Security aspects of quantum key distribution with sub-Poisson light

Edo Waks, Charles Santori, and Yoshihisa Yamamoto*

Quantum Entanglement Project, ICORP, JST, E. L. Ginzton Laboratories, Stanford University, Stanford, California 94305

(Received 1 April 2002; published 22 October 2002)

The security of quantum key distribution with sub-Poisson light sources is investigated. It is shown that a quantitative analysis of the security of such sources requires only two measured values, the efficiency and second-order correlation. These two numbers represent figures of merit, which characterize the performance of such light sources. We show that sub-Poisson light sources can offer significant improvements in communication rate over Poisson light in the presence of realistic experimental imperfections. We also investigate the amount of channel loss that can be tolerated for secure communication to be possible, and show that this only depends on the second-order correlation, provided the device efficiency exceeds a critical value. If this critical efficiency is exceeded, an inefficient source can perform as well as an efficient one at sufficiently high channel losses.

DOI: 10.1103/PhysRevA.66.042315 PACS number(s): 03.67.Dd, 42.50.Dv

I. INTRODUCTION

Quantum cryptography is a method by which two parties can potentially exchange an unconditionally secure secret message. The security of this message is ensured by the laws of quantum mechanics, which forbid any third-party eavesdropper from localizing the state of a quantum system simultaneously in two noncommuting observables. The first protocol for quantum cryptography was proposed by Bennett and Brassard in 1984 [1], and has since been known as BB84. A good review of the BB84 protocol and quantum cryptography in general can be found in Ref. [2].

In BB84, the sender of the message, Alice, encodes each bit of a secret key in a two-level quantum system (qubit). The qubit is sent to the receiver, Bob, over a quantum channel. The enemy, Eve, is allowed to tap the quantum channel and perform any measurement allowed by the laws of quantum mechanics. To prevent eavesdropping, Alice randomly prepares the qubit in one of two nonorthogonal bases. Eve does not know the preparation basis, which is needed in order to make a proper measurement. Without this information, Eve will make the wrong measurement some of the times and unavoidably distort the wave function of the qubit. Such distortions result in an increased error rate for Bob, revealing the presence of the eavesdropper.

For practical implementations of quantum cryptography, the information carrier of choice is almost exclusively the photon. The wave function of the photon is typically very robust to environmental noise, and a photon can be sent through a single-mode fiber for many kilometers without prohibitively large loss. Several versions of BB84 using fiber-optic technology have already been implemented [3–6]. Alternate implementations based on free space propagation show that a single photon can be reliably sent through open space over a 1 km distance in broad daylight [7]. These fiber and free space experiments demonstrate that quantum key distribution can be made into a practical technology.

One of the difficulties of implementing quantum key distribution is generating single photons. All of the above implementations use attenuated laser light to approximate single photons. In such cases the photon number follows a Poisson distribution. By making the average photon number much less than 1, the probability of generating two or more photons can be suppressed. This is done at the expense of having a large contribution of vacuum states, which reduces the communication rate. The problem with generating more than one photon is that such states are vulnerable to photon splitting attacks. The BB84 protocol assumes that Alice only prepares one qubit to be sent to Bob. If she accidentally prepares two, Eve can steal one of the qubits and relay the other one to Bob without being detected. Thus, multiphoton states pose a dangerous security loophole.

The effect of multiphoton states on the security of BB84 has already been studied [8,9]. The presence of such states can strongly degrade the security of the secret key. Worse yet, the impact of the multiphoton states becomes stronger with increasing channel loss. Thus, even if only a minute fraction of the signals contain more than one photon, they can create a significant security risk at high loss levels. At some critical loss level, they can even render the entire key completely insecure. For these reasons there has recently been an effort to create devices which better approximate a single-photon state.

One approach to reducing photon splitting attacks has been to engineer single-photon turnstile devices. Such sources would ideally generate exactly one photon on request. Already, there are several promising experimental implementations of devices generating single photons on demand [10–20]. Unfortunately, a perfect heralded single-photon device can never be made in practice. All real devices suffer from two important device imperfections. First, all devices have some degree of intrinsic loss, which creates an unavoidable vacuum contribution. Second, there is always some probability of inadvertently generating a multiphoton state due to factors such as scattered background light and substrate photoluminescence. Thus, it is dangerous to completely ignore photon splitting attacks even when using such devices for single-photon preparation.

*Also at NTT Basic Research Laboratories, Atsugi, Kanagawa, Japan.

It is commonly accepted that the use of nonideal single-photon devices, which we will refer to as sub-Poisson light sources, will enhance the performance of a cryptography system. However, to date there has been no real quantitative analysis of the security of such devices. Adding to the difficulty of a security analysis is the fact that, unlike Poisson light, we do not have complete information about the photon number distribution of sub-Poisson light sources. Such information can only be measured by a detector that can count photon number, and this is difficult to do. The sub-Poisson nature of the device is typically measured by a Hanbury-Brown and Twiss intensity interferometer. This measurement gives us the normalized second-order correlation $g^{(2)}$ [21].

In this paper we will show that $g^{(2)}$ and the average photon number per pulse $\overline{n}$ are sufficient to analyze the security of sub-Poisson light sources. These two numbers can be accurately measured in a lab, and serve as figures of merit for the expected security behavior of the device. We explicitly calculate the expected communication rate for BB84, and compare the performance of sub-Poisson sources to Poisson light in the presence of realistic channel losses and detector dark counts. It is known that multiphoton states and detector dark counts put an upper limit on the acceptable amount of channel losses [9]. Here we show that the amount of acceptable channel loss for sub-Poisson sources can be significantly greater than Poisson light. Furthermore, the maximum channel loss is only a function of $g^{(2)}$, provided the device efficiency exceeds a critical value. This is an important result, since device losses can be substantial in current implementations of sub-Poisson sources. As long as the efficiency exceeds this critical level (which is well within technological capabilities for typical cases), an inefficient device can tolerate the same amount of channel loss as a very efficient device.

To analyze the performance of sub-Poisson sources, we first calculate rigorous bounds on the communication rate after error correction and privacy amplification. These bounds, based on the assumption that Eve attacks each qubit independently, use the security proof of BB84 given in Ref. [8]. Such calculations give us security estimates against eavesdroppers with highly advanced technological capabilities. Unfortunately, the equations involved in calculating such rates are complicated. It is difficult to get analytical solutions for important quantities such as the maximum acceptable channel loss and critical efficiency, forcing us to resort to numerical methods. In the second part of the paper we use an approximate analysis to derive analytical estimates on such quantities. Such an analysis allows us to get closed-form solutions that give a better intuitive understanding of the issues and tradeoffs of sub-Poisson light sources. These estimates are compared to the exact numerical results, and shown to be accurate to within about a factor of 2.

II. RATE CALCULATIONS FOR SUB-POISSON LIGHT

The security of BB84 is a complex subject with a fairly long history. Adding to the difficulty of the problem is the fact that for practical systems, the basic BB84 protocol must be augmented by two additional steps, error correction and privacy amplification. These two steps use only public discussion. The purpose of error correction is to eliminate errors in the quantum transmission, which may occur from either eavesdropping or experimental imperfection. A good discussion of error correction can be found in Ref. [22]. Because all practical systems have a base line error rate, there is always some potential for information leakage to an eavesdropper. Privacy amplification is used to eliminate this leaked information by compressing the error corrected transmission into a shorter final key. Even if Eve has substantial information about the error corrected transmission, after privacy amplification she will know virtually nothing about this final key [23].

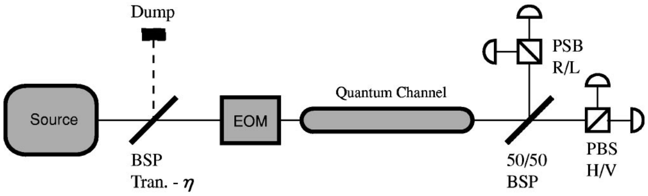

FIG. 1. Schematic of experimental configuration of quantum key distribution with BB84.

Several proofs of security currently exist for the BB84 protocol against the most general attacks allowed by quantum mechanics [24–26]. Unfortunately, these proofs do not apply to sources that sometimes produce more than one photon, so they cannot be used to analyze practical systems. A proof of security which can be applied to realistic sources has been derived [8], and was used to characterize the performance of BB84 with Poisson light. This proof requires an auxiliary restriction that Eve attacks each photon individually. We will use this proof to perform an analysis of BB84 with sub-Poisson light sources. It has come to our attention that a new proof has been proposed, which applies to realistic sources and does not require restriction to individual attacks [27]. Such a proof would represent the most complete security analysis of BB84 known to date. We believe that our analysis of sub-Poisson light can be extended to this more general proof of security.

Figure 1 shows the setup which we will consider. We assume that the photon source creates a train of light pulses at a fixed repetition rate. Each light pulse is assumed to be contained in an interval $[0,\Delta]$, which is smaller than the duty cycle of the experiment. Under these conditions we can define the photon number operator

$$\hat{n}=\int_0^\Delta \hat{a}^\dagger(t)\hat{a}(t)dt. \tag{1}$$

In the above equation $\hat{a}^\dagger(t)$ is the photon creation operator in the time domain. The average number of photons in a duty cycle is simply given by $\overline{n}=\langle\hat{n}\rangle$. We can also define the second-order correlation as

$$g^{(2)}=\frac{\int_0^\Delta\int_0^\Delta\langle\hat{a}^\dagger(t)\hat{a}^\dagger(t')\hat{a}(t')\hat{a}(t)\rangle dtdt'}{\overline{n}^2}. \tag{2}$$

It is not difficult to show, using the commutation relation

$$[\hat{a}(t),\hat{a}^{\dagger}(t')]=\delta(t-t'), \tag{3}$$

that the expression for $g^{(2)}$ can be rewritten in the form

$$g^{(2)}=\frac{\langle\hat{n}(\hat{n}-1)\rangle}{\overline{n}^2}. \tag{4}$$

The numbers $\overline{n}$ and $g^{(2)}$ will form the basis for the security analysis.

For completeness, we assume that the information is encoded in the polarization of the photon. Thus, an electro-optic modulator is used to set the polarization of the photon before injection into the quantum channel. Alternate implementations based on momentum and time can be treated in a completely analogous way. For these schemes the electro-optic modulator will typically be placed in an appropriate Mach-Zehnder interferometer configuration. We also allow for Alice to intentionally introduce an additional amount of loss η via a beam splitter, as shown in Fig. 1. It may at first seem counterintuitive to introduce additional loss, but we will show that, at times, this is necessary for secure communication. Bob's detection apparatus is composed of a 50-50 beam splitter which partitions the light into two polarizing beam splitters, one measuring in the horizontal/vertical (H/V) basis, the other in the right/left (R/L) circularly polarized basis. This technique is referred to as passive modulation, and obviates the need for an active polarization rotator at Bob's detection site.

In analyzing communication rates for BB84, an important security parameter is the disturbance measure ϵ, given by

$$\epsilon=\frac{p_{err}+p_d/2}{p_{click}}. \tag{5}$$

In the above equation, p_{err} and p_d are the probabilities that a pulse causes an error and a multiple detection event, respectively, and p_{click} is the probability that a pulse causes a single detection event. When the number of dual detection events is negligibly small, we have $\epsilon=e$, where e is the bit error rate of the transmission. In this limit the communication rate is given by [8]

$$R=\frac{p_{click}}{2}\{\beta\tau(e)-f(e)h(e)\}. \tag{6}$$

The parameter β is the fraction of detection events originating from single photons given by

$$\beta=\frac{p_{click}-p_m}{p_{click}}, \tag{7}$$

where p_m is the probability that the source generated more than one photon. The compression function $\tau(e)$ accounts for Eve's attacks on the raw quantum key, and is given by

$$\tau(e)=-\log_2\left[\frac{1}{2}+2\frac{e}{\beta}-2\left(\frac{e}{\beta}\right)^2\right]. \tag{8}$$

TABLE I. Values of $f(e)$ for different error rates.

e	$f(e)$
0.01	1.16
0.05	1.16
0.1	1.22
0.15	1.35

The function $h(e)$ is the Shannon entropy function of a single bit given by

$$h(e)=-e\log_2 e-(1-e)\log_2(1-e). \tag{9}$$

The function $f(e)$ characterizes the performance of the error correction algorithm. When $f(e)=1$, the algorithm is working at the Shannon limit. This limit defines the ultimate performance of an error correction algorithm and cannot be exceeded. Thus, $f(e)\geqslant 1$ in general (see Ref. [22] for discussion).

In order to analyze the security of BB84, we need values for p_{click}, e, and p_m, as well as the function $f(e)$. The value of $f(e)$ depends on which error correction algorithm is used. One such algorithm, which performs very close to the Shannon limit, can be found in Ref. [22]. Values of $f(e)$ for this algorithm at different error rates are given in Table I. The function is linearly interpolated for intermediate error values.

Bob's detection events can be separated into a signal component that originates from Alice's transmission, and a dark count component that originates from Bob's detectors. Thus we have

$$p_{click}=p_{signal}+d-p_{signal}d \tag{10}$$

$$\approx p_{signal}+d. \tag{11}$$

where d is the probability of a dark count. The above approximation is valid when p_{signal} and d are small, so that we may ignore a simultaneous signal and dark count event. In general, our calculations will assume that multiple detection events are negligibly small and can thus be neglected. This is a very good approximation for most quantum key distribution experiments.

The signal contribution to the detection events is given by

$$p_{signal}=\sum_{n=0}^{\infty}p(n)[1-(1-T)^n]. \tag{12}$$

The parameter T in the above equation is the total optical loss from the quantum channel and Bob's detection apparatus. In general, we cannot evaluate this expression because we do not know $p(n)$. But as mentioned before, we are considering the limit where dual fire events are negligible. In this limit we can keep the above expression only to first order in T. Using the approximation $(1-T)^n\approx(1-nT)$, we have

$$p_{signal}\approx\overline{n}T, \tag{13}$$

where $\bar{n}$ is the average number of photons injected by Alice into the quantum channel. The probability d is given by the dark count rate of the detectors multiplied by the measurement time window. Thus, $d = r_d \tau_w$.

The error rate e will receive a contribution from both the signal and dark count component. Errors from the signal component occur because of imperfect state preparation, channel decoherence, and imperfect polarization optics at Bob's detection unit. We define a baseline signal error rate μ, which contains all of these effects. For good systems, μ is typically less than 2%. A second error component comes from the dark counts at Bob's detection unit. Each dark count is completely uncorrelated with Alice's signal and thus causes a 50% error rate. Using the above definitions we have

$$e = \frac{\mu p_{signal} + d/2}{p_{click}}. \tag{14}$$

Finally, we must come up with a bound on p_m. For this we need $g^{(2)}$. From Eq. (4) we can write

$$g^{(2)} = \frac{\sum_{i=2}^{\infty} i(i-1)p(i)}{\overline{n^2}}. \tag{15}$$

Using the fact that $i(i-1) \geqslant 2$ for all $i \geqslant 2$, we have the bound

$$g^{(2)} \geqslant \frac{\sum_{i=2}^{\infty} 2p(i)}{\overline{n^2}}$$

$$= \frac{2p_m}{\overline{n^2}},$$

or alternately

$$p_m \leqslant \frac{\overline{n^2} g^{(2)}}{2}. \tag{16}$$

Thus, $g^{(2)}$ allows us to put an upper bound on the probability of creating a multiphoton state, which is exactly what we need to characterize the security of the system.

We now come back to the issue of intentionally adding losses after the device. It can be shown that adding linear loss to the source does not change $g^{(2)}$. The average photon number, on the other hand, is reduced to $\eta\bar{n}$. Substituting this back into p_{click} and p_m, we get

$$p_{click} \rightarrow \bar{n}\eta T + d, \tag{17}$$

$$p_m \rightarrow \frac{\overline{n^2}\eta^2 g^{(2)}}{2}. \tag{18}$$

As can be seen from the above equations, the probability p_{click} reduces only linearly with η, while p_m reduces quadratically. This means that by adding attenuation we can reduce the number of multiphoton states relative to the single-photon states. At larger loss levels the number of multiphoton states may be too big to allow secure communication. By introducing additional loss we can suppress this contribution to allow higher channel losses, at the expense of bit rate. We cannot do this indefinitely, however, because at some point the dark counts will start to dominate p_{click}.

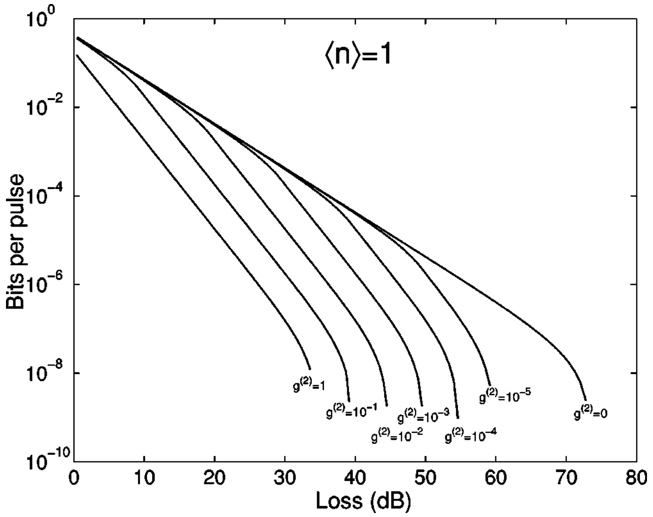

FIG. 2. Secure bits per pulse as a function of channel loss. Each device is assumed to produce an average photon number $\bar{n} = 1$.

We compare the communication rate as a function of the channel loss T for various sources ranging from Poisson light to ideal single-photon devices. The dark count rate r_d of a very good commercial avalanche photodiode can be around 20 s^{-1}. The measurement window τ_w is ultimately limited by the time jitter of the detector, which is usually around 500 ps. The dark count probability under these conditions is $d = 4 \times 10^{-8}$, where the factor of 4 comes from four detectors. We set the base line error rate μ to 1%. The additional loss η is assumed to be an adjustable parameter, and the bit rate is optimized with respect to this parameter for each value of T. Figure 2 shows the calculation results for the case where $\bar{n} = 1$. The normalized communication rate is plotted as a function of channel loss for different values of $g^{(2)}$. Poisson light corresponds to the curve $g^{(2)} = 1$, while the curve $g^{(2)} = 0$ is an ideal single-photon turnstile device. Note that the Poisson light bit rate decreases faster than the ideal single-photon device. This is because the single-photon device does not suffer from photon splitting attacks. Thus, the rate decrease is only due to the increasing channel loss. For Poisson light, as the channel loss increases, the effect of the multiphoton states is enhanced, forcing us to reduce the average number of photons. Intermediate devices with $0 < g^{(2)} < 1$ feature two types of behaviors. At low channel losses, they behave very similar to the ideal device where the bit rate decreases in proportion to the channel transmission. At higher loss levels, the multiphoton states start to make a significant contribution and the behavior gradually switches over to that of Poisson light.

As can be seen, each curve features a cutoff channel loss, beyond which secure communication is no longer possible. A

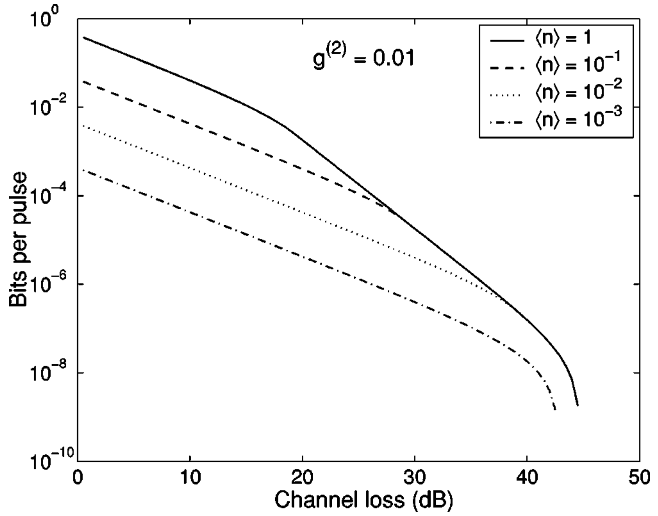

FIG. 3. Secure bits per pulse as a function of channel loss for devices with different efficiencies. All devices have $g^{(2)}=0.01$.

smaller $g^{(2)}$ implies that more loss can be tolerated, as expected. We would now like to investigate the effect of imperfect efficiency on the device performance. Figure 3 shows how the bit rate of the system varies with the efficiency of the device when $g^{(2)}=0.01$. At low loss levels the bit rate of the system decreases with decreased efficiency, as expected. But at higher loss levels most of the curves meet with the ideal curve, leaving the cutoff loss unaffected. Only the extremely lossy device with efficiency of 10^{-3} fails to rejoin the ideal curve, and features a smaller cutoff loss. The reason that most of the curves rejoin the ideal curve is that, at high loss levels, added attenuation is already required in order to reduce the effect of photon splitting attacks. For lossy devices, some of this attenuation is provided by device inefficiency. If this inefficiency does not exceed the attenuation required at the cutoff loss, then at some loss level, the curve for the lossy device will rejoin that of a lossless one. This leads us to the conclusion that, given $g^{(2)}$ and the system parameters such as the detector dark count rate d and the signal error rate μ, a critical efficiency value exists. If the device efficiency exceeds this critical efficiency, then the device can tolerate the same maximum channel losses as a perfectly efficient one. Furthermore, as channel losses increase, there will be a crossover point where the communication will no longer depend on the device efficiency. The value of the channel loss where this crossover point occurs, however, does depend on the device efficiency. Figure 3 shows that for the particular value of $g^{(2)}=0.01$, which is a realistic value for good single-photon devices, the critical efficiency is below 10^{-2}. Such efficiencies are within the reach of today's technological capabilities.

Unfortunately, it is very difficult to get a closed-form solution of the critical efficiency and loss cutoff from Eq. (6) because of the nonlinear nature of the equation. This forces us to resort to numerical methods. In the following section we use an approximate method to get a closed-form estimate on these two important quantities. This estimate will allow us to get a better intuitive understanding of the different tradeoffs involved.

III. ESTIMATES FOR DEVICE PERFORMANCE

In this section we derive closed-form approximations for the cutoff loss and critical efficiency of a sub-Poisson light source. Using the arguments presented in Ref. [9], we put an upper bound on the allowable error rate using the condition

$$e=\frac{\beta}{4}. \tag{19}$$

Since β is the fraction of single-photon states in the key, the condition above defines the point where Eve can intercept and resend all single-photon states, and perform a photon splitting attack on the multiphoton states. Secure communication is not possible beyond this point. We find the channel loss where the above condition is satisfied, which will serve as an estimate for the loss cutoff. The efficiency that optimizes the cutoff loss will give us an estimate for the critical efficiency. A device with efficiency exceeding this value can be attenuated down to the critical efficiency if the channel losses are close to the cutoff. Comparison with numerical calculations from Eq. (6) will show that the above estimates give a remarkably close approximation to the real value.

Note that both the error rate [given in Eq. (14)] and the parameter β [given in Eq. (7)] are functions of the channel transmission T. We can plug these equations back into Eq. (19) and solve for the channel transmission, which is given by

$$T=\frac{1}{1-4\mu}\left(\frac{d}{\overline{n}}+\frac{\overline{n}g^{(2)}}{2}\right). \tag{20}$$

The above equation gives us the value of the channel transmission where Eve can intercept and resend all single photons and perform a photon splitting attack on all multiphoton states. Here μ, d, and $g^{(2)}$ are considered to be fixed system parameters. When using Poisson light sources, the average photon number $\overline{n}$ is an adjustable parameter, which can be made arbitrarily large or small. This is because Poisson light sources, such as lasers, start with a macroscopically large number of photons that can be attenuated down to the desired final average. With sub-Poisson light the average is only adjustable by introducing loss, as previously discussed, and can never exceed the device efficiency.

Equation (20) shows more clearly the tradeoffs involved in optimizing T. If $\overline{n}$ is set too low, the first term on the right side of the equation becomes large. If it is set too high, the second term becomes large. For an ideal device we can set $\overline{n}=1$ and $g^{(2)}=0$, so that

$$T_{min}^{ideal}=d/(1-4\mu). \tag{21}$$

When the device is not ideal we can easily minimize T with respect to $\overline{n}$, resulting in the conditions

$$\overline{n}_c = \sqrt{\frac{2d}{g^{(2)}}}, \tag{22}$$

$$T_{min} = \frac{\sqrt{2dg^{(2)}}}{1-4\mu}. \tag{23}$$

In the above equations, $\overline{n}_c$ is the average photon number which minimizes Eq. (20), and T_{min} is the obtained minimum channel transmission. Equation (22) gives us an estimate for the critical efficiency. If the device efficiency exceeds this value, one can always attenuate down to optimal value when the channel transmission is close to its minimum value. If the device efficiency is below this value, however, there is no way to increase it in order to achieve the optimal efficiency. Note that for $\mu = 0$ and $g^{(2)} = 1$, we reproduce the bound derived in Ref. [9] for Poisson light. The above equations, however, can now be applied to any sources between Poisson light and ideal single-photon devices.

We note that on initial inspection there is an apparent inconsistency in Eq. (23) in the limit $g^{(2)} \to 0$. The equation predicts $T_{min} = 0$ in this limit, but we know that we can never do better than an ideal single-photon source, which is bounded by Eq. (21). However, note that in this limit $\overline{n}_c \to \infty$. The average photon number cannot be made arbitrarily large, and is ultimately limited by $g^{(2)}$. Using Eq. (4) and the fact that $\langle \hat{n}^2 \rangle \geqslant \overline{n}^2$, we have the bound

$$\overline{n} \leqslant \frac{1}{1-g^{(2)}}. \tag{24}$$

When $g^{(2)} \to 0$, $\overline{n} \leqslant 1$, with equality holding when the device creates exactly one photon per pulse. Thus, we should only use Eqs. (22) and (23) if $\overline{n}_c \leqslant 1$. For typical experiments we have $g^{(2)} = 0.01$ and $d = 4 \times 10^{-8}$, giving us $\overline{n}_c = 3 \times 10^{-3}$, which is well below 1.

Figure 4 shows a comparison between our estimate for the cutoff loss and critical efficiency, and the actual value calculated numerically from Eq. (6). In both cases, the estimate predicts the actual value to within a factor of 2 over a four-order-of-magnitude range for $g^{(2)}$.

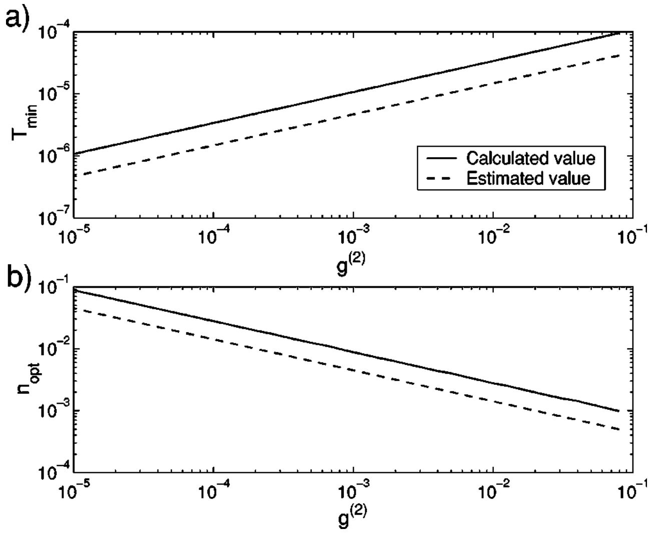

FIG. 4. (a) Comparison of the minimum channel transmission estimated by Eq. (23) and the actual value numerically calculated from Eq. (6). (b) Comparison of the critical efficiency estimated by Eq. (22) and the actual value numerically calculated from Eq. (6).

IV. DISCUSSION

We investigated the security of quantum key distribution with sub-Poisson light sources and showed that such sources can provide significantly improved performance over Poisson light. Furthermore, if the efficiency of a device exceeds some critical value, then this device can tolerate the same maximum amount of channel loss as a perfectly efficient device. We found an approximate closed form solution for this critical efficiency, which depends on only the dark count rate d and the second-order correlation $g^{(2)}$. For typical values of these two numbers this critical efficiency is around 3×10^{-3}, which is well within the reach of currently available devices. Thus, sub-Poisson devices are a promising technology for improving the performance of quantum cryptography systems.

[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), pp. 175–179.

[2] G. Brassard and C. Crepeau, SIGACT News **27**, 13 (1996).

[3] P. D. Townsend, IEEE Photonics Technol. Lett. **10**, 1048 (1998).

[4] C. Marand and P. T. Townsend, Opt. Lett. **20**, 1695 (1995).

[5] G. Rigbordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 517 (2000).

[6] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Johnson, T. Tsegaye, D. Ljunggren, and E. Sundberg, Opt. Express **4**, 383 (1999).

[7] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, Phys. Rev. Lett. **84**, 5652 (2000).

[8] N. Lütkenhaus, Phys. Rev. A **61**, 2304 (2000).

[9] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[10] C. Santori, M. Pelton, G. Solomon, Y. Dale, and Y. Yamamoto, Phys. Rev. Lett. **86**, 1502 (2001).

[11] P. Michler, A. Kiraz, C. Becher, W. V. Schoenfeld, P. M. Petroff, L. D. Zhang, E. Hu, and A. Imamoglu, Science **290**, 2282 (2000).

[12] B. Lounis and W. E. Moener, Nature (London) **407**, 491 (2000).

[13] R. Brouri, A. Beveratos, J. P. Poizat, and P. Grangier, Phys. Rev. A **6206**, 3817 (2000).

[14] Z. Yuan, B. E. Kardynal, R. M. Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper, Science **295**, 102 (2002).

[15] C. Brunel, B. Lounis, P. Tamarat, and M. Orrit, Phys. Rev. Lett. **83**, 2722 (1999).

[16] F. De Martini, G. Di Giuseppe, and M. Marrocco, Phys. Rev. Lett. **76**, 900 (1996).

[17] J. Kim, O. Benson, H. Kan, and Y. Yamamoto, Nature (London) **397**, 500 (1999).

[18] C. Kurtsiefer, S. Mayer, P. Zarda, and H. Weinfurter, Phys. Rev. Lett. **85**, 290 (2000).

[19] E. Moreau *et al.*, Appl. Phys. Lett. **79**, 2865 (2001).

[20] V. Zwiller, H. Blom, P. Jonsson, N. Panev, S. Jeppesen, T. Tsegaye, E. Goobar, M. Pistil, L. Samuelson, and G. Björk, Appl. Phys. Lett. **78**, 2476 (2001).

[21] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, Berlin, 1994).

[22] G. Brassard and L. Salvail, *Advances in Cryptology—EUROCRYPT '93*, edited by T. Hellseth, Lecture Notes in Computer Science Vol. 765 (Springer, Berlin, 1994), pp. 410–423.

[23] C. H. Bennett, G. Brassard, C. Cripeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[24] D. Mayers, Natural Hazards **48**, 351 (2001).

[25] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowder, in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2000), pp. 715–724.

[26] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

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