Differential-phase-shift quantum key distribution using coherent light

K. Inoue,[1] E. Waks,[2] and Y. Yamamoto[1,2]
[1]*NTT Basic Research Laboratories, NTT Corporation, Atsugi-shi 243-0198, Japan*
[2]*Quantum Entanglement Project, ICORP, JST, E. L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4085, USA*
(Received 13 February 2003; published 27 August 2003)

Differential-phase-shift quantum key distribution based on two nonorthogonal states is described. A weak coherent pulse train is sent from Alice to Bob, in which the phase of each pulse is randomly modulated by $\{0,\pi\}$. Bob measures the differential phase by a one-bit delay circuit. The system has a simple configuration without the need for an interferometer and a bright reference pulse in Alice's site, unlike the conventional QKD system based on two nonorthogonal states, and has an advantage of improved communication efficiency. The principle of the operation is successfully demonstrated in experiments.

DOI: 10.1103/PhysRevA.68.022317 PACS number(s): 03.67.Dd, 42.50.Dv

Quantum key distribution (QKD) offers an ultimately secure communication based on the laws of quantum mechanics. Several schemes have been proposed, such as those based on four nonorthogonal states [Bennett-Brassard 1984 protcol (BB84)] [1], quantum entanglement [Ekert 1991 protocol (E91), Bennett-Brassard-Mermin 1992 protocol (BBM92)] [2,3], two nonorthogonal states [Bennett 1992 protocol (B92)] [4], and a variant of the four-state scheme [5].

The B92 protocol uses weak coherent light with the setup shown in Fig. 1. Alice sends two sequential coherent pulses by using an unbalanced interferometer: a weak signal pulse and a bright reference pulse. The weak pulse is randomly phase-modulated by $\{0,\pi\}$. Bob measures the signal and reference combined at the output of another unbalanced interferometer in which the phase of one arm is randomly modulated by $\{0,\pi\}$. When the phase modulation is matched between Alice and Bob, Bob can count a photon from which Alice and Bob create a secret key. The security of this scheme is based on the fact that coherent states of light with an average photon number less than one are nonorthogonal when they have opposite phases. If an eavesdropper (Eve) tries an intercept-resend attack, she has to send a fake signal even when she does not measure a photon (inconclusive measurement result) due to the existence of the bright reference pulse. This results in errors, which reveals the presence of the eavesdropping.

This paper presents a QKD system based on two nonorthogonal states. Weak coherent light is sent from Alice to Bob, which is randomly phase-modulated by $\{0,\pi\}$ for each time slot. Even without a bright reference pulse, the system can prevent an eavesdropper from performing an intercept-resend attack.

Figure 2 shows the setup of the proposed system. Alice randomly phase-modulates a pulse train of weak coherent states by $\{0,\pi\}$ for each pulse and sends it to Bob with an average photon number less than one per pulse. Bob divides each incoming pulse into two paths and recombines them by 50:50 beam splitters, where the path-length difference is set equal to the time interval of the sequential pulses. Photon detectors are placed at the two outputs of the recombining beam splitter. At the detectors, the partial wave functions of two sequential pulses interfere with each other, as illustrated in Fig. 2. With an appropriate phase in the interferometer, detector 1 clicks for 0 phase difference between the two consecutive pulses and detector 2 clicks for π phase difference.

Using the above setup, Alice and Bob create a secret key by the following protocol. After raw transmission, Bob tells Alice the time instances at which a photon is counted. From this time information and her modulation data, Alice knows which detector clicked in Bob's site. Under the agreement that the click by detector 1 denotes "0" and the click by detector 2 denotes "1," for example, Alice and Bob obtain an identical bit string.

This bit string can be guaranteed not to be attacked by an eavesdropper as follows. Here, we consider a simple intercept-resend attack using the same measuring setup as Bob's. Because the average photon number per pulse is less than one, an eavesdropper (Eve) does not measure a photon for some time slots. For an unmeasured time slot, she sends a pulse with a randomly chosen phase. From this fake signal, Bob obtains data "1" in the following three different cases: (a) Alice sends "1" $\rightarrow$ Eve measures and resends "1" $\rightarrow$ Bob measures "1," (b) Alice sends "1" $\rightarrow$ Eve measures no photon but resends "1" $\rightarrow$ Bob measures "1," and (c) Alice sends "0" $\rightarrow$ Eve measures no photon but resends "1" $\rightarrow$ Bob measures "1." The probabilities for these cases are approximately $\overline{n}^2$, $(1/2)\overline{n}(1-\overline{n})$, and $(1/2)\overline{n}(1-\overline{n})$, respectively, where it is assumed the average photon number per pulse $\overline{n}$ is much smaller than one. Case (c) introduces a bit error with the probability of $(1-\overline{n})/2$ in Bob's "1." The situation is the same for data "0." Thus, Alice and Bob can find the existence of eavesdropping from this error rate.

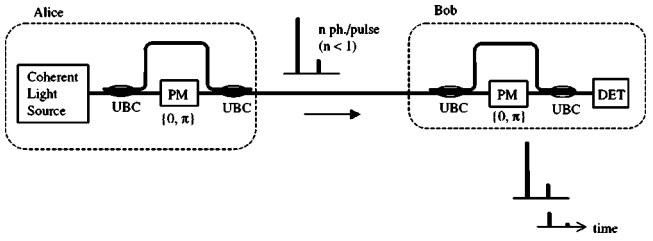

FIG. 1. Configuration of the conventional B92 system. UBC, unbalanced coupler; PM, phase modulator; and DET photon detector.

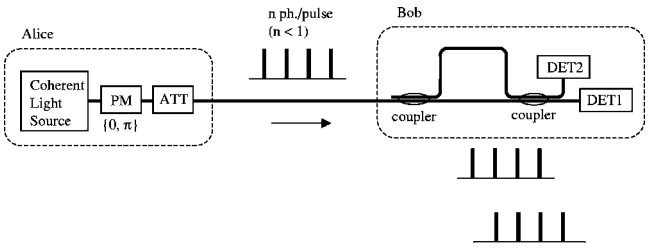

FIG. 2. Configuration of the proposed system. PM, phase modulator; ATT, attenuator; and DET, photon detector.

Another eavesdropping strategy is that Eve sends a signal only when she detects a photon. She sends a single photon split into two time slots through an interferometer identical to Bob's one, in which the relative phase between the two time slots is 0 or π according to the measured phase difference. For unmeasured time slots she sends no photon. This fake signal generates the same count rate in Bob's detectors as the original one. Bob does not notice the eavesdropping from the photon counting rate. However, bit error is introduced from this fake signal as follows. When a photon split into two time slots arrives at Bob's site, he counts a photon possibly at three time instances. First, a photon passes through the short path in Eve's interferometer and the short path in Bob's interferometer. Second, a photon passes through the short path in Eve's and the long paths in Bob's, and through the long path in Eve's and the short path in Bob's. Third, a photon passes through the long path in Eve's and the long path in Bob's. At the second time instance, the detectors click according to the phase difference between the two time slots, which gives a correct answer. Bob does not notice eavesdropping in this case. However, no interference occurs and the detectors click randomly at the first and third time instances. Bit error is introduced from these detection events. The probability of clicks at the first or third time instances is 1/2, thus the error rate is 1/4. The eavesdropping is revealed from this error rate.

In general words, Alice sends coherent states of an average photon number less than one with opposite phases, $|u_0\rangle$ and $|u_1\rangle$. They are nonorthogonal to each other, thus possible measurement results that Eve can obtain are $|u_0\rangle$, $|u_1\rangle$, and an inconclusive one [6]. If Eve resends something in place of the inconclusive result, a bit error can be introduced in Bob's measurement. If she resends a vacuum state instead, that vacuum state can be coupled to a conclusively re-sent state ($|u_0\rangle$, or $|u_1\rangle$) in Bob's interferometer, which can result in a bit error. In both cases, the eavesdropping is revealed by checking some test bits. Unfortunately, however, full security analysis has not been made. It is likely that more sophisticated the intercept-resend strategy Eve follows, more work Bob has to do in order to verify the security of the communication line.

The present system looks similar to differential-phase-shift QKD recently proposed by the authors [7]. The difference is in Alice's configuration; sequential coherent pulses are directly phase-modulated while a single photon is split into three time slots by a three-path delay line before phase modulation in the previous scheme. The present configuration is simpler and thus more practical. Theoretically speaking, four fully nonorthogonal states are utilized in the previous scheme while the present scheme uses two nonorthogonal states.

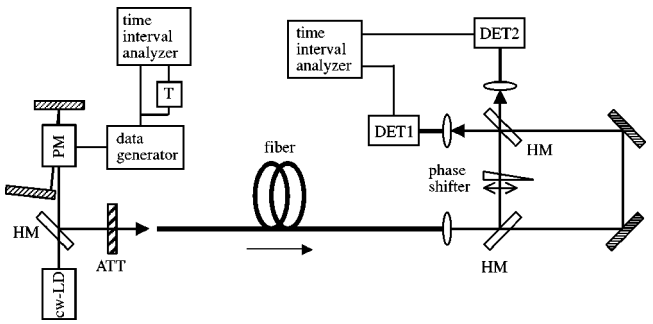

FIG. 3. Experimental setup. PM, phase modulator; ATT, attenuator; HM, half mirror; and DET, photon detector.

This system is suitable for fiber transmissions. The bit information of the above system is carried by the phase difference between two sequential pulses. Though the polarization state changes after propagating through fiber, two sequential pulses experience the same change and thus have the same polarization state at the fiber output, as long as the time interval of two sequential pulses is much shorter than time constant of change in the fiber. This condition is satisfied in actual system, because change in temperature and/or mechanical pressure have slow time constant compared with the pulse interval. Therefore, nearly prefect interference between two sequential pulses is possible. An issue is polarization dependency in the receiver. In the present system, no polarization sensitive device (e.g., optical modulator) is needed in Bob's site, and thus no polarization control is necessary in principle.

The stability in Bob's interferometer is an issue in the differential phase detection. The phase delay in the interferometer, which depends on the optical length and the light wave frequency, should be adjusted so that a photon always clicks detector 1 (or 2) when sequential pulses have 0 (or π) phase difference. Fortunately, our receiver consists of only passive elements. All-passive interferometers can be implemented into one monolithic chip by the silica-based waveguide technology [8–10], in which optical length can be set accurate and stable. Stable and polarization insensitive operation is possible in waveguide circuits. Note that no interferometer is used in Alice's site, unlike conventional phase-encoding QKD systems, which is preferable for simplicity.

A high communication efficiency is another advantage of the proposed system. In conventional B92 protocol [4], the key creation efficiency is $\bar{n}/2$, in which the factor 1/2 reflects the fact that basis-mismatched photons do not contribute to the key creation. On the other hand, the present system utilizes all photons for creating the key, thus the key creation efficiency is $\bar{n}$. In addition, no reference pulse is necessary, so that the clock frequency can be higher than the conventional B92 protocol.

Experiments were carried out to demonstrate the fundamental operation, with the setup shown in Fig. 3. A cw laser diode with an external cavity ($\lambda = 840$ nm) was used as a signal source. By taking data within time windows as de-

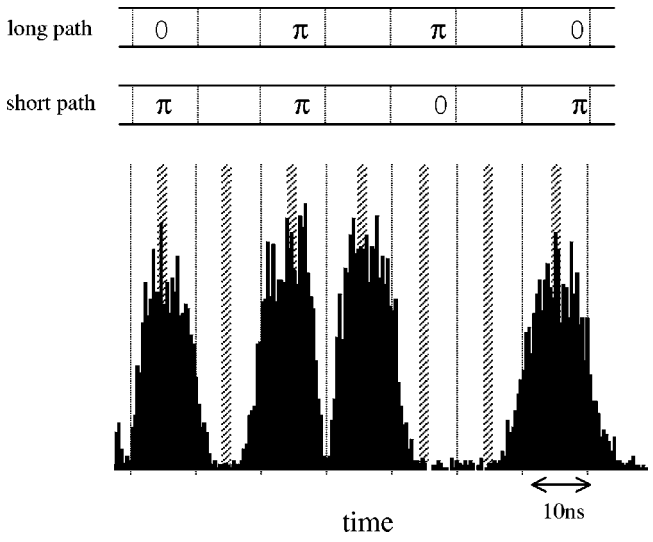

FIG. 4. Histogram of the detected signal at detector 2 for a fixed pattern. Shown above is the corresponding phase-modulation pattern. Data within shaded time windows are taken for sifted data.

scribed later, we can use cw light as a signal carrier at the expense of the efficiency. Note that this source setup can be easily changed to a pulsed light source by placing a high-speed amplitude modulator just after the cw light source, though the cw light was directly used in our experiment simply because we did not have such a modulator. The light from the laser diode was phase-modulated by a phase modulator whose bandwidth was 120 MHz. The modulator was driven by a 100-Mbit/s pseudorandom binary sequence from a data generator. In order to reduce the driving voltage for (0, π) modulation, the setup was constructed for the light to pass through the modulator four times. The modulated light was coupled to a single mode fiber of 20 m length, and then it reached the receiver. The light power input into the fiber was attenuated to be less than one photon per one-bit period on average. In the receiver, the incoming light passed through an open-space Mach-Zehnder interferometer. The path-length difference was 3 m, which introduced one-bit delay of 10 ns at 100 Mbit/s. A phase shifter was placed in the short path for phase adjustment. The two outputs from the interferometer were coupled to single mode fibers in order to achieve good spatial matching for high visibility. The obtained visibility was about 98% for nonmodulation condition. The fiber outputs were coupled to photon detectors. The excess loss in the receiver was about 10 dB, including the quantum efficiency of the detector, the fiber coupling loss, and the loss due to the optical elements.

Figure 4 shows a histogram of photons counted by one detector for a fixed modulation pattern. Since the modulator had a finite response time, the histogram showed a tailing distribution, not an ideal rectanglelike distribution. In transient regions, the detection event is in intermediate states between ''1'' and ''0,'' from which Bob cannot obtain correct answers. In the middle of bit periods, however, the modulator completely switches to ''1'' or ''0.'' Thus, Bob can obtain correct answers by taking data within a time window in the middle of a bit period. While this scheme of using cw light is simpler than the use of pulsed light, a disadvantage is that photons detected outside the time windows are not utilized to create a sifted key, and thus the key creation efficiency is reduced. The reduction ratio depends on the bandwidth of a phase modulator. For a large bandwidth, the width of the time window can be large and the efficiency closes to 1. Note that Eve cannot use a pulsed light source to neatly cheat Bob somehow in this cw scheme, because Bob can check it if the detection events are uniformly distributed in time, and he notices something wrong when the detection events are concentrated on particular time windows by eavesdropping using pulsed light.

TABLE I. Number of data relative to the total number for each case.

		Bob's detection (%)	
		DET1	DET2
Alice's modulation	(0, 0)	1.4	20.7
	$(0,\pi)$	26.3	1.0
	$(\pi,0)$	27.2	0.7
	(π,π)	0.9	21.8

After confirming the interference for a fixed pattern, a random pattern was sent from Alice to Bob. Then after selecting data within time windows, Alice's modulation pattern and Bob's detection event were compared. The time window for the data selection was 2 ns out of 10-ns bit period, meaning that one fifth of the detected photons were utilized for creating a sifted key. The result is summarized in Table I, in which the number of data relative to the total number is listed for each case. A correlation between the modulation pattern and the detection event was demonstrated, such that detector 1 clicked for modulation patterns of (0, π) or (π, 0) and detector 2 clicked for (0, 0) or (π, π). The error rate was 4% on average. An error rate of 1–2 % resulted from the imperfection in the interference, and the other was caused by the imperfection in the phase-modulation and some errors in data acquisition. The sifted data were then processed to a final key string through error correction and privacy amplification assuming the eavesdropping that introduces an error rate of 1/4 (i.e., the second intercept-resend attack described above). The compression ratio from the sifted data to the final key was 58%. In this experiment, the photon-counting rate was 80000 counts/s, the sifted data rate was 16 000 bit/s, and the creation rate of the final key was 9280 bit/s. Taking the receiver loss into account, photon arrival rate at the receiver was 800×10^3 counts/s, which corresponds to a situation that signal with 0.1 photon per one-bit period (i.e., 10×10^6 counts/s) is sent from Alice and reaches Bob after 11 dB transmission loss.

In summary, differential-phase-shift QKD using coherent light was proposed and experimentally demonstrated. Alice sends weak coherent states that are phase-modulated for each pulse, and Bob measures the signal by a one-bit delay circuit. The system has a simple configuration favored for practical implementation and can offer a higher key creation efficiency.

[1] C.H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.
[2] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[4] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[6] B. Huttner, A. Muller, J.D. Gautier, H. Zbinden, and N. Gisin, Phys. Rev. A **54**, 3783 (1996).
[7] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[8] A. Himeno, K. Kato, and T. Miya, IEEE J. Sel. Top. Quantum Electron. **4**, 913 (1998).
[9] Y. Inoue, H. Takahashi, S. Ando, T. Sawada, A. Himeno, and M. Kawachi, J. Lightwave Technol. **15**, 1947 (1997).
[10] G. Bobfrate, M. Harlow, C. Ford, G. Maxwekk, and P.D. Townsend, Electron. Lett. **37**, 846 (2001).