ISSN 1054-660X, Laser Physics, 2008, Vol. 18, No. 6, pp. 810–814.

Implementation of Polarization-Coded Free-Space BB84 Quantum Key Distribution

Y.-S. Kim, Y.-C. Jeong, and Y.-H. Kim

Department of Physics, Pohang University of Science and Technology (POSTECH), Pohang, 790-784, Korea
e-mail: yoonho@postech.ac.kr

Received December 9, 2007

Abstract—We report on the implementation of a Bennett–Brassard 1984 quantum key distribution protocol over a free-space optical path on an optical table. Attenuated laser pulses and Pockels cells driven by a pseudo-random number generator are employed to prepare polarization-encoded photons. The sifted key generation rate of 23.6 kbits per second and the quantum bit error rate (QBER) of 3% have been demonstrated at the average photon number per pulse $\mu = 0.16$. This QBER is sufficiently low to extract final secret keys from shared sifted keys via error correction and privacy amplification. We also tested the long-distance capability of our system by adding optical losses to the quantum channel and found that the QBER remains the same regardless of the loss.

PACS numbers: 03.67.Dd, 03.67.Hk, 42.79.Sz

DOI: 10.1134/S1054660X08060212

1. INTRODUCTION

Quantum cryptography or quantum key distribution (QKD) allows two distant parties, Alice and Bob, to share a string of random bits (0s and 1s) or cryptographic keys securely from an eavesdropper [1]. Since the security of quantum cryptography is based on the laws of quantum physics, it provides the most secure way of distributing cryptographic keys.

Since its first proposal in 1984 by Bennett and Brassard (BB84) [2], quantum cryptography research has progressed rapidly both theoretically and experimentally. Theoretically, new quantum cryptography protocols (such as the entanglement-based Ekert protocol [3], the two-state B92 protocol [4], the orthogonal state Goldenberg–Vaidman scheme [5], the six-state protocol [6], the decoy-state protocol [7], etc.) have been proposed and rigorous security proofs of some of these QKD protocols have been discovered [8–10]. Furthermore, it has been shown that QKD could be implemented using weak coherent states if the average photon number per pulse μ is sufficiently small ($\mu < 1$), although original quantum cryptography protocols have been developed for single-photon states or entangled-photon states [1, 11]. Experimentally, QKD implementations have been demonstrated over the distance of tens of kilometers in optical fibers [13–17], several kilometers in free space [18–21], and recently, QKD has been demonstrated even over 100 km in free space [22].

Experimental implementations of free-space QKD reported to date usually involve custom-made electronics and optics and complete system control (including electronics, raw key generation, key sifting, error correction, and privacy amplification) was normally implemented with dedicated software [18–22]. Efforts are now being made to reduce the cost of building a QKD system by using more and more commercially available devices [23]. In this paper, we report a long-distance capable free-space BB84 QKD system which is built only with commercially available optics and PC-based control electronics. The complete system control was implemented using the LabVIEW programming language and the QKD system operates at the clock rate of 1 MHz. Our free-space QKD system, nevertheless, exhibits a quantum bit error rate (QBER) as low as 2.8% at the sifted key generation rate of tens of kilohertz. The long-distance capability of our QKD system was tested experimentally by adding the optical losses to the quantum channel and we have found that the QBER remains the same regardless of the loss.

Let us first briefly discuss the BB84 quantum cryptography protocol, which makes use of two sets of nonorthogonal basis states of a single photon [2]. Typically, the four polarization states are chosen to form the two linear nonorthogonal basis states, namely, the $\{|H\rangle, |V\rangle\}$ basis and the $\{|-45°\rangle), |+45°\rangle)\}$ basis. Alice and Bob must agree via the public channel that the bit value 0 is to be encoded in the polarization states $|H\rangle$ or $|-45°\rangle$ and the bit value 1 is to be encoded in $|V\rangle$ or $|+45°\rangle$.

Alice initiates the quantum key distribution process by generating a random sequence of 0s and 1s (Alice's raw key) and encoding them into the polarization state of a photon using the randomly selected nonorthogonal basis states, the $\{|H\rangle, |V\rangle\}$ basis or the $\{|-45°\rangle, |+45°\rangle\}$ basis (see Fig. 1). The polarization-encoded photons are then launched to Bob. Bob then randomly selects the measurement basis for each incoming photon and records the detection events (i.e., measured polarization states) as well as the measurement basis associated with each detection event. Bob's detection events are then

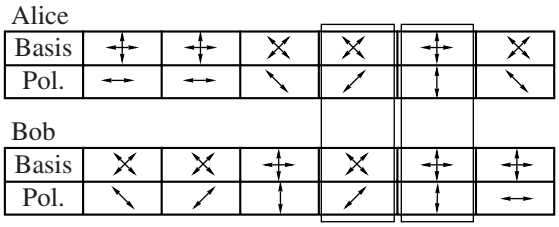

Fig. 1. BB84 QKD protocol. Shared key bits are generated only when the basic choices, which are announced publicly, of Alice and Bob are the same.

converted back to a series of 0s and 1s to form Bob's raw key, which inherently contains some error bits. This is because, when Alice's and Bob's bases do not match (with a 50% probability), there is a 50% probability that Bob's detection event gives a different bit value than Alice's. If Alice's and Bob's bases do match, they share the same bit values as long as the optical quantum channel is not perturbed in any way.

To establish an identical set of shared error-free keys between Alice and Bob, the key sifting procedure is applied to Alice's and Bob's raw keys. Alice and Bob first announce via a classical public communication channel their state preparation and measurement bases without revealing the actual bit values. They then remove the bit values which came from mismatched basis choices. The key sifting procedure, therefore, throws away 50% of the raw key, on average, to form the sifted key shared by Alice and Bob. If the complete BB84 protocol is implemented with perfect devices and there are no eavesdropping attacks, there will be no error bits in the shared sifted keys.

2. EXPERIMENTAL SETUP

The schematic of our BB84 experimental setup, which consists of the transmitter (Alice), the receiver (Bob), and the quantum and public channels linking Alice and Bob, is shown in Fig. 2. The complete experimental setup was built using only commercially available optical and electronic components.

Let us first discuss the transmitter (Alice) part of the BB84 QKD setup. The photon source in our experiment is a pulsed-diode laser (Coherent, CUBE 785-40C), which emits a train of 5-ns laser pulses at 780 nm. The laser operates at a 1-MHz clock rate, derived from Alice's computer equipped with a digital input/output board (DIO; National Instruments PCI-6534). The laser pulse is then strongly attenuated by using a set of neutral density filters, a half-wave plate, and a polarizer (not shown in Fig. 2), so that the average photon number per pulse $\mu < 1$. The photon pulse is then randomly encoded in one of the four polarization states ($|H\rangle$, $|V\rangle$, $|-45°\rangle$, and $|+45°\rangle$) by using a pair of high-speed RTP Pockels cells (PC1 and PC2; Leysop, RTP-3-20). To generate the encoding signal for the Pockels cells, two sets of pseudorandom strings of 0s and 1s are generated and recorded at Alice's computer. The first random number string is used for Alice's raw key and the other is used to randomly choose the polarization basis. These random number strings are then converted by the DIO to 1-MHz TTL signals to control the two Pockels cells. Since the conversion process takes considerable processing times and memory, we operate the QKD system at the 1-s burst mode. The interval between the successive 1-s bursts varied from 10 to 30 s depending on the available memory at Alice's computer. A beam splitter (BS) then splits the photon pulse in two: the reflected one is used to monitor the average photon number per pulse and the transmitted photon pulse is launched to Bob via a ×5-beam expander (BE).

Bob's setup consists of passive optical components, single-photon detector packages, and a computer equipped with a counter/timer board (National Instruments PCI-6602). Incoming photons are received via a ×5 BE to reduce the beam diameter and an interference filter (IF) with a 3-nm full-width at half-maximum bandwidth is used to cut down the level of environmen-

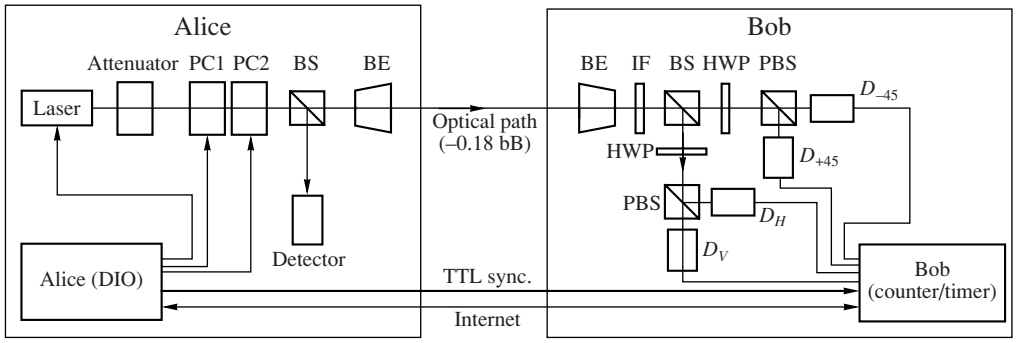

Fig. 2. BB84 QKD experimental setup. The single-photon detectors associated with the measurement basis output ports are labeled as D_H, D_V, $D_{-45°}$, and $D_{+45°}$. See text for details.

Table 1. BB84 QKD experimental results for several different values of μ. The QBER value 2.98 (0.19), for example, refers to 2.98% total QBER, which includes the dark count contribution of 0.19%

μ	Sifted key rate, kbps	QBER, %
0.160	23.6	2.98 (0.19)
0.202	30.4	2.84 (0.15)
0.242	35.5	2.89 (0.13)
0.269	40.4	2.87 (0.11)
0.318	47.4	2.85 (0.09)
0.481	67.5	2.81 (0.07)

tal noise photons. A beam splitter (BS) is then used to randomly direct the incoming photon to one of the two measurement bases $\{|H\rangle, |V\rangle\}$ or $\{|-45°\rangle, |+45°\rangle\}$. As shown in Fig. 2, the polarization measurement basis is set with a half-wave plate (HWP) and a Glan–Thompson polarizing beam splitter (PBS). The orientations of the HWPs are set so that the reflected path of the BS would function as the $\{|H\rangle, |V\rangle\}$ measurement basis and the transmitted path of the BS would function as the $\{|-45°\rangle, |+45°\rangle\}$ measurement basis. A single-photon detection event, for example, at D_V, the detector would mean that the polarization state of the incoming photon has been projected to the state $|V\rangle$.

The single-photon detector package actually consists of the free space to a fiber coupler and a multimode fiber-coupled single-photon counting module (Perkin-Elmer, SPCM-AQR4C). The total detection efficiency of the detector package is measured to be roughly 41% (75% fiber coupling efficiency and 55% quantum efficiency of the single-photon counting module). The dark count rate of the single-photon counting module is measured to be roughly 300 Hz before gating. To minimize the effects of the dark counts, we have gated the single-photon counting modules with a 1-MHz TTL timing pulse so that the detectors are turned on only for about 125 ns or about the expected arrival time of the photon. Finally, the counter/timer which records all of Bob's detection events is synchronized with Alice's setup using the same 1-MHz TTL timing pulse.

The optical link between Alice and Bob is established using a 17-m optical path on the optical table. The optical path, which forms the quantum channel between Alice and Bob, was constructed by using several mirrors and the overall loss is measured to be –0.18 dB. The public channel consisted of a coaxial cable, which carries the TTL timing pulse from Alice to Bob and the internet was used to generate the sifted keys from the raw keys.

3. RESULTS AND DISCUSSION

A set of experiments was performed using several different values of the average photon number per pulse μ. For each experimental run, we record the sifted key generation rate (in bits per second) and evaluate the quantum bit error rate (QBER) of the sifted key. As mentioned earlier, if the QKD is implemented with ideal devices and there are no eavesdropping attacks, Alice's sifted key and Bob's sifted key should be completely identical. Real experimental devices are, however, plagued with imperfections, so that Bob's sifted key is not necessarily identical to Alice's sifted key. For example, imperfections in the Pockels cells, half-wave plates, polarizers, detectors, etc., may all contribute to errors in the sifted key. The error revealed can be quantified by evaluating QBER = $N_{\text{wrong}}/N_{\text{total}}$, which is the ratio between the number of wrong bits (N_{wrong}) to the total number of bits (N_{total}) in some subset of the sifted key.

In our experiments, all optical elements were aligned with great care to keep the effects of the optical imperfections on the QBER as low as possible, and the single-photon counting modules were gated for 125 ns (at 1 MHz) to minimize the effect of the dark counts on the QBER. Furthermore, any detection event at Bob's that reports two or more detectors "clicking" simultaneously is discarded from the sifted key. (Such multiphoton events may have come from the multiphoton pulse or detector dark counts.)

The experimental data are summarized in Table 1. The sifted key generation rate in our experiment varied from 23.6 kbps (kilobytes per second) to 67.5 kpbs depending on the μ value. Note that, although the total QBER appears to be slightly decreasing as we increase μ, this does not mean that the optical alignment of the experimental setup has been changed. It merely reflects the fact that the dark-count contribution (which is random) to the QBER becomes less significant if the number of photon-counting events gets more and more dominant than the random dark counts of the single-photon counting modules.

Next, to investigate the long-distance capability of our BB84 QKD system, we have tested the performance of the BB84 QKD system under additional losses in the optical quantum channel. The additional channel losses were simulated by inserting a set of uncoated glass plates at normal angles to the path of the photon.

This experiment was performed at μ = 0.242 and a total of five glass plates were inserted into the quantum channel one by one. The experimental data for this set of measurements are summarized in Table 2. As expected, the channel loss results in a reduced sifted key generation rate. It is interesting to note that the QBER remains roughly the same while additional channel loss is added. (As before, the dark count contribution to the QBER rises with a reduced sifted key generation rate.)

As mentioned earlier, BB84 QKD implemented with ideal devices would give QBER = 0 if there are no eavesdropping attacks. If there is an eavesdropping

Table 2. Effects of additional channel loss to QBER for $\mu = 0.242$. A set of glass plates is added to the quantum channel to simulate the channel loss

Glass plates	Sifted key rate, kpbs	QBER, %
0	35.0	2.83 (0.13)
1	27.4	2.87 (0.16)
2	26.6	2.97 (0.17)
3	23.2	2.97 (0.19)
4	19.0	2.95 (0.24)
5	17.3	2.99 (0.26)

attack to the quantum channel, the net result, in general, is the increase of the QBER in Alice's and Bob's sifted keys. On the other hand, as we have demonstrated in this paper, a nonzero QBER can also be attributed to imperfect devices. Since the QBER resulted from eavesdropping attacks and the QBER due to imperfect devices are indistinguishable, Alice and Bob must always assume that errors in their sifted keys come from eavesdropping attacks to the quantum channel.

Sifted keys with errors, therefore, cannot be considered secure until classical post-processing procedures (error correction and privacy amplification) are applied to the sifted keys to extract the final secure keys [1]. The QBER value is found to be directly related to the classical post-processing processes (hence, security of the QKD system) and, if the QBER value is too high, no secure keys can be extracted from the sifted keys. For the BB84 QKD protocol, the QBER upper bounds for the nonzero secure key extraction rates from the sifted keys are known to be 11% with a privacy amplification and a one-way error correction and 20% with a privacy amplification and a two-way error correction [9, 10, 24].

For example, if a BB84 QKD system generated sifted keys with QBER = 11%, no final secure keys can be generated if only a one-way error correction is applied to the sifted keys. By using a two-way error correction, it is possible to generate a final secure key, but at the expense of the key generation rate. Interestingly, the final secure key generation rate can be estimated without actually performing the error correction and privacy amplification procedures by using the following relation [24]:

$$\mathcal{R} = 1 - 2\mathcal{H}(\mathrm{QBER}), \quad (1)$$

where $\mathcal{R}$ is the yield of the final secure key from the sifted key, and $\mathcal{H}$ is the binary Shannon entropy $\mathcal{H}(x) = -x\log_2 x - (1-x)\log_2(1-x)$.

Our BB84 QKD system demonstrated a sifted key generation rate of 23.6 kbps at $\mu = 0.16$ with QBER = 3% (see Table 1). From this data set, we estimate that our BB84 QKD system would generate the final secure keys at the rate of 14.5 kbps if classical post-processing procedures were applied to the sifted keys.

4. CONCLUSIONS

We have successfully implemented the BB84 quantum key distribution protocol in free space using attenuated laser pulses as the carrier of the quantum information. The complete QKD system was built using only commercially available optical and electronic components and the Lab VIEW programming language was used for system control and key sifting.

Our QKD system demonstrated a low quantum bit error rate of 3% and this value remained the same even in the presence of additional channel losses applied to the quantum channel. This suggest that our BB84 QKD system is capable of generating final secure keys at a rate close to the sifted key generation rate and is applicable to long-distance quantum key distribution.

Currently, we are in the process of implementing the decoy-state method in the BB84 QKD system we have developed [7]. Additionally, we are upgrading the system electronics to an FPGA (field-programmable gate array) based system for continuous operation.

ACKNOWLEDGMENTS

We would like to thank Won-Young Hwang, Vadim Makarov, and Joonwoo Bae for many helpful discussions and comments. This work was supported in part by the Korea Science and Engineering Foundation (R01-2006-000-10354-0), the Korea Research Foundation (R08-2004-000-10018-0), and the Ministry of Commerce, Industry, and Energy of Korea through the Industrial Technology Infrastructure Building Program.

REFERENCES

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," Rev. Mod. Phys. **74**, 145 (2002).
2. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
3. A. Ekert, "Quantum Cryptography Based on Bells Theorem," Phys. Rev. Lett. **67**, 661 (1991).
4. C. H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States," Phys. Rev. Lett. **68**, 3121 (1992).
5. L. Goldenberg and L. Vaidman, "Quantum Cryptography Based on Orthogonal States," Phys. Rev. Lett. **75**, 1239 (1995).
6. D. Bruβ, "Optimal Eavesdropping in Quantum Cryptography with Six States," Phys. Rev. Lett. **81**, 3018 (1998).
7. W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett. **91**, 057901 (2003).
8. D. Mayers, "Quantum Key Distribution and String Oblivious Transfer in Noisy Channels," in *Advances in Cryptography-Proceedings of Crypto'96*," Lect. Notes Comput. Sci. **1109**, 343 (1996).

9. K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally Secure Key Distribution Based on Two Nonorthogonal States," Phys. Rev. Lett. **90**, 167904 (2003).
10. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of Quantum Key Distribution with Imperfect Devices," Quantum Inf. Comput. **4**, 325 (2004).
11. B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum Cryptography with Coherent States," Phys. Rev. A **51**, 1863 (1995).
12. C. H. Bennett, F. Bessette, G. Brassard, et al., "Experimental Quantum Cryptography," J. Cryptology **5**, 3 (1992).
13. R. J. Hughes, G. G. Luther, G. L. Morgan, et al., "Quantum Cryptography over Underground Optical Fibers," in *Advances in Cryptography-Proceedings of Crypto'96*, Lect. Notes Comput. Sci. **1109**, 329 (1995).
14. C. Marand and P. D. Townsend, "Quantum Key Distribution over Distances as Long as 30 km," Opt. Lett. **20**, 1695 (1995).
15. A. Muller, H. Zbinden, and N. Gisin, "Quantum Cryptography over 23 km in Installed Under-Lake Telecom Fibre," Europhys. Lett. **33**, 335 (1996).
16. D. Stucki, N. Gisin, O. Guinnard, et al., "Quantum Key Distribution over 67 km with a Plug&Play System," New J. Phys. **4**, 41 (2002).
17. C. Gobby, Z. L. Yuan, and A.J. Shields, "Quantum Key Distribution over 122 km of Standard Telecom Fiber," Appl. Phys. Lett. **84**, 3762 (2004).
18. W. T. Buttler, R. J. Hughes, P. G. Kwiat, et al., "Practical Free-Space Quantum Key Distribution over 1 km," Phys. Rev. Lett. **81**, 3283 (1998).
19. W. T. Buttler, R. F. Hughes, S. K. Lamoreaux, et al., "Daylight Quantum Key Distribution over 1.6 km," Phys. Rev. Lett. **84**, 5652 (2000).
20. R. Hughes, J. E. Nordholt, D. Derkacs, et al., "Practical Free-Space Quantum Key Distribution over 10 km in Daylight and at Night," New J. Phys. **4**, 43 (2002).
21. C. Kurtsiefer, P. Zarda, M. Haider, et al., "Long-Distance Free-Space Quantum Cryptography," Proc. SPIE **4917**, 25 (2002).
22. T. Schmitt-Manderbach, H. Weier, M. Fürst, et al., "Experimental Demonstration of Free-Space Decoy-state Quantum Key Distributio over 144 km," Phys. Rev. Lett. **98**, 010504 (2007).
23. J. L. Duligall, M. S. Godfrey, K. A. Harrison, et al., "Low Cost and Compact Quantum Key Distribution," New J. Phys. **8**, 249 (2006).
24. P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys. Rev. Lett. **85**, 441 (2000).