Entangled quantum-key-distribution randomness

I. J. Owens,* R. J. Hughes, and J. E. Nordholt
Physics Division, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA
(Received 7 May 2008; published 5 August 2008)

Random number generators are important components of information security systems. In particular, cryptography standards require that the numbers generated by quantum key distribution applications meet a rigorous set of standardized randomness tests. To date, implementations of entangled quantum key distribution (EQKD) have not included any randomness assessment. We report on the results of randomness tests and highlight how typical EQKD system operation affects the successes and failures in meeting the fundamental test criteria.

DOI: 10.1103/PhysRevA.78.022307 PACS number(s): 42.50.Ex, 03.67.Dd, 42.65.Lm

INTRODUCTION

The growing field of quantum information science and advances in computational complexity threaten modern and present-day cryptography systems. Quantum key distribution (QKD) has emerged as a technology to counter these threats. In QKD, a random bit string or key is established between two parties through a quantum communication channel. This key is often established using the polarization of photons, and the randomness of the bit sequence is an important part of the security guarantee. Randomness tests have been applied to both attenuated [1] and entangled light sources [2,3]. For weak laser quantum key distribution (WLQKD), an external random number generator determines the state that is sent by the transmitter. It is important that this number source provides true random numbers to ensure sufficient entropy in the final key. A properly tuned entangled quantum key distribution (EQKD) source produces its own random numbers, a fact which potentially has security advantages. However, published papers [4–8] on the topic of EQKD have either not examined the foundational importance of randomness or limited statistical testing to the postprocessed portion of the key and not included both the raw sifted bits and basis selection in the analysis [2,3]. It is important to test the raw sifted bits and basis selection because postprocessing procedures such as entropy filtering, error correction, and privacy amplification hide the true entropy content of the bit sequence. In this note, we describe the outcome of standardized randomness tests of both the raw sifted bits and basis selection in an entangled photon implementation of the BB84 protocol to examine the true viability of entangled photon source as a random number generator in an EQKD system. In particular, we highlight the elements of practical EQKD systems and how the device physics and system control affect randomness outcomes.

DESCRIPTION OF SPDC PROCESS AND DETECTION

In our experiment, we produced entangled photons generated by the process of spontaneous parametric down conversion (SPDC). The SPDC process occurs when a laser beam photon of angular frequency ω_p pumps a crystal with a $\chi^{(2)}$ nonlinearity creating correlated pairs of photons that are historically referred to as the signal and idler. Energy and wave-vector momentum conservation lead to pairs with a high degree of temporal and spatial correlation as follows:

$$\omega_p = \omega_s + \omega_i,$$

$$\underline{k}_p = \underline{k}_s + \underline{k}_i,$$

where ω refers to the frequency and $\underline{k}$ the wave vector of the pump p, signal s, and idler i photons, respectively.

A β-barium borate (BBO) crystal-based entangled photon source is the basis of the EQKD setup which includes channel optics and detectors as shown in Fig. 1. The core of the EQKD source consists of a pair of crossed type I phase matched BBO crystals sandwiched together [9] with their optical axes orthogonal to one another. The pump's polarization vector was placed at 45° to these axes, and the two crystals are thin enough (~200 μm combined) that both are within the pump laser's coherence length, and the down-conversion amplitudes within the two crystals are coherent. In Fig. 1, a half wave plate (HWP) and quarter wave plate (QWP) are used to rotate the 400 nm ultraviolet (UV) pump polarization and phase before it enters the BBO crystal to ensure that the pump beam is polarized in the correct orientation when it enters the crystal. In cryptography, a transmitter is often referred to as Alice and a receiver as Bob. In this system, Alice and Bob are composed of identical hardware and we designate both Alice and Bob as receivers. Alice and Bob use a beam splitter (BS), wave plates, and polarizing beam splitters (PBS) to randomly select a basis and measure each of four linearly polarized states horizontal (H), vertical (V), diagonal (D), or antidiagonal (A). Each particular state represents either a 0 or 1 that is used to create a binary string. We defined the bases labels as H/V ("X") and D/A ("Z").

The system consists of two optical receivers which make what should be a random basis selection and then determine the bit values of each photon. Each Alice and Bob optical receiver contained a set of four passively quenched silicon avalanche photodiodes (SiAPDs) and a 780-nm-long pass filter at the entrance. The optical receiver records time stamps in each of the four polarization state detectors with each receiver's respective time interval analyzer (TIA) board as shown in Fig. 1. Each TIA board is fed with a one pulse

*iowens@lanl.gov

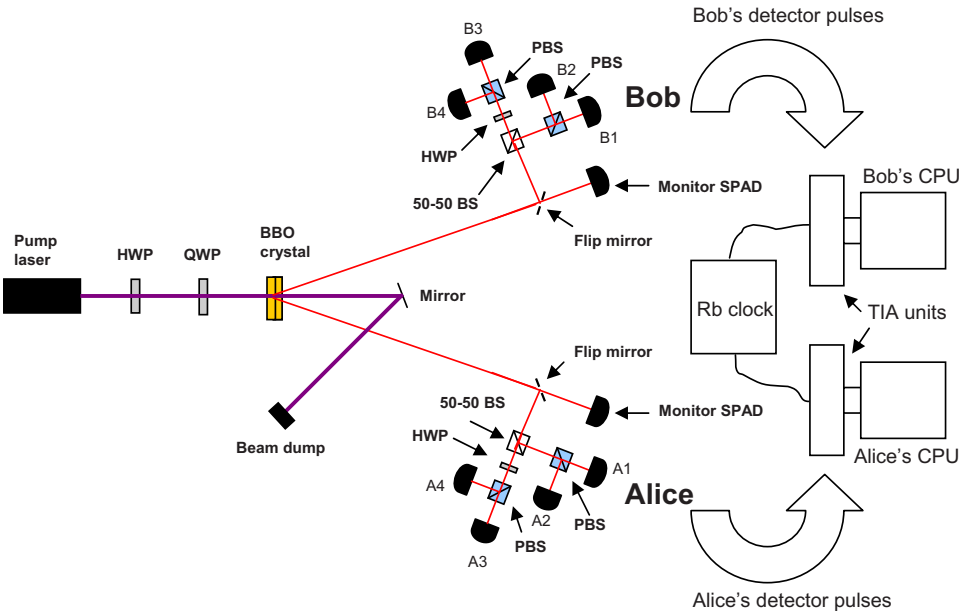

FIG. 1. (Color online) EQKD setup with entangled photon source, channel optics, rubidium (Rb) clock, time interval analyzer (TIA) units, and single photon avalanche diode (SPAD) detectors.

per second reference signal and 10 MHz rubidium (Rb) reference clock signal for timing accuracy. The time stamp information for each detector is recorded and filed by instrumentation software. Each timing board channel is represented by a particular bit value (0 or 1) and basis (X or Z). Alice sends all of her time stamps to Bob in two separate blocks that are sorted by basis, but not bit value. After Bob receives Alice's time stamp blocks, he combines them with his blocks of time stamps and analyzes them using a cross correlation analysis. The time stamps were correlated with an iterative technique that selects timing events that occur within a 1 ns coincidence window. After the coincidences are generated, Bob uses the indices of the correlated time stamp locations to generate his raw key and sends a set of sifted bit location indices to Alice. At this point in the acquisition, Alice and Bob have created the sifted bit strings that are required for randomness tests.

DETECTOR COUNT RATES AND VISIBILITY

We recorded the individual count rates on all eight detectors and the four coincidence count rates for the bit values combinations and joint basis selection. A list of the individual and coincidence combination detector counts is shown in Figs. 2(a)–2(f). Variations in the efficiency for each detector optical path made it intractable to perfectly balance the individual count rate on each detector. However, increasing or decreasing the detector excess bias voltage enhances or lowers the photon detection probability and subsequent count rate allowing some flexibility for count rate balance [10]. We adjusted the voltage bias on each detector such that the overall coincidence counts remained within 5% for each detector combination that represents a bit value (0 or 1) in the short duration (1.77 and 3.12 h) data runs as shown in Figs. 2(b) and 2(d). A 5% balance between the detector count rates is required to ensure an even distribution of zeros and ones. A block of 20 000 bits was sampled for each data set in the short duration test, but all 1 529 016 bits were used from the long duration (68 h) data. For the long duration data runs, fixed adjustment of the voltage bias was not sufficient to guarantee that all four coincidence count combinations would be balanced within 5% as shown in Fig. 2(f).

In addition to detector count rates, we measured the source and system entanglement visibility to ensure that Alice's and Bob's bits are closely matched for consistent and accurate randomness testing and comparison. We determined the source entanglement visibility by measuring the polarization of entangled photons along two angles α and β for each photon in a pair at Alice's and Bob's actively quenched monitor SPAD detectors as shown in Fig. 1, and measuring the number of coincident detection events for each axis orientation $N(\alpha,\beta)$, the visibility can be written as

$$v = [N(\alpha,\beta)_{\max} - N(\alpha,\beta)_{\min}]/[N(\alpha,\beta)_{\max} + N(\alpha,\beta)_{\min}], \quad (1)$$

where the "max" and "min" states correspond to parallel and crossed polarizers, respectively. The source visibility was measured to be 99.9% in the H/V basis and 96.3% in the D/A basis. We used flip mirrors to redirect the entangled beams to the optical receivers and recorded the total system visibility by using the coincidence count rates obtained in each individual basis during the data acquisition for the randomness tests. For the short duration run, the total visibility for both bases was 95% as shown in Fig. 3. During the longer duration run, the total visibility declined throughout the duration of the scan and dropped to an average of 92% as indicated in Fig. 4. It is important to note that as the overall system visibility decreases, it is less likely that both Alice's and Bob's zero and one values will be balanced together due to the increased bit error rate.

DESCRIPTION OF RANDOMNESS TESTING AND RESULTS

A variety of different statistical tests can be applied to a bit sequence to evaluate and compare to a true random se-

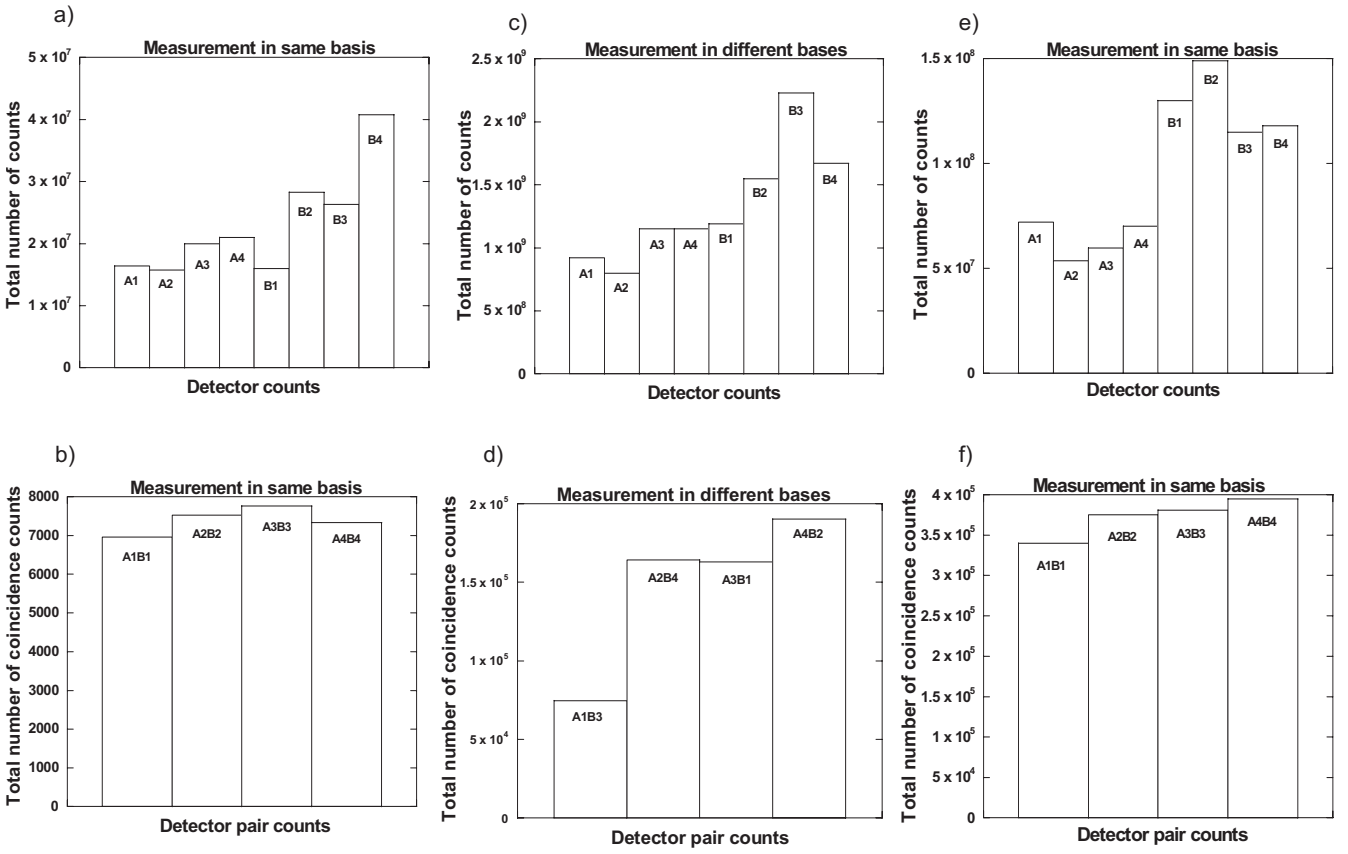

FIG. 2. Alice's and Bob's short [(a)–(d)] and long [(e) and (f)] duration individual and coincidence combination detector counts.

quence. The National Institute of Standards and Technology (NIST) federal information processing standards (FIPS) security requirements for cryptographic modules 140-2 tests [11] were performed as well as the more extensive special publication NIST 800-22 [12] suite. These tests are intended to test random number generators that may be used for many purposes including cryptography, modeling, and simulation applications. The FIPS 140-2 was performed on individual bit streams that contained 20 000 bits and on bit stream blocks within the longer duration data sets with 1 493 016 bits each. For the FIPS-140-2 tests a label of success or failure is used to indicate the appearance of randomness for the frequency (monobit), poker, runs, and long runs tests. The frequency test counts the number of ones in the 20 000 bit stream. The poker test divides the bit stream into 5000 consecutive 4-bit segments to count the number of oc-

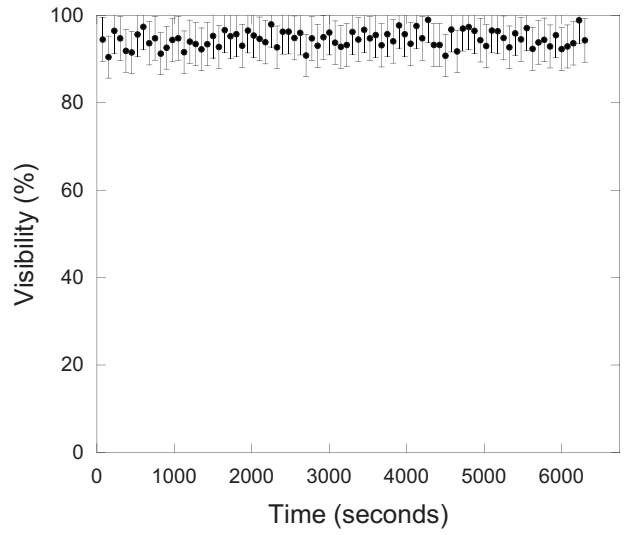

FIG. 3. Total visibility measured during the short duration data run.

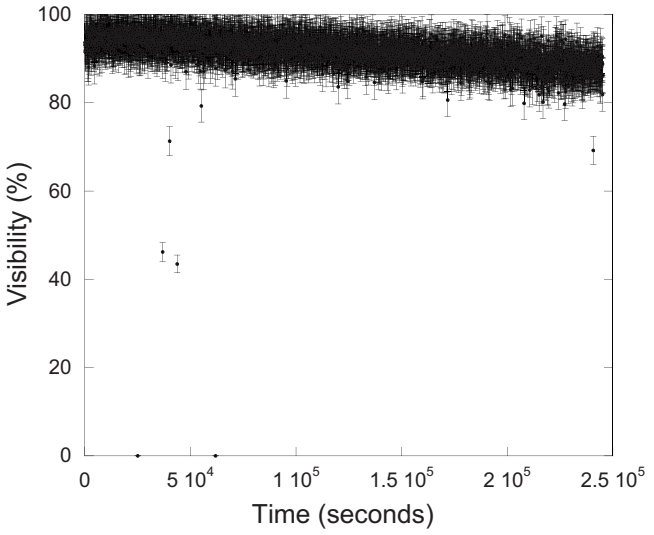

FIG. 4. Total visibility measured during the long duration data run.

TABLE I. NIST 800-22 test of Alice's, Bob's, and joint basis selection long duration data bits.

Test description	Alice's P values	Alice's results	Bob's P values	Bob's results	Basis selection P values	Basis selection results
Frequency	0.050467	Success	0	Failure	0	Failure
Runs	0	Failure	0	Failure	0	Failure
Long runs	0	Failure	0	Failure	0	Failure
Random binary matrix	0.540191	Success	0.065466	Success	0.634269	Success
Discrete Fourier transform	0.310393	Success	0.043048	Success	0.105728	Success
Nonperiodic templates	0.1246	Success	0.1207	Success	0.1101	Success
Overlapping templates	0	Failure	0	Failure	0	Failure
Universal test	0	Failure	0	Failure	0	Failure
Linear complexity	0.510840	Success	0.765907	Success	0.252626	Success
Approximate entropy	0	Failure	0	Failure	0	Failure
Random excursions	NA	Failure	NA	Failure	NA	Failure
Random excursions variant	NA	Failure	NA	Failure	NA	Failure
Block frequency	0	Failure	0	Failure	0	Failure
Serial	0.084557	Success	0.158937	Success	0.164428	Success
Cumulative sums (forward)	0	Failure	0	Failure	0	Failure
Cumulative sums (backward)	0	Failure	0	Failure	0	Failure

currences of the 16 possible 4-bit values. The runs test is defined by the maximal sequence of consecutive bits of either all ones or all zeros that is part of the incidence of runs of all lengths in the stream. The long runs tests check for a sequence of ones or zeros of length 26 or more. The detector count rates were balanced such that all of the FIPS-140-2 tests yielded successful results. These tests were performed as a basic detector balance check before starting the extensive NIST-800-22 tests with the longer duration data sets. To perform all 16 tests in the NIST 800-22 suite required the longer data sets with more than a million bits. A detailed description of each of the 16 tests is provided on the NIST website [12]. For each test in the NIST-800-22 test a P value was determined. We selected a standard significance level α of 0.01. A summary of the results for the NIST 800-22 is shown in Table I.

In addition to random binary bit strings, quantum key distribution protocols such as the standard BB84 and its modified forms require that Alice's and Bob's individual bits are not correlated with their joint basis selection. To test for the existence of correlation between Alice's and Bob's bits and their joint basis selection, the Pearson correlation test was performed. An average correlation coefficient and P value was calculated for all cases.

DATA DISCUSSION

The results of the tests showed that it is possible to set the voltage bias on each detector to balance the count rates needed to meet the FIPS-140-2 test criteria for the short duration data streams. These tests were conducted for instances where Alice and Bob measure in the same and different bases as well as their joint basis selection. However, for the longer duration run, individual data streams randomly pass and fail the FIPS-140-2 tests for Alice's and Bob's bit values and their basis selection. All tests yielded a success or failure conclusion except for the random excursions test which indicated that there were an insufficient number of cycles to generate a P value. In addition to randomness we tested for a correlation between bit value and individual basis selection. The average correlation coefficient ($C_{\mathrm{av}}=-0.00414$) and P value ($P_{\mathrm{av}}=0.001\,166$) obtained from all of the Pearson correlation tests combined indicated that Alice's and Bob's bit values were not correlated with the binary sequence that represented their joint basis selection.

There are many experiment-based factors to consider in assessing the quality of agreement to randomness criteria. For example, increasing the laser power changes the data acquisition rate allowing for the possibility of creating more bits for statistical comparison, but not the actual randomness of the data sequence itself. Electronic considerations such as detector dark counts (<1 kHz) and timing jitter (<1 ns) are themselves inherently random processes and do not affect the randomness of the data. Optical components such as 50/50% beam splitters are highly sensitive to mechanical alignment making it difficult to equalize the light output for the two transmission paths. Multiple detectors with different quantum efficiencies are used making it virtually impossible to balance the ratio of detector output pulses without compensation. It is possible to mitigate for the difference in detector quantum efficiency by placing neutral density filters in front of the detectors or adjusting the voltage bias applied to the passively quenched diodes. However, the data demonstrates that it was not possible to consistently meet the randomness criteria for each test in a long duration data run by balancing the detector pair coincidence count rates with a fixed detector voltage bias. This type of system requires an algorithm for automated control of the voltage bias to ensure that each individual block passes. Further, the data indicates a slow and gradual decrease in the overall visibility throughout the

longer duration data run. The decrease in the visibility scales directly with an increase in the error rate between Alice's and Bob's bit strings making it implausible that both of their raw sifted keys will pass the randomness test. This drift in visibility is likely due to fluctuations in crystal and detector temperature and could be alleviated by active temperature control of both elements.

SUMMARY

We performed standardized randomness and correlation tests on the raw sifted bits and basis selection strings intended for EQKD operation. It was important to test the raw sifted bits and joint basis selection because this is the part of the QKD key that shows true suitability for generating high quality cryptographic numbers. The short duration data runs easily met the FIPS-140-2 randomness criteria which served as a starting point for examining the longer duration data runs. For the longer duration data runs, the device physics involved in balancing the detector coincidence count rates prevented consistent randomness outcomes for the NIST 800-22 test suite. In the future, it will be useful to obtain at least 100 data streams that contain a million bits for each test to permit more rigorous adherence to the selected significance level. Pearson correlation coefficients tests indicated that Alice's and Bob's bit strings do not show any simple correlation with their joint basis selection as required for a practical QKD protocol. Improvements in the automation control of the data acquisition will likely allow enhanced ability for raw EQKD sifted bits to satisfy standardized randomness criteria.

ACKNOWLEDGMENTS

The authors thank Jim W. Harrington, Danna Rosenberg, Charles G. Peterson, and Marco Fiorentino for helpful discussions and software assistance. Financial support from the Intelligence Community (IC) is gratefully acknowledged.

[1] M. A. Hai-Qiang *et al.*, Appl. Opt. **44**, 36 (2005).
[2] M. A. Hai-Qiang *et al.*, Chin. Phys. Lett. **21**, 1961 (2004).
[3] M. Fiorentino *et al.*, Phys. Rev. A **75**, 032334 (2007).
[4] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000).
[5] D. G. Enzer, R. J. Hughes, C. G. Peterson, and P. G. Kwiat, New J. Phys. **4**, 45 (2002).
[6] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).
[7] C. Z. Peng, T. Yang, X. H. Bao, Jun Zhang, X. M. Jin, F. Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B. L. Tian, and J. W. Pan, Phys. Rev. Lett. **94**, 150501 (2005).
[8] I. Marcikic, A. Linares, and C. Kurtsiefer, Appl. Phys. Lett. **89**, 101122 (2006).
[9] P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, Phys. Rev. A **60**, R773 (1999).
[10] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, Appl. Opt. **35**, 1956 (1996).
[11] NIST FIPS 140-2, http://csrc.nist.gov/publications/PubsFIPS.html.
[12] NIST special publication 800-22, http://csrc.nist.gov/rng/.