Differential Phase Shift Quantum Key Distribution

Kyo Inoue*
NTT Basic Research Laboratories, NTT Corporation, Atsugi-shi, 243-0198 Japan
and E. L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4085

Edo Waks and Yoshihisa Yamamoto†
E. L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4085
(Received 30 October 2001; revised manuscript received 25 March 2002; published 27 June 2002)

A novel quantum cryptography scheme is proposed, in which a single photon is prepared in a linear superposition state of three basis kets. A photon split to three pulses is sent from Alice to Bob, where the phase difference between sequential two pulses carries bit information. Bob measures the phase difference by passive differential phase detection. This scheme is suitable for fiber transmission systems and offers a key creation efficiency higher than conventional fiber-based BB84.

DOI: 10.1103/PhysRevLett.89.037902 PACS numbers: 03.67.Dd, 42.50.Dv

Quantum key distribution (QKD) allows two parties (Alice and Bob) to share an unconditionally secure secret key. Security is guaranteed by the laws of quantum mechanics, ensuring that the key shared by Alice and Bob can be safely used as a one-time pad. Typical schemes for QKD are the following: use of two nonorthogonal bases (BB84) [1], use of two nonorthogonal states (B92) [2], and use of entangled photons (E91, BBM92) [3,4]. This paper proposes a novel QKD scheme, which utilizes fully nonorthogonal four states. A photon split into three pulses is sent from Alice to Bob, in which the phases of two sequential probability amplitudes are randomly modulated. Bob extracts the bit information by measuring the differential phase. This scheme is suitable for fiber transmission systems, while offering a key creation efficiency higher than conventional fiber-based BB84.

Figure 1 shows the setup of the proposed QKD system. In Alice's site, a photon from a single-photon source [5–14] is divided into three paths (a, b, and c) and recombined by beam splitters (BS) or optical switches (SW). The time delays between paths a and b and between paths b and c are equally T. The splitting ratios of the beam splitters are such that the probabilities for a photon to pass through each route are equal. The recombined photon is randomly phase modulated for each pulse by 0 or π [15]. Bob divides the incoming photon into two paths and recombines them by 50:50 beam splitters. The path lengths are such that the time delay is equal to the pulse interval T. The recombining beam splitter has two output ports, at which photon detectors (DET1, DET2) are placed, respectively.

In the above setup, Bob counts a photon possibly at four time instances as illustrated in Fig. 1. (i) A photon passes through path a in Alice and the short path in Bob. (ii) A photon passes through path a in Alice and the long path in Bob, and through path b in Alice and the short path in Bob. (iii) A photon passes through path b in Alice and the long path in Bob, and through path c in Alice and the short path in Bob. (iv) A photon passes through path c in Alice and the long path in Bob. Two probability amplitudes interfere with each other at time instances (ii) and (iii), for which the detectors click according to the phase difference between these two probability amplitudes. The phase difference is 0 or $\pm\pi$ depending on Alice's modulation, provided that the phase delay in each path is appropriately adjusted. DET1 clicks for 0 phase difference and DET2 clicks for $\pm\pi$ phase difference.

Using the above setup, a secret key is created as follows. (1) When Bob's detectors click at the second or third time instances, he records the time and which detector clicks. (2) Bob tells Alice the time instance of the photon detection. (3) From this information and her modulation data, Alice knows which detector clicked in Bob's site. (4) Alice and Bob have an identical bit string, provided that the DET1 click represents "0" and the DET2 click represents "1." In the above protocol, Bob only tells the time-instance to Alice, and the bit information is not leaked to the public.

The security of this scheme is discussed next. A full analysis of the QKD security is complicated [17–22] and beyond the scope of the present paper. We consider some simple eavesdropping strategies. A simple beam splitting attack fails when an ideal single-photon source is used, while some information is leaked for a nonideal source or when weak coherent light is used for practical implementation. The security for coherent light has been discussed

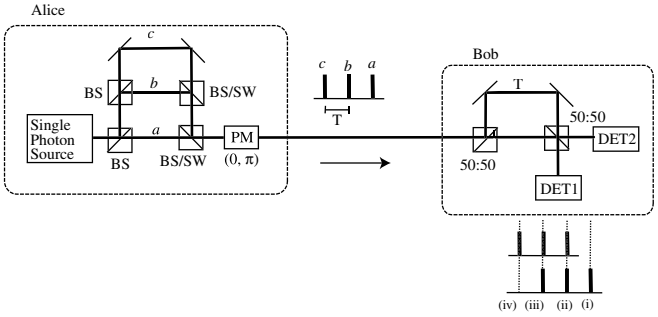

FIG. 1. Setup of the proposed QKD scheme. BS: beam splitter; SW: switch; PM: phase modulator; DET: photon detector.

[17,21], and we will not describe it in detail. One thing noted here is that an eavesdropper (Eve) cannot obtain bit information perfectly from a photon taken by beam splitting. In the beam splitting attack, Eve taps one photon out of multiple photons in a coherent pulse, and then obtains bit information by measuring the photon after Alice and Bob exchange supplementary information through a public channel. In conventional BB84, Eve can measure bit information perfectly from a tapped photon. In the present scheme, on the other hand, Eve cannot do so (as far as authors' consideration) because she cannot measure one of the two phase differences with 100% probability. Thus, the present scheme may be more robust against the beam splitting attack for weak coherent light.

A simple eavesdropping strategy next to the beam splitting attack is an intercept/resend attack using the same receiver setup as Bob. In trying this attack, Eve detects a photon at four possible time instances as Bob does. She obtains partial information when a photon is counted at (ii) or (iii), while she gets no information when it is counted at (i) or (iv). Several resending strategies are possible based on these measurement results.

From the measurement at (ii) or (iii), Eve knows one of the two phase-differences. If Eve sends a photon split into two pulses having the measured phase difference, she changes the counting rate at each time-instance in Bob. When Eve measures the phase difference between the first two pulses and resends a fake photon accordingly, Bob counts the photon at time-instances (i), (ii), or (iii). The probability ratio of the click at (i), (ii), and (iii) is 1:2:1. When Eve measures the phase difference between the second two pulses, Bob's detectors can click at time-instances (ii), (iii), and (iv) with a probability ratio of 1:2:1. Thus, the overall ratio of the clicks at (i), (ii), (iii), and (iv) becomes 1:3:3:1. On the other hand, the counting ratio for a photon split into three pulses is 1:2:2:1. Therefore, this cheating is revealed by monitoring the counting rate at each time-instance.

In order to keep the counting rate unchanged, Eve has to send a photon split into three pulses. There are two possibilities here. One is that Eve resends a photon every time she intercepts the signal, to keep the bit rate unchanged. When she counts a photon at (i) or (iv), she sends a photon full randomly, which introduces a bit error with a 0.5-probability in Bob. When she counts a photon at (ii) or (iii), she sends a photon for which one of the two phase-differences has the measured value and the other is random, which can introduce a bit error in case that Bob measures the random phase difference. The probability of this error occurring is $1/4$. The former measurement takes place with a $1/3$ probability and the latter measurement does with a $2/3$ probability, thus an overall error rate of $1/3 \times 1/2 + 2/3 \times 1/4 = 1/3$ is introduced by this signal resending. It is also possible for Eve to send a photon only when she counts a photon at (ii) and (iii), in order to make the error rate small. The error rate introduced by this resending is $1/4$, but the bit rate is reduced as a penalty, and Bob has a chance to find the cheating from the bit-rate reduction as well as bit errors. If Eve has a means of lossless signal transmission, she can use the second resending without changing the bit rate by manipulating the transmission loss to compensate the bit rate reduction. Both intercept/resend attacks cause bit error, and the eavesdropping is revealed by checking some test bits between Alice and Bob.

Theoretically speaking, a photon sent from Alice to Bob is one of the following four states:

$$|\phi\rangle = (1/\sqrt{3})\{|1\rangle_a|0\rangle_b|0\rangle_c \pm |0\rangle_a|1\rangle_b|0\rangle_c \pm |0\rangle_a|0\rangle_b|1\rangle_c\}, \quad (1)$$

where subscripts a, b, and c represent the states passing through paths a, b, and c, respectively. This three-dimensional Hilbert space is expanded by the three orthogonal basis states $|1\rangle_a|0\rangle_b|0\rangle_c$, $|0\rangle_a|1\rangle_b|0\rangle_c$, and $|0\rangle_a|0\rangle_b|1\rangle_c$. These four states are nonorthogonal with each other, and the security of this scheme is guaranteed by the fact that such states cannot be identified by a single measurement.

Bit information is carried by the phase difference between two sequential pulses in this scheme. They experience the same phase change and the same polarization change during propagation through the fiber transmission line. The differential phase and the relative polarization state between adjacent time slots are preserved irrespective of fiber fluctuations, which is favored for fiber transmission systems. Practical issues are the polarization-dependence of optical components in Bob's setup and the phase stability of the interferometers. Fortunately, Bob's interferometer consists of all passive elements, and Alice's interferometer does so if she uses beam splitters for recombining pulses. Such passive interferometers can be fabricated in one glass chip by the silica-based waveguide technology [23], which has been developed for fiber communication systems. Stable polarization-insensitive devices have been realized by that technology [24], indicating that the technology is available for stable, polarization-insensitive operation. Another practical issue is retiming. The effective fiber length can drift due to long-term temperature change, which changes the photon arriving time. This can be dealt with by, for example, sending timing pulses via wavelength division multiplexing.

A feature of the present scheme is its higher efficiency than conventional one. There have been several QKD protocols that do not use the polarization state and thus are preferable for fiber transmission systems. A typical one is phase-encoding BB84 [25–27], where Alice splits a photon into two time slots and sends it to Bob. The phase difference between these two slots is modulated by two nonorthogonal basis $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$. Bob measures the phase difference either in the $\{0, \pi\}$ basis or the $\{\pi/2, 3\pi/2\}$ basis, using an interferometer with a phase modulator or two interferometers. Then, Alice and Bob create a secret key from basis-matched bits. In this setup, there are cases that no interference occurs and Bob cannot

measure the phase difference, similar to the detector click at (i) or (iv) in our scheme illustrated in Fig. 1. The probability that the interference occurs is $1/2$, and the probability that the basis is matched between Alice and Bob is $1/2$. Thus, the overall probability of creating a key bit is $1/4$. In our scheme, on the other hand, photons counted at time-instances (ii) and (iii) fully contribute to the key. The probability for these events is $2/3$. Thus, the key creation efficiency is $8/3$ times higher than the conventional phase-encoding BB84. When passive beam splitters are used in Alice's site, the efficiency of sending a photon is $1/3$ in our system, while it is $1/2$ in the phase-encoding BB84. The photon sending efficiency is smaller in the present scheme, but the overall efficiency is still higher than in the previous scheme. When weak coherent light is used instead of single photons, the recombining loss does not matter.

There is a unique phase-encoding BB84 system, in which two sequential pulses are sent from Bob to Alice and sent back to Bob [28]. It is constructed for the two pulses to necessarily interfere with each other, thus the loss due to noninterfering events is eliminated, resulting in a key creation efficiency of $1/2$. The system is skillfully designed for stable operation. However, a disadvantage is that the pulse repetition rate cannot be high because of the Rayleigh scattering, and the bit rate is relatively low as a result. In addition, the system is not fitted to a single-photon source, which is not available at the present but has a potentiality for ideal QKD systems in the future [5–14].

In practice, information capacity after error correction and privacy amplification is important. The explicit number is dependent on various factors, e.g., transmission loss, dark count of photon detectors, performance of interferometers, assumed eavesdropping strategy, the average photon number in case of weak coherent light, etc. Intrinsic system parameters that determine the capacity are the efficiency from raw data to sifted data and the error rate introduced by eavesdropping. As described above, the efficiency to obtain sifted data in the present scheme is $8/3$ times that in the conventional phase-encoding BB84 system, while the error rate introduced by the simple intercept/resend attack is $1/4$, which is the same as BB84. Thus, the final information capacity may be $8/3$ times larger than the conventional phase-encoding BB84, provided that other parameters are the same.

The efficiency in the proposed scheme can be higher by increasing the number of paths in Alice's interferometer. Alice splits a photon into N (≥ 3) sequential pulses with an equal probability and an equal interval by such an interferometer, and modulates the phase of each pulse by $\{0, \pi\}$. Bob reads out the phase difference between neighboring two pulses by the same setup as shown in Fig. 1. Following the procedure for the three-pulse system, Alice and Bob can create a secret key also in this multipulse configuration. The key creation efficiency is $(1 - 1/N)$, thus it increases for a larger N at the expense of complexity.

In summary, a novel scheme of quantum cryptography was proposed. A photon split into three sequential pulses is sent from Alice to Bob, in which each pulse is randomly phase modulated by 0 and π. A secret key is created from measuring the differential phase by an interferometer. The scheme is suitable for fiber transmission systems and offers a key creation efficiency higher than conventional fiber-based BB84.

*Electronic address: kyo@will.brl.ntt.co.jp
†Also at NTT Basic Research Laboratories.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[2] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[5] F. De Martini, G. Di Giuseppe, and M. Marrocco, Phys. Rev. Lett. **76**, 900 (1996).
[6] C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, Phys. Rev. Lett. **83**, 2722 (1999).
[7] B. Lounis and W. E. Moerner, Nature (London) **407**, 491 (2000).
[8] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, Nature (London) **397**, 500 (1999).
[9] R. Brouri, A. Beveratos, J. Poizat, and P. Grangier, Opt. Lett. **25**, 1294 (2000).
[10] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, Phys. Rev. Lett. **85**, 290 (2000).
[11] P. Michler *et al.,* Science **290**, 2282 (2000).
[12] V. Zwiller *et al.,* Appl. Phys. Lett. **78**, 2476 (2001).
[13] C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, Phys. Rev. Lett. **86**, 1502 (2001).
[14] Z. Yuan *et al.,* Science **295**, 102 (2002).
[15] The authors came up with this modulation setup after the first submission, while a setup in the first manuscript is cited in Ref. [16] as our proposal.
[16] W. T. Buttler, J. R. Torgerson, and S. K. Lamoreaux, quant-ph/020398.
[17] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[18] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. Nui, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[19] B. A. Slutsky, R. Rao, P. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).
[20] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
[21] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[22] E. Waks, A. Zeevi, and Y. Yamamoto, quant-ph/0012078.
[23] A. Himeno, K. Kato, and T. Miya, IEEE J. Sel. Top. Quantum Electron. **4**, 913 (1998).
[24] Y. Inoue, H. Takahashi, S. Ando, T. Sawada, A. Himeno, and M. Kawachi, J. Lightwave Technol. **15**, 1947 (1997).
[25] J. G. Rarity, P. C. M. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).
[26] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).
[27] R. J. Hughes, G. L. Morgan, and C. G. Peterson, J. Mod. Opt. **47**, 533 (2000).
[28] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett. **34**, 2116 (1998).