Decoy State Quantum Key Distribution

Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen

Center for Quantum Information and Quantum Control, Department of Electrical & Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada

(Received 31 October 2004; published 16 June 2005)

There has been much interest in quantum key distribution. Experimentally, quantum key distribution over 150 km of commercial Telecom fibers has been successfully performed. The crucial issue in quantum key distribution is its security. Unfortunately, all recent experiments are, in principle, insecure due to real-life imperfections. Here, we propose a method that can for the first time make most of those experiments secure by using essentially the same hardware. Our method is to use decoy states to detect eavesdropping attacks. As a consequence, we have the best of both worlds—enjoying unconditional security guaranteed by the fundamental laws of physics and yet dramatically surpassing even some of the best experimental performances reported in the literature.

DOI: 10.1103/PhysRevLett.94.230504 PACS numbers: 03.67.Dd, 03.67.Hk

Quantum key distribution (QKD) allows two users, Alice and Bob, to communicate in absolute security in the presence of an eavesdropper, Eve. Unlike conventional cryptography, the security of QKD is based on the fundamental laws of physics, rather than unproven computational assumptions. The security of QKD has been rigorously proven in a number of recent papers [1]. See also [2]. There has been tremendous interest in experimental QKD [3,4], with the current world record distance of 150 km of Telecom fibers [4].

Unfortunately, all those exciting recent experiments are, in principle, insecure due to real-life imperfections. More concretely, highly attenuated lasers are often used as sources. But, these sources sometimes produce signals that contain more than one photon. Those multiphoton signals open the door to powerful new eavesdropping attacks including a photon number splitting attack. For example, Eve can, in principle, measure the photon number of each signal emitted by Alice and selectively suppress single-photon signals. She splits multiphoton signals, keeping one copy for herself and sending one copy to Bob. Now, since Eve has an identical copy of what Bob possesses, the unconditional security of QKD [in, for example, standard Bennett-Brassard 1984 (BB84) protocol [5]] is completely compromised.

In summary, in standard BB84 protocol, only signals originated from *single* photon pulses emitted by Alice are guaranteed to be secure. Consequently, paraphrasing Gottesman-Lo-Lütkenhaus-Preskill (GLLP) [6], the secure key generation rate (per signal state emitted by Alice) can be shown to be given by:

$$S \geq Q_\mu\{-H_2(E_\mu) + \Omega[1 - H_2(e_1)]\}, \qquad (1)$$

where Q_μ and E_μ are, respectively, the gain and quantum bit error rate (QBER) of the signal state [7], Ω and e_1 are, respectively, the fraction and QBER of detection events by Bob that have originated from single-photon signals emitted by Alice, and H_2 is the binary Shannon entropy.

It is *a priori* very hard to obtain a good lower bound on Ω and a good upper bound on e_1. Therefore, prior art methods (as in GLLP [6]) make the most pessimistic assumption that all multiphoton signals emitted by Alice will be received by Bob. For this reason, until now, it has been widely believed that the demand for unconditional security will severely reduce the performance of QKD systems [6,8–11].

In this Letter, we present a simple method that will provide very good bounds to Ω and e_1. Consequently, our method for the first time makes most of the long distance QKD experiments reported in the literature unconditionally secure. Our method has the advantage that it can be implemented with essentially the current hardware. So, unlike prior art solutions based on single-photon sources, our method does not require daunting experimental developments. Our method is based on the decoy state idea first proposed by Hwang [12]. While the idea of Hwang was highly innovative, his security analysis was heuristic. The key point of the decoy state idea is that Alice prepares a set of additional states—decoy states, in addition to standard BB84 states. Those decoy states are used for the purpose of detecting eavesdropping attacks only, whereas the standard BB84 states are used for key generation only. The only difference between the decoy state and the standard BB84 states is their intensities (i.e., their photon number distributions).

By measuring the yields and QBER of decoy states, we will show that Alice and Bob can obtain reliable bounds to Ω and e_1, thus allowing them to surpass all prior art results substantially [13]. Here, we give for the first time a rigorous analysis of the security of decoy state QKD. Moreover, we show that the decoy state idea can be combined with the prior art GLLP [6] analysis.

Preliminary versions of our result in this Letter appeared in public in June to September 2004 in [14,15], where we presented not only the general theory, but also proposed the idea of using only a few decoy states (for example, three

states—the vacuum, a weak decoy state with $\mu_{\text{decoy}} \ll 1$, and a signal state with $\mu = O(1)$. We call this a Vacuum + Weak decoy state protocol). Subsequently, our protocols for decoy state QKD have been analyzed in [16] and more systematically in [17]. See also [18]. Recently, we have provided the first experimental demonstration of decoy state QKD in [19].

We now present the general theory of our new decoy state schemes. We will assume that Alice can prepare phase-randomized coherent states and can turn her power up and down for each signal. This may be achieved by using standard commercial variable optical attenuators (VOAs) [20]. Let $|\sqrt{\mu}e^{i\theta}\rangle$ denote a weak coherent state emitted by Alice. Assuming that the phase, θ, of all signals is totally randomized, the probability distribution for the number of photons of the signal state follows a Poisson distribution with some parameter μ. That is to say that, with a probability $p_n = e^{-\mu}\mu^n/n!$, Alice's signal will have n photons. In summary, we have assumed that Alice can prepare any Poissonian (with parameter μ) mixture of photon number states and, moreover, Alice can vary the parameter, μ, for each individual signal.

Let us consider the gain Q_μ for a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$. (Here and thereafter, we actually mean the random mixture of $|\sqrt{\mu}e^{i\theta}\rangle$ over all values of θ as the phase is assumed to be totally randomized.) We have:

$$Q_\mu = Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + Y_2 e^{-\mu}(\mu^2/2) + \cdots + Y_n e^{-\mu}(\mu^n/n!) + \cdots, \tag{2}$$

where Y_n is the yield of an n-photon signal [21] and where $Y_0 \geq 0$ gives the detection events due to background including dark counts and stray light from timing pulses.

Similarly, the QBER can depend on the photon number. Let us define e_n as the QBER of an n-photon signal. The QBER E_μ for a coherent state $|\sqrt{\mu}e^{i\theta}\rangle$ is given by

$$Q_\mu E_\mu = Y_0 e^{-\mu} e_0 + Y_1 e^{-\mu}\mu e_1 + Y_2 e^{-\mu}(\mu^2/2)e_2 + \cdots + Y_n e^{-\mu}(\mu^n/n!)e_n + \cdots, \tag{3}$$

which is the weighted average of the QBERs of various photon number eigenstates.

Essence of the decoy state idea.—Let us imagine that a decoy state and a signal state have the same characteristics (wavelength, timing information, etc.). Therefore, Eve cannot distinguish a decoy state from a signal state and the only piece of information available to Eve is the number of photons in a signal. Therefore, the yield, Y_n, and QBER, e_n, can depend on only the photon number, n, but not which distribution (decoy or signal) the state is from. We emphasize that the essence of the decoy state idea can be summarized by the following two equations:

$$Y_n(\text{signal}) = Y_n(\text{decoy}) = Y_n \tag{4}$$

$$e_n(\text{signal}) = e_n(\text{decoy}) = e_n. \tag{5}$$

While a few decoy states are sufficient, for ease of discussion, we will for the moment consider the case where Alice will pick an infinite number of possible intensities for decoy states. Let us imagine that Alice varies over all nonnegative values of μ randomly and independently for each signal. Alice and Bob can experimentally measure the yield Q_μ and the QBER E_μ. Since the relations between the variables Q_μ's and Y_n's and between E_μ's and e_n's are linear, given the set of variables Q_μ's and E_μ's measured from their experiments, Alice and Bob can deduce mathematically with high confidence the variables Y_n's and e_n's. This means that Alice and Bob can constrain simultaneously the yields, Y_n, and QBER, e_n, simultaneously for *all* n. Suppose Alice and Bob know their channel property well. Then, they know what range of values of Y_n's and e_n's is acceptable. Any attack by Eve that will change the value of any one of the Y_n's and e_n's substantially will, in principle, be caught with high probability by our decoy state method. Therefore, in order to avoid being detected, the eavesdropper, Eve, has very limited options in her eavesdropping attack. In summary, the ability for Alice and Bob to verify experimentally the values of Y_n and e_n's in the decoy state method greatly strengthens their power in detecting eavesdropping, thus leading to a dramatic improvement in the performance of their QKD system.

The decoy state method allows Alice and Bob to detect deviations from the normal behavior due to eavesdropping attacks. Therefore, in what follows, we will consider normal behavior (i.e., the case of no eavesdropping). Details of QKD setup model can be seen in [17].

Yield.—Let us discuss the yields, Y_n's, in a realistic setup. (a) The case $n = 0$. In the absence of eavesdropping, Y_0 is simply given by the background detection event rate p_{dark} of the system. (b) The case $n \geq 1$. For $n \geq 1$, yield Y_n comes from two sources: (i) the detection of signal photons η_n and (ii) the background event p_{dark}. The combination gives, assuming the independence of background and signal detection events,

$$Y_n = \eta_n + p_{\text{dark}} - \eta_n p_{\text{dark}} \approx \eta_n + p_{\text{dark}}, \tag{6}$$

where in the second line we neglect the cross term because the background rate (typically 10^{-5}) and transmission efficiency (typically 10^{-3}) are both very small.

Suppose the overall transmission probability of each photon is η. In a normal channel, it is common to assume independence between the behaviors of the *n photons*. Therefore, the transmission efficiency for n-photon signals η_n is given by:

$$\eta_n = 1 - (1 - \eta)^n. \tag{7}$$

(For a small η and ignore the dark count, $Y_n \approx n\eta$.)

QBER.—Let us discuss the QBERs, e_n's, in a realistic experiment. (a) If the signal is a vacuum, Bob's detection is due to background including dark counts and stray light due to timing pulses. Assuming that the two detectors have equal background event rates, then the output is totally

random and the error rate is 50%. That is, the QBER for the vacuum $e_0 = 1/2$. (b) If the signal has $n \geq 1$ photons, it also has some error rate, say e_n.

More concretely, e_n comes from two parts, erroneous detections and background contribution,

$$e_n = \left(e_{\text{detector}}\eta_n + \frac{1}{2}p_{\text{dark}}\right)/Y_n, \tag{8}$$

where e_{detector} is independent of n.

The values of Y_n and e_n can be experimentally verified by Alice and Bob using our decoy state method. Any attempt by Eve to change them significantly will almost always be caught.

Combining decoy state idea with GLLP.—Suppose key generation is done on signal state $|\sqrt{\mu}e^{i\theta}\rangle$. In principle, Alice and Bob can isolate the single-photon signals and apply privacy amplification to them only. Therefore, generalizing the work in GLLP, we find Eq. (1) where the gain of the signal state, $Q_\mu = \Sigma_{k=0}^{\infty} Y_k e^{-\mu}(\mu^k/k!)$ [this comes directly from Eq. (2)], and the fraction of Bob's detection events that have originated from single-photon signals emitted by Alice is given by:

$$\Omega = \frac{Q_1}{Q_\mu}, \tag{9}$$

where

$$Q_1 = Y_1 \mu e^{-\mu} \tag{10}$$

is the gain for the single-photon state.

The derivation of Eq. (1) assumes that error correction protocols can achieve the fundamental (Shannon) limit. However, practical error correction protocols are generally inefficient. As noted in [22], a simple way to take this inefficiency into account is to introduce a function, $f(e) > 1$, of the QBER, e. By doing so, we find that the key generation rate for practical protocols is given by:

$$S \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \tag{11}$$

where q depends on the implementation (1/2 for the BB84 protocol, because half the time Alice and Bob bases are not compatible, and if we use the efficient BB84 protocol [23], we can have $q \approx 1$. For simplicity, we will take $q = 1$ in this Letter), and $f(e)$ is the error correction efficiency [22].

Let us now compare our result in Eq. (11) with the prior art GLLP result. In the prior art GLLP [6] method, secure key generation rate is shown to be at least

$$S \geq Q_\mu\left\{-H_2(E_\mu) + \Omega\left[1 - H_2\left(\frac{E_\mu}{\Omega}\right)\right]\right\}, \tag{12}$$

where Ω, the fraction of "untagged" photons (which is a pessimistic estimation of the fraction of detection events by Bob that have originated from single-photon signals emitted by Alice), is given by

$$1 - \Omega = p_{\text{multi}}/Q_\mu, \tag{13}$$

where p_{multi} is the probability of Alice's emitting a multiphoton signal. Equation (13) represents the worst situation where all the multiphotons emitted by Alice will be received by Bob.

Comparing our result [given in Eq. (11)] with the prior art GLLP result [given in Eq. (12)], we see that the main difference is that in our result, a much better lower bound on Ω and a much better upper bound on e_1 can be obtained.

Implication of our result.—We obtain a substantially higher key generation rate than in [6]. In more detail, note that, from Eq. (6), Y_n for $n > 2$ is of similar order to Y_1. Therefore, from Eq. (11) it is now advantageous for Alice to pick the average photon number in her signal state to be $\mu = O(1)$. Therefore, the key generation rate in our new method is $O(\eta)$ where η is the overall transmission probability of the channel. In comparison, in prior art methods for secure QKD, μ is chosen to be of order $O(\eta)$, thus giving a net key generation rate of $O(\eta^2)$. In summary, we have achieved a substantial increase in net key generation rate from $O(\eta^2)$ to $O(\eta)$. Moreover, as will be discussed below, our decoy state method allows secure QKD at much longer distances than previously thought possible.

More concretely, we [15] have applied our results to various experiments in the literature. The results are shown in Fig. 1 using the Gobby-Yuan-Shields (GYS) [3] experiment as an example. We found that the optimal averaged number μ in GYS that maximizes the key generation rate in our decoy state method in Eq. (11) is, indeed, of $O(1)$

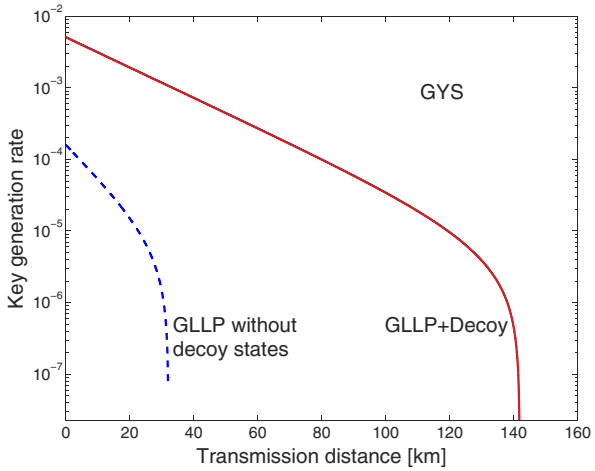

FIG. 1 (color online). This figure is obtained by writing a simple program. The line of GLLP without decoy state uses the formula (12) and GLLP + Decoy uses the formula (11) according to the parameters given in experiment GYS [3]. With decoy states, the maximal distance increases to over 140 km. For comparison, we found that with prior art method, the secure distance is only about 30 km. We have also proven that an upper bound of distance of secure BB84 with the GYS parameters is 208 km because this corresponds to the point where $e_1 = 1/4$ and the protocol is insecure due to an intercept-resend attack. We have checked that our results are stable to small perturbations to the background event rate p_{dark} and average photon number μ (both up to 20% change).

(roughly 0.5). Therefore, the key generation rate is of order $O(\eta)$. We remark that the calculated optimal value of photon number of 0.5 is, in fact, *higher* than what experimentalists have been using. Experimentalists often liberally pick 0.1 as a convenient number for average photon number without any security justification. In other words, operating their equipment with the parameters proposed in the present Letter will allow experimentalists to not only match, but also *surpass* their current experimental performance (by having at least fivefold the current experimental key generation rate). This demonstrates clearly the power of decoy state QKD. Moreover, Fig. 1 shows that with our decoy state idea, secure QKD can be done at distances over 140 km with only current technology.

In summary, our result shows that we can have the best of both worlds: enjoy both unconditional security and record-breaking experimental performance. The general principle of decoy state QKD developed here can have widespread applications in other setups (e.g., open-air QKD or QKD with other photon sources) and to multiparty quantum cryptographic protocols such as [24]. As demonstrated clearly in [17], one can achieve almost all the benefits of our decoy state method with only one or two decoy states. See also [16]. Recently, we have experimentally demonstrated decoy state QKD in [19].

We have benefited greatly from enlightening discussions with many colleagues including particularly G. Brassard. Financial support from funding agencies such as CFI, CIPI, CRC program, NSERC, OIT, and PREA are gratefully acknowledged. H.-K. L. also thanks travel support from the INI, Cambridge, UK, and from the IQI at Caltech through NSF Grant No. EIA-0086038.

[1] D. Mayers, Journal of the Association for Computing Machinery **48**, 351 (2001); preliminary version: D. Mayers, *Advances in Cryptology-Proc. Crypto '96*, edited by N. Koblitz, Lect. Notes. Comput. Sci. Vol. 1109 (Springer-Verlag, Berlin, 1996), pp. 343–357; H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999); E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC '00)* (ACM Press, New York, 2000), pp. 715–724; M. Ben-Or, Presentation at MSRI, available online at http://www.msri.org/publications/ln/msri/2002/qip/ben-or/1/; P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[2] A. K. Ekert and B. Huttner, J. Mod. Opt. **41**, 2455 (1994); D. Deutsch *et al.*, Phys. Rev. Lett. **77**, 2818 (1996); **80**, 2022(E) (1998).

[3] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

[4] T. Kimura *et al.*, Jpn. J. Appl. Phys. **43**, L1217 (2004).

[5] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[6] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[7] Here, the gain means the ratio of the number of Bob's detection events (where Bob chooses the same basis as Alice) to Alice's number of emitted signals. QBER means the error rate of Bob's detection events for the case that Alice and Bob use the same basis.

[8] H. Inamori, N. Lütkenhaus, and D. Mayers, quant-ph/0107017.

[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[10] Prior art methods to extend the unconditionally secure distance of QKD usually require either single-photon sources, low-loss fibers, or new types of single-photon detectors. Unfortunately, those prior art solutions require daunting experimental developments.

[11] Incidentally, Koashi [M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004)] has recently proposed an alternative method to extend the distance of secure QKD. However, our method and results differ substantially from those of Koashi.

[12] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[13] By using decoy states, we are considering a theoretical extension of BB84, rather than standard BB84. It will be interesting to apply the work of M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004) to this new setting.

[14] H.-K. Lo, in *Proceedings of 2004 IEEE ISIT* (IEEE Press, New York, 2004), p. 137, and presentation at the Fields Institute Conference on QIQC, http://www.fields.utoronto.ca/programs/scientific/04-05/quantumIC/abstracts/lo.ppt July, 2004.

[15] X. Ma, "*Security of Quantum Key Distribution with Realistic Devices*," University of Toronto, Master Report, quant-ph/0503057.

[16] X.-B. Wang, this issue, Phys. Rev. Lett. **94**, 230503 (2005).

[17] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, quant-ph/0503005 [Phys. Rev. A (to be published)].

[18] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, quant-ph/0503002.

[19] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, quant-ph/0503192.

[20] Variable optical attenuators (VOAs) at repetition rates as high as 100 GHz are commercially widely available. Those attenuators can be directly applied to fiber-optics based QKD systems.

[21] Y_n is the conditional probability that Bob detects a signal, given that an n-photon signal is emitted by Alice.

[22] G. Brassard and L. Salvail, *Advances in Cryptology, Eurocrypt '93* (Springer-Verlag, Berlin, 1993), pp. 410–423.

[23] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, No. 2, 133 (2005).

[24] K. Chen and H.-K. Lo, quant-ph/0404133.