-purity photon-number–path entangled state. To verify the preparation of Eq. (1), we can make use of the two-photon dip by connecting the two output fibers (modes 3 and 4) of the FBS to single-photon counting detectors and observing the coincidence count between them. As demonstrated in Ref. [15], the high visibility (approaching 100%) two-photon dip is the de facto signature of the two-photon photon-number–path entangled state in Eq. (1).

Figure 2(a) shows the experimental data, i.e., coincidences between single-photon detectors connected to modes 3 and 4 of the FBS. The data demonstrate near-perfect two-photon visibility: a Gaussian fit (solid curve) to the data resulted in a visibility of $100 \pm 0.0168\%$. The coincidence between detectors D1 and D3 shows a dip with the same visibility. We note that, in the present QRNG, observing the two-photon dip is sufficient to characterize the quantum state needed for the QRNG operation. This process is much simpler and easier than characterizing the two-photon polarization entanglement by means of quantum state tomography [8].

The projection measurement in Eq. (1) would then reveal quantum mechanical randomness, and this can be accomplished by connecting a photon number resolving detector at each output mode of the FBS. Since we need to resolve only the two-photon state, $|2\rangle$, we implemented the photon number resolving detector with a FBS, two single-photon counting detectors, and a coincidence circuit (with a 3 ns coincidence window), as shown in Fig. 1. Provided that the quantum state in Eq. (1) is being measured, the coincidence event between detectors D1 and D2 or D3 and D4 tells us that the state has collapsed to $|0\rangle_3 \otimes |2\rangle_4$ or $|2\rangle_3 \otimes |0\rangle_4$, respectively. Figures 2(b) and 2(c) show the D1–D2 and D3–D4 coincidence measurements, respectively, as a function of the AG delay: the peaks at the zero AG delay are the result of

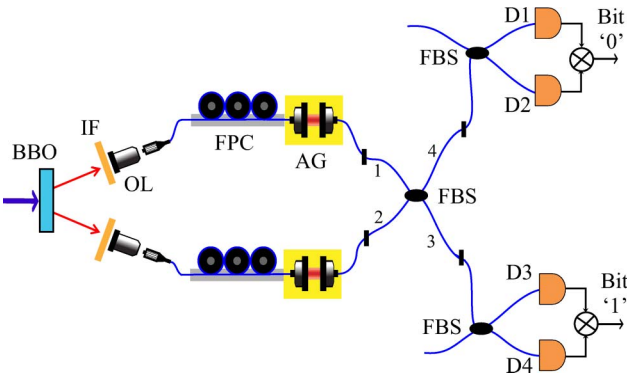


Fig. 1. (Color online) Schematic of the experiment. The two-photon photon-number–path entangled state is prepared by interfering the SPDC photon pair at a FBS. The coincidence events between detectors D1–D2 and D3–D4 form bit value 0 and bit value 1, respectively.

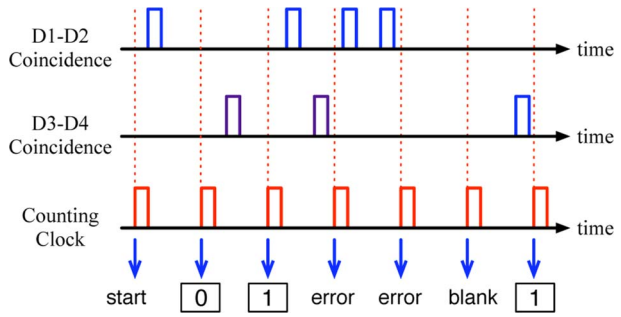


Fig. 3. (Color online) Bit sequence generation scheme. D1–D2 coincidence and D3–D4 coincidence occur randomly because of the entangled state in Eq. (1). If there is a D1–D2 or D3–D4 coincidence event between two successive counting clock pulses, we record a bit value of 0 or 1, respectively. If there are two or more such events within the time period, we record that as an error. The error bit can be removed by increasing the counting clock frequency.

the projection measurement on the photon-number–path entangled state in Eq. (1) [20].

Clearly, the projection measurement in Eq. (1) would leave us either with a D1–D2 coincidence or a D3–D4 coincidence, and this event is truly quantum mechanically random with equal probability. We can thus make use of these coincidence events to generate a bit sequence that is truly quantum mechanically random. We emphasize that, for this type of coincidence measurement to have the above operational interpretation, it is essential to ensure that what is being measured is the photon-number–path entangled state in Eq. (1). To do this, we keep the AG at the zero delay position and constantly monitor the D1 to D3 coincidence. Otherwise, the output becomes a classical random process that is due to multiple beam splitters and coincidence measurements.

The schematic for the random bit sequence generation is shown in Fig. 3. A counter/timer board (National Instruments PCI-6602) records the bit sequences with an external function generator as the counting clock. Whenever there is a coincidence event (D1–D2 or D3–D4) between the two adjacent clock pulses, the event is recorded as a 0 bit value for the D1–D2 coincidence and a bit value of 1 for the D3–D4 coincidence. When there are two or more events within the time period, we record an error bit at the next clock pulse.

### 3. Error Analysis

In our scheme, if the input state to the FBS is given as $|\psi\rangle_i = |1\rangle_1 \otimes |1\rangle_2$, it is guaranteed that all the error bits originate from these multiple D1–D2 or D3–D4 coincidence events during the clock sequence. For this to happen, it is critical to make sure that the output state of the FBS is indeed described by the state in Eq. (1). This condition was ensured in our experiment by the near-perfect two-photon quantum interference exhibited in Fig. 2(a). The bit error rate (BER), the ratio of the number of error bits to the number of total bits, can be evaluated as follows. Assuming that the probability of a single D1–D2 or D3–D4 coincidence event during the clock cycle is equal,

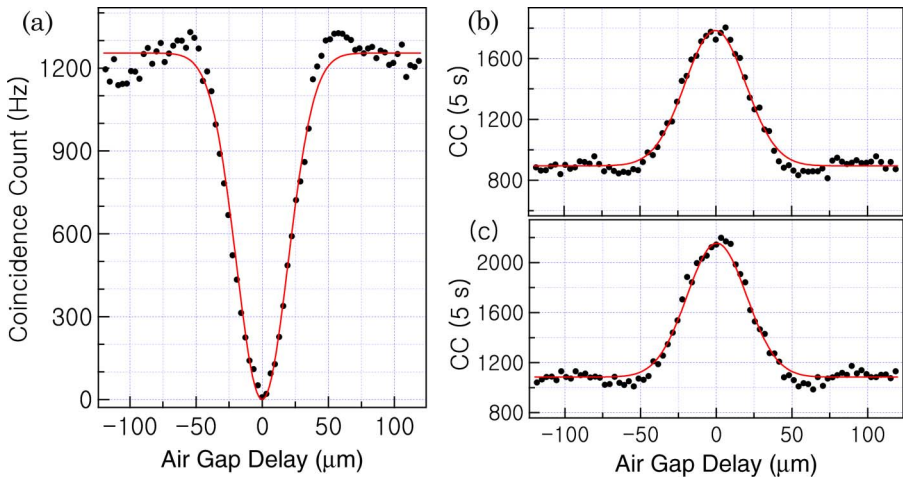


Fig. 2. (Color online) (a) Coincidence between two detectors placed at the end of the first FBS. The solid curve represents a Gaussian fit to the data and the resulting visibility is $100 \pm 0.0168\%$. The D1–D3 coincidence shows a dip with the same visibility. (b) D1–D2 coincidence and (c) D3–D4 coincidence exhibit peaks at the delay where the dip occurs.

the probability of generating a bit is given as $(1-t)/f$, where $f$ is the clock frequency and $t$ varies between $0 \le t \le 1$. Then, the probability of this bit to become an error bit is $\int_0^1 R_B(1-t)/f\,dt = R_B/2f$, where $R_B$ is the bit generation rate determined from the coincidence rates D1–D2 and D3–D4. If $N$ is the number of total bits in the sequence, the number of error bits is $NR_B/2f$. The BER thus is calculated to be

$$\mathrm{BER} = \frac{R_B}{2f}. \tag{2}$$

The above relation was tested by measuring the BER versus the clock frequency. In this experiment, $R_B = 668\,\mathrm{Hz}$, as determined from the coincidence rates. Figure 4 shows the experimental data that are in good agreement with Eq. (2).

Another potential source of error is due to the fact that the SPDC process is in fact described by

$$|\psi\rangle = |0\rangle + \eta|1\rangle_1 \otimes |1\rangle_2 + \eta^2|2\rangle_1 \otimes |2\rangle_2 + \ldots, \tag{3}$$

where $\eta$ is the pair-photon generation efficiency. The effect of the double-pair amplitude, which is proportional to $\eta^2$, on the QRNG scheme can be studied by evaluating the state at the output of the FBS in Fig. 1, which is due to the double-pair amplitude at the input. It is straightforward to show that the double-pair amplitude, $|2\rangle_1 \otimes |2\rangle_2$, at the input modes of the FBS in Fig. 1, with the Hong–Ou–Mandel interference condition satisfied, is unitarily transformed to

$$\frac{\sqrt{6}}{4}(|4\rangle_3 \otimes |0\rangle_4 + |0\rangle_3 \otimes |4\rangle_4) + \frac{|2\rangle_3 \otimes |2\rangle_4}{2}. \tag{4}$$

The first two amplitudes in Eq. (4) correspond to the four-photon photon-number–path entangled state. Thus, the double-pair amplitude in Eq. (3) can actually be used to generate random bit sequences by using proper projection measurement schemes and by assigning bit values of 1 and 0 to the $|4\rangle_3 \otimes |0\rangle_4$ and $|0\rangle_3 \otimes |4\rangle_4$ measurements, respectively.

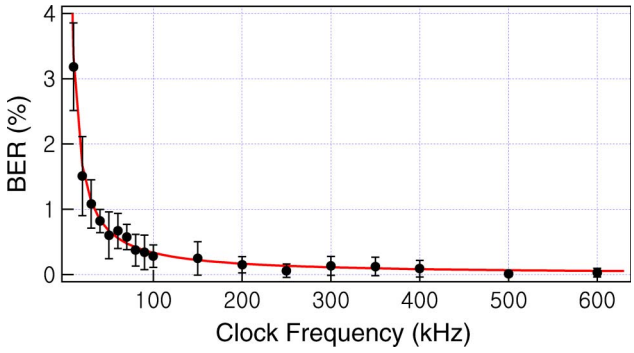


Fig. 4. (Color online) BER versus the counting clock frequency. The solid curve represents Eq. (2) with $R_B = 668\,\mathrm{Hz}$. The filled circles represent the experimental data with one standard deviation error bar.

The third amplitude in Eq. (4) would then contribute to the error, and this is the only amplitude that could cause D1–D2–D3–D4 fourfold coincidences in the scheme shown in Fig. 1. However, since $\eta \ll 1$ even in the case of ultrabright entangled photon sources [21], the double-pair term can be ignored in most situations. Furthermore, in our experiment, we constantly monitored the D1–D2–D3–D4 fourfold coincidences but observed none. We therefore conclude that errors to the random bit sequences in our scheme arise only from multiple D1–D2 or D3–D4 coincidences within the clock period and, thus, the BER is well described by Eq. (2).

### 4. Unbiasing and Randomness Test

Random bit sequences are recorded at a clock frequency of 500 kHz where the experimental BER is zero; higher clock rates do not improve the random bit generation rate. To make sure the two-photon state in Eq. (1) is maintained for the duration of the random bit recording session, the D1–D3 coincidence was monitored at all times; nonzero D1–D3 coincidence events are not present in our experimental data.

The 0 and 1 recorded random binary sequences should, in principle, be unbiased, i.e., the number of 0s and 1s should be the same. However, due to experimental imperfections, such as detection efficiency mismatches and different optical losses, the 0s occur somewhat less than the 1s in our experiment as shown in Figs. 2(b) and 2(c). We thus applied the well-known unbiasing algorithm to the recorded bit sequence: two successive bits are grouped together, forming four possible pairs: 00, 01, 10, and 11. If the binary sequence is biased, the probabilities of 00 and 11 are not equal so we discard these groups. The probabilities of 01 and 10 are, however, equal so we convert the bit group 01 as 0 and 10 as 1 [22,23]. As a result, we are left with a set of unbiased random binary sequence of 0s and 1s. In our experimental data, the length of the final unbiased bit sequence was 23.96% of that of the original biased bit sequence.

Three sets of 1 Mbit long (1,009,000 to be exact) unbiased random binary sequences are recorded and the randomness of the sequences are tested by using the widely used NIST statistical test suite (STS) [24]. The STS consists of a set of 15 randomness tests, evaluating the P value to quantify the randomness of the sequence. In short, if the P value is less than significance level $\alpha$, the STS concludes that the sequence is not random with a confidence of $1-\alpha$. The significance level of 0.01 (the default setting of the STS and a common value used in cryptography) was chosen for the tests and the three random sequences passed all the tests in the STS; see Table 1. We note that the STS test does not guarantee randomness unless the length of the sequence is infinitely long [24]. The results, however, indicate the absence of any statistical patterns in the sequence.

Table 1. Results (P Values) of the Statistical Randomness Test Obtained with the NIST STS [24] [a]

| Test | Set 1 | Set 2 | Set 3 |
|---|---|---|---|
| Approximate entropy | 0.03385 | 0.89904 | 0.05049 |
| Block frequency | 0.02526 | 0.59674 | 0.04524 |
| Cumulative sums | 0.24325 | 0.68146 | 0.44076 |
| FFT | 0.10392 | 0.31056 | 0.31494 |
| Frequency | 0.22990 | 0.94286 | 0.36920 |
| Linear complexity | 0.23791 | 0.13744 | 0.55239 |
| Longest run | 0.23024 | 0.54439 | 0.38463 |
| Nonoverlapping templates | 0.53029 | 0.54345 | 0.51499 |
| Overlapping template | 0.80689 | 0.66523 | 0.49260 |
| Rank | 0.97541 | 0.34506 | 0.91025 |
| Random excursions | 0.56713 | 0.56957 | 0.76068 |
| Random excursions variant | 0.39073 | 0.52697 | 0.74450 |
| Runs | 0.92430 | 0.13432 | 0.51448 |
| Serial | 0.24637 | 0.32450 | 0.26694 |
| Universal | 0.40244 | 0.79281 | 0.75569 |

[a]Three sets of 1 Mbit long unbiased random binary sequences generated by the QRNG were tested. These results indicate that there are no statistical patterns in the tested random number sets.

## 5. Summary

In summary, we demonstrated a novel quantum random number generator based on the two-photon photon-number–path entangled state. Since the randomness in our scheme is based on the projection measurement of the entangled two-photon state, the bit sequence is truly quantum mechanically random. In addition, our QRNG scheme is simple to implement and characterize compared with other schemes. Finally, we note that the random bit generation rate can be substantially improved by utilizing a high-brightness two-photon source based on quasi-phase-matched crystals [21].

This research was supported, in part, by the Korea Science and Engineering Foundation, R01-2006-000-10354-0, the Korea Research Foundation, KRF-2006-312-C00551, and the Ministry of Knowledge and Economy of Korea through the Ultrashort Quantum Beam Facility Program.

## References

1. T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," Rev. Sci. Instrum. **71**, 1675–1680 (2000).
2. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," J. Mod. Opt. **47**, 595–598 (2000).
3. P. X. Wang, G. L. Long, and Y. S. Li, "Scheme for a quantum random number generator," J. Appl. Phys. **100**, 056107 (2006).
4. H.-Q. Ma, Y. Xie, and L.-A. Wu, "Random number generation based on the time of arrival of single photons," Appl. Opt. **44**, 7760–7763 (2005).
5. M. Stipcevic and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," Rev. Sci. Instrum. **78**, 045104 (2007).
6. M. A. Wayne, G. Akselrod, E. R. Jeffrey, and P. G. Kwiat, "High-speed quantum random number generation," in *International Conference on Quantum Information* (Optical Society of America, 2007). paper JWC49.
7. H.-Q. Ma, S.-M. Wang, D. Zhang, J.-T. Chang, L.-L. Ji, Y.-X. Hou, and L.-A. Wu, "A random number generator based on quantum entangled photon pairs," Chin. Phys. Lett. **21**, 1961–1965 (2004).
8. M. Fiorentino, C. Santori, S. M. Spillane, R. G. Beausoleil, and W. J. Munro, "Secure self-calibrating quantum random-bit generator," Phys. Rev. A **75**, 032334 (2007).
9. C. K. Hong and L. Mandel, "Experimental realization of a localized one-photon state," Phys. Rev. Lett. **56**, 58–60 (1986).
10. Implementation of the beam splitter QRNG scheme reported in Ref. [8] makes use of only the signal photon of the SPDC signal–idler photon pair. The scheme, therefore, is equivalent to illuminating a beam splitter with a weak thermal light [11,12].
11. D. V. Strekalov, Y.-H. Kim, and Y. Shih, "Experimental study of a subsystem in an entangled two-photon state," Phys. Rev. A **60**, 2685–2688 (1999).
12. S.-Y. Baek, O. Kwon, and Y.-H. Kim, "Temporal shaping of a heralded single-photon wave packet," Phys. Rev. A **77**, 013829 (2008).
13. S. Takeuchi, "Beamlike twin-photon generation by use of type II parametric downconversion," Opt. Lett. **26**, 843–845 (2001).
14. Y.-H. Kim, "Quantum interference with beamlike type-II spontaneous parametric down-conversion," Phys. Rev. A **68**, 013804 (2003).
15. C. K. Hong, Z. Y. Ou, and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," Phys. Rev. Lett. **59**, 2044–2046 (1987).
16. Generally speaking, although commonly in use, it is incorrect to say that two photons must simultaneously arrive at a beam splitter to exhibit two-photon quantum interference. The condition for observing two-photon quantum interference involving a beam splitter is that the two biphoton detection amplitudes be indistinguishable. It is in fact possible to observe two-photon quantum interference without actually overlapping two photons at the beam splitter. See Refs. [17–19].
17. T. B. Pittman, D. V. Strekalov, A. Migdall, M. H. Rubin, A. V. Sergienko, and Y. H. Shih, "Can two-photon interference be considered the interference of two photons?," Phys. Rev. Lett. **77**, 1917–1920 (1996).
18. Y.-H. Kim, "Two-photon interference without bunching two photons," Phys. Lett. A **315**, 352–357 (2003).
19. Y.-H. Kim and W. P. Grice, "Quantum interference with distinguishable photons through indistinguishable pathways," J. Opt. Soc. Am. B **22**, 493–498 (2005).
20. Y.-H. Kim and W. P. Grice, "Observation of correlated-photon statistics using a single detector," Phys. Rev. A **67**, 065802 (2003).
21. A. Fedrizzi, T. Herbst, A. Poppe, T. Jennewein, and A. Zeilinger, "A wavelength-tunable fiber-coupled source of narrowband entangled photons," Opt. Express **15**, 15377–15386 (2007).
22. J. von Neumann, "Various techniques used in connection with random digits," National Bureau of Standards Applied Mathematics Series No. 12, (National Bureau of Standards, 1951), pp.36–38.
23. Y. Peres, "Iterating von Neumann's procedure for extracting random bits," Ann. Stat. **20**, 590–597 (1992).
24. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Publication 800-22 (NIST, 2008), http://csrc.nist.gov/rng/.