Security of differential-phase-shift quantum key distribution against individual attacks

Edo Waks
E. L. Ginzton Labs, Stanford University, Stanford, California 94305, USA

Hiroki Takesue
NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa, Japan

Yoshihisa Yamamoto
E. L. Ginzton Labs, Stanford University, Stanford, California 94305, USA
and National Institute of Informatics, Tokyo, Japan
(Received 28 October 2005; published 31 January 2006)

We derive a proof of security for the differential-phase-shift quantum key distribution protocol under the assumption that Eve is restricted to individual attacks. The security proof is derived by bounding the average collision probability, which leads directly to a bound on Eve's mutual information on the final key. The security proof applies to realistic sources based on pulsed coherent light. We then compare individual attacks to sequential attacks and show that individual attacks are more powerful.

DOI: 10.1103/PhysRevA.73.012344 PACS number(s): 03.67.Dd

I. INTRODUCTION

The goal of quantum cryptography is to exchange an unconditionally secure secret key over a potentially hostile environment. To date, a variety of protocols have been proposed to accomplish this goal. The first of these protocols was originally proposed by Bennett and Brassard in 1984 (BB84) [1]. Since that ground-breaking result, a variety of additional protocols have been proposed [2–6], with varying advantages and disadvantages.

One of the more recent protocols is known as the differential-phase-shift quantum key distribution (DPSQKD for short) [7]. This protocol appears to have several important advantages which make it extremely promising for practical systems. First, DPSQKD can be easily implemented in optical fibers using readily available optical telecommunication tools. Second, there is good indication that DPSQKD is largely insensitive to multiphoton states generated by the source, as opposed to other protocols such as BB84. This allows the communicating parties to transmit much brighter coherent states, leading to higher communication rates and longer communication distances.

To date, all security statements about DPSQKD have been based on considering only very restricted types of eavesdropping attacks, such as intercept and resend or inserting a beamsplitter. This leads to the possibility that more sophisticated attacks based on generalized quantum measurements may exist which could potentially nullify many of the advantages of DPSQKD. Thus, it is important to have a security proof for this protocol which works for a more general class of attacks. Furthermore, because robustness to photon splitting attacks is one of the main features of this protocol, it is important that the proof of security includes these types of attacks.

The most general attacks that one may consider in quantum cryptography are known as coherent or joint attacks. In these types of attacks Eve treats the entire key as a single quantum system, which is entangled with a probe state. The probe is only measured after all classical information is exchanged. Coherent attacks allow Eve to take advantage of correlations induced by classical information exchanged during error correction and privacy amplification. The proof of security against coherent attacks is extremely difficult. To date, there are several proofs of security for the BB84 protocol against these most general types of attacks [8,9]. A general security proof for the B92 [4] protocol has also been derived [10]. In order to make the problem more tractable, one often restricts eavesdropping to individual attacks. In these types of attacks, it is assumed that Eve attaches an independent probe to each photon, and then measures the probes independently. The security of the BB84 protocol against individual attacks has been investigated in several works [11–13]. The security of the B92 protocol against individual attacks has also been proven [14]. The restriction to individual attacks is often considered a realistic assumption because the capability to perform joint attacks is well beyond the domain of modern technology. Such attacks would require that an eavesdropper possess a probe of extremely large dimensionality (on the order of the length of the string) with indefinite coherence time, and processes the probe states with a quantum computer. Even individual attacks require a degree of quantum computational power which seems out of reach for the foreseeable future.

In this paper, we derive a proof of security for DPSQKD against individual attacks. The proof applies to realistic sources based on attenuated lasers, and accounts for the Poisson nature of the photon statistics injected into the channel. Security is proved by deriving a bound on Eve's average collision probability, which directly leads to a bound on her mutual information for the final key [15]. We use this result to calculate the communication rate of DPSQKD in the limit of large strings. We then compare this rate to that of the

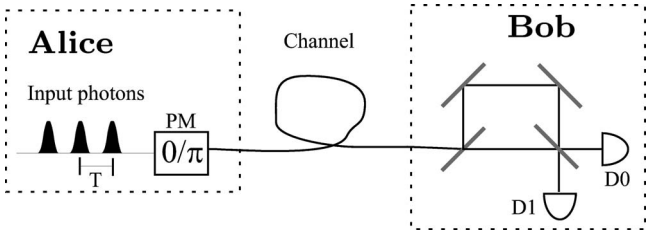

FIG. 1. A basic DPSQKD system.

BB84 protocol using both single photon sources and Poisson light sources. We show that DPSQKD achieves rates very close to the BB84 protocol with an ideal single photon source, and significantly outperforms the BB84 protocol with Poisson light. This is an important result because DPSQKD requires only attenuated laser light and linear optics, in contrast to single photon sources which are difficult to implement. In the final section of this paper, we consider another type of eavesdropping attack known as a sequential attack. These types of attacks are not individual attacks, so they are not accounted for by our proof of security. However, they are conceptually simple and have raised a level of concern regarding the security of DPSQKD. We calculate the communication rate against these types of attacks and compare it to the rate for individual attacks. It turns out that in our parameter range of interest, the communication rate for individual attacks is always lower than the sequential attacks. Thus security against individual attacks automatically implies security against sequential attacks.

II. DIFFERENTIAL PHASE SHIFT QKD

Figure 1 shows the basic idea behind DPSQKD. Alice prepares a periodic train of attenuated laser pulses whose phase is randomly modulated to be 0 or π. The coherent pulses are sent down the quantum channel and received by Bob, who measures them using an unbalanced interferometer which combines the partial wave at time slot n with time slot $n+1$ on a beamsplitter. If the phase difference between these two pulses is 0, a detection event will only occur in detector D0. Similarly, if the phase difference is $\pm\pi$, detection events will only occur in detector D1. Bob records the detection events and the times they that occurred at. Once the quantum communication is done, Bob announces at which times he detected a photon. This information allows Eve to determine Bob's string based on her knowledge of the phase differences. Error correction and privacy amplification can then be performed on the sifted key to create the final secure key.

To get an idea as to why this protocol is secure, let us consider some simple attacks Eve might try to perform. Two basic attacks are shown in Fig. 2. The first attack is an intercept and resend strategy, in which Eve uses the same type of interferometer as Bob. When Eve gets a detection event time t_m, she learns the phase difference between the pulses at time t_m and t_{m+1}. She then prepares a pair of pulses with the measured phase difference and sends them to Bob. If Bob detects a photon at time t_m, then Eve has successfully stolen a bit without inducing errors. However, if a detection instead occurs at times t_{m+1} or t_{m-1}, then Bob will observe a 50% error rate, and Eve will have no knowledge about that bit of the key. This strategy, therefore, induces a 25% overall error rate which can be detected by Alice and Bob, revealing Eve's presence.

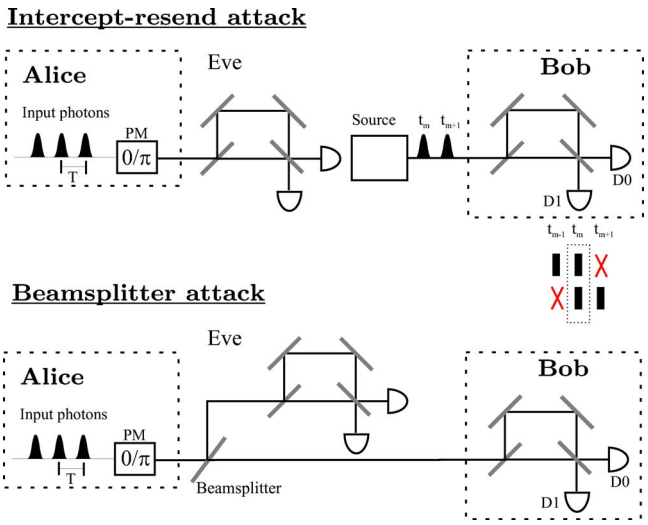

FIG. 2. (Color online) Schematic of intercept-resend and beamsplitter eavesdropping strategies.

In the second strategy, Eve inserts a beamsplitter into the channel to pull of a fraction of the light. This split off fraction is then measured by an unbalanced interferometer, while the remainder is sent to Bob. We assume Eve posseses a lossless channel with which she can transmit the unsplit photons to Bob. This allows her to split off a fraction of the photons equal to the channel loss without modifying the communication rate. Because coherent states are being used, Eve's detection events are independent of Bob's. Thus, the probability that Eve knows the value of a bit at time m given Bob detected a photon at that time, denoted $p_e(m)$, is simply given by

$$p_{split}(m) = \bar{n}(1-\eta) \approx \bar{n}, \tag{1}$$

where $\bar{n}$ is the average number of photons per pulse. For small values of $\bar{n}$, this attack provides little information about the sifted key. If Eve delays her measurement and uses an optical switch, she can improve the attack by a factor of 2.

III. PHOTON SPLITTING IN DPSQKD

In this section we lay the groundwork for the proof of security. We start by giving a mathematical description of individual attacks. We then investigate photon splitting attacks in DPSQKD. The state prepared by Alice, denoted $|\psi\rangle$, is a set of consecutive coherent state pulses. The phase shift ϕ_n is the phase induced by the phase modulator on pulse n. This phase can take on the values 0 and π. If Alice transmits N coherent pulses, we have

$$|\psi\rangle = \bigotimes_{n=0}^{N-1} |\alpha e^{i(\phi+\phi_n)}\rangle \tag{2}$$

where ϕ is the initial phase of the coherent state. We define the bosonic operator $\hat{\psi}^\dagger$ as

$$\hat{\psi}^\dagger = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{i\phi_n} \hat{\mathbf{a}}_n^\dagger, \tag{3}$$

where $\hat{\mathbf{a}}_n^\dagger$ is the creation operator for a photon in time slot n. Assuming that the time slots do not overlap, these different operators commute with each other. Thus, the state in Eq. (2) can be rewritten as

$$|\psi\rangle = \sum_{j=0}^{\infty} \sqrt{P(j)} e^{ij\phi} \frac{(\hat{\psi}^\dagger)^j}{\sqrt{j!}} |0\rangle, \tag{4}$$

where $P(j)$ is a Poisson distribution with an average photon number $N\bar{n}$, and $\bar{n}=|\alpha|^2$. A fundamental assumption of the DPSQKD protocol is that Eve does not possess a phase reference. Because of this, the above state should be averaged out over the different values of the phase ϕ, resulting in the mixed state

$$\rho_e = \sum_{j=0}^{\infty} P(j) |\psi_j\rangle\langle\psi_j|, \tag{5}$$

where $|\psi_j\rangle=(\hat{\psi}^\dagger)^j/\sqrt{j!}|0\rangle$. With no loss of generality, Eve can measure the photon number using a state preserving quantum nondemolition measurement. She can then split off $N\bar{n}T$ of the photons, where T is the transmission efficiency of the channel, and send them to Bob, while storing $N\bar{n}(1-T)$ photons coherently to be measured after Alice and Bob have revealed all classical information.

There are now two components of the eavesdropping strategy which must be addressed. The first is how much information can be extracted from the split photons. This component is analogous to the information obtained from photon splitting attacks in BB84. Second, in the presence of channel noise Eve can potentially attack the fraction of the key that she transmits to Bob by entangling it with a probe state. This part of the eavesdropping attack is analogous to the general POVM attacks on single photon states. We will investigate the split photon component first, and then the POVM on the transmitted photons.

Our analysis makes an auxiliary assumption that Eve attacks each photon individually. For the photons that are transmitted to Bob, each one is individually split and attached to an independent probe. The probes are then independently measured after all classical communication is received. The split photons are also individually stored and measured. The individual attacks assumption implies that Eve cannot use the measurement results of one photon to refine her measurement on the rest of the photons. Thus, if Eve has split off k photons, she has k copies of the state $\hat{\psi}^\dagger|0\rangle$. Eve stores these k copies coherently until all public information is revealed. After the quantum transmission is done, Bob will publicly announce the time slots in which he had a detection event. Let B be the set of all time slots in which a detection event was observed, and $\bar{B}$ be the set of all other time slots. The operator $\hat{\psi}^\dagger$ can be rewritten as

$$\hat{\psi}^\dagger = \frac{1}{\sqrt{N}} \left[\sum_{m\in B} e^{i\phi_m} (\hat{\mathbf{a}}_m^\dagger + e^{i\Delta\phi_m} \hat{\mathbf{a}}_{m+1}^\dagger) + \sum_{n\in\bar{B}} e^{i\phi_n} \hat{\mathbf{a}}_n^\dagger \right] |0\rangle. \tag{6}$$

For each time slot in B, Eve can perform the following unitary transformation

$$\hat{\mathbf{a}}_m^\dagger \to \frac{1}{\sqrt{2}} (\hat{0}_m^\dagger + \hat{1}_m^\dagger), \tag{7}$$

$$\hat{\mathbf{a}}_{m+1}^\dagger \to \frac{1}{\sqrt{2}} (\hat{0}_m^\dagger - \hat{1}_m^\dagger), \tag{8}$$

where $\hat{0}_m^\dagger$ and $\hat{1}_m^\dagger$ are orthogonal modes. There is no loss of generality in assuming that this transformation is performed, because it is unitary and simply represents a transformation of the measurement basis. If measurement basis $|E\rangle$ is optimal for the state in Eq. (6), then the basis $U^\dagger|E\rangle$ is now optimal after the unitary transformation U is applied. The state of each split photon is now given by

$$\hat{\psi}^\dagger = \frac{1}{\sqrt{N}} \left[\sum_{m\in B} e^{i\phi_m} \sqrt{2} \hat{x}_i^\dagger + \sum_{n\in\bar{B}} e^{i\phi_n} \hat{\mathbf{a}}_n^\dagger \right], \tag{9}$$

where $\hat{x}_i^\dagger$ is $\hat{0}_i^\dagger$ if Alice sent a binary 0, and $\hat{1}_i^\dagger$ if Alice sent 1. Thus, Eve's split photons are in a linear superposition of all the bits of the secret key, plus the irrelevant time slots where no photon was detected. However, because Eve does not know the phases ϕ_m, her state is in fact a mixture of the different values of ϕ_m. Specifically,

$$\begin{aligned} \rho_e &= \sum_{\phi_1\ldots\phi_k} p(\phi_1, \ldots, \phi_k) \hat{\psi}^\dagger |0\rangle\langle 0| \hat{\psi} \\ &= \frac{1}{N} \left[2 \sum_{m\in B} |x_m\rangle\langle x_m| + \sum_{n\in\bar{B}} |n\rangle\langle n| \right]. \end{aligned} \tag{10}$$

In the above equation $|x_m\rangle=\hat{x}_m^\dagger|0\rangle$ and $|n\rangle=a_n^\dagger|0\rangle$. The phases ϕ_i are summed over the possible values of 0 and π, which have equal probability so that $p(\phi_1, \ldots, \phi_k)=1/2^k$. From Eq. (10) we see that Eve's state is, in fact, a random mixture of orthogonal states. This turns the problem into one of classical probability theories instead of quantum measurement. That is, if Bob recorded y detection events, each split photon will reveal a bit of Eve's key with probability $2y/N$, and will reveal no information at all with probability $1-2y/N$.

Let us define T as the channel transmission and $\bar{n}$ as the average number of photons per pulse. After N pulses, Bob will observe on average $N\bar{n}T$ detection events. Assuming Eve has possession of a lossless channel, she must transmit $N\bar{n}T$ photons to Bob, and can split off the remainder $N\bar{n}(1-T)$ photons to be stored coherently. After Bob reveals the time slots of his detection events, Eve can measure her split photons, in which case she learns $2N\bar{n}^2T(1-T)$. Thus, from the split photons Eve learns a fraction $2\bar{n}(1-T)\approx 2\bar{n}$ of the shifted key. If $\bar{n}=0.1$, Eve learns only 20% of the final key.

The most important aspect of the above conclusion is that, in contrast to BB84, the amount of information Eve obtains from photon splitting attacks is independent of channel loss. In BB84, as the channel losses get larger Eve can preferentially transmit multiphoton states and block off an appropriate fraction of the single photon states to conserve the overall communication rate. As the channel loss becomes larger, this type of attack gives her complete information over an increasingly larger fraction of the key. This results in a final communication rate which is roughly a quadratic function of channel loss, and hence decreases very quickly. In contrast, in DPSQKD the fraction of the final key that is revealed is only a function of $\bar{n}$. This leads to a communication rate which decreases only linearly with a channel loss, indicating robustness against photon splitting attacks.

IV. PROOF OF SECURITY

In the previous section we showed that due to photon splitting, Eve obtains complete information over a fraction $2\bar{n}$ of the key. When $\bar{n}$ is small, photon splitting attacks are largely ineffective. However, in the presence of channel noise Eve can also attack the photons that she transmits to Bob by entangling them with a probe state, and then measuring the probe after all classical information has been revealed.

Because we restrict our attention to individual attacks, it is assumed that Eve attaches an independent probe to each photon, and these probes are all measured independently. The goal of a proof of security is to come up with a bound for the average collision probability [11], defined as

$$P_c = \sum_{x,z,m} p^2(X=x|Z=z,M=m)p(z,m), \tag{11}$$

where X is the key Alice transmitted to Bob, Z is the information Eve obtained from measuring the photon, and M is the set of time slots in which Bob detected a photon, which is also known to Eve. For the case of individual attacks, bit i originated from one photon which is correlated to an independent probe state Z_i, as well as M_i which is the time of the detection. In this case, the collision probability simplifies to a product of the collision probabilities of each individual bit [16]. Thus,

$$P_c = \prod_i Pc_0, \tag{12}$$

where

$$Pc_0 = \sum_{x,z,m} p^2(X_i=x|Z_i=z,M_i=m)p(Z_i=z,M_i=m). \tag{13}$$

If bit i occurred in a time slot where Eve has obtained its value due to photon splitting, then $Pc_i=1$. Let $\bar{S}$ be the set of all bits that occurred in time slots which do not coincide with a photon splitting measurement. We now have

$$P_c = \prod_{i\in\bar{S}} Pc_0. \tag{14}$$

We adopt a simplified notation such that $P(X_i=x|Z_i=z,M_i=m)=p(x|z,m)$, and use similar notation for all other probability distributions. Appendix A shows that the expression in Eq. (13) can be rewritten as

$$Pc_0 = \sum_m p(m)\left(1-\frac{1}{2p(m)}\sum_z \frac{p(z,m|0)p(z,m|1)}{p(z,m)}\right), \tag{15}$$

where 0 and 1 are the possible values of the bit that Alice transmitted.

We now develop a mathematical formalism for all possible measurements Eve can perform. We define $|E_i\rangle$ as the initial state of Eve's Hilbert space. We do not assume anything about the dimensionality of this space. The initial state of a photon-probe system is given by

$$|\Psi\rangle = \frac{1}{\sqrt{N}}\sum_n e^{i\phi_n}|n\rangle|E_i\rangle, \tag{16}$$

where $|n\rangle$ is once again defined as $\hat{\mathbf{a}}_n^\dagger|0\rangle$ and represents a photon in time slot n. The most general unitary transformation Eve can apply to the system is described by

$$|n\rangle|E_i\rangle \rightarrow \sum_m |m\rangle|E_{n,m}\rangle, \tag{17}$$

where $|E_{n,m}\rangle$ are states in Eve's Hilbert space and are not assumed to be normalized or orthogonal. Plugging the above relation back into Eq. (16) and rearranging the summation we obtain

$$|\Psi\rangle = \frac{1}{\sqrt{N}}\sum_m |m\rangle\sum_n e^{i\phi_n}|E_{n,m}\rangle = \frac{1}{\sqrt{N}}\sum_m |m\rangle|J_m\rangle. \tag{18}$$

After Bob's interferometer, the state is once again transformed into

$$|\Psi\rangle = \frac{1}{2\sqrt{N}}\sum_m [(|J_m\rangle+|J_{m+1}\rangle)|0_m\rangle + (|J_m\rangle-|J_{m+1}\rangle)|1_m\rangle], \tag{19}$$

where $|0_m\rangle$ and $|1_m\rangle$ represent a photon in the output ports of Bob's interferometer which corresponds to a binary 0 or 1 at time m.

In Appendix B, it is shown that the probability of an error given that Bob detected, a photon at time m is given by the expression

$$p_{e|m} = \frac{1}{2}\left[1-\frac{1}{Np(m)}(\langle E_{m,m}|E_{m+1,m+1}\rangle + \langle E_{m,m+1}|E_{m+1,m}\rangle)\right]. \tag{20}$$

Eve will measure her probe in the basis $|z\rangle$, which cannot depend on ϕ_m since this information is unavailable. We define the number $E_{n,m}(z)=\langle z|E_{n,m}\rangle$. Without the loss of generality we can assume this to be a real number. We do not need to introduce complex numbers in this case because a probe state with a complex probability amplitude can always be replaced by a probe of higher dimensionality with real prob-

ability amplitudes which perform at least as well [11]. We also define the following expressions:

$$Q_m(z) = E_{m,m}(z) + E_{m+1,m}(z), \tag{21}$$

$$P_m(z) = E_{m,m}(z) - E_{m+1,m}(z), \tag{22}$$

$$Q_{m+1}(z) = E_{m,m+1}(z) + E_{m+1,m+1}(z), \tag{23}$$

$$P_{m+1}(z) = E_{m,m+1}(z) - E_{m+1,m+1}(z). \tag{24}$$

In Appendix C we show that the collision probability is given by the expression

$$Pc_0 = 1 - \frac{1}{4N}\sum_{m,z} \frac{[Q_m^2(z) + Q_{m+1}^2(z) + \sum_{n\neq m,m+1} E_{n,m}^2 + E_{n,m+1}^2][P_m^2(z) + P_{m+1}^2(z) + \sum_{n\neq m,m+1} E_{n,m}^2 + E_{n,m+1}^2]}{\sum_n E_{n,m}^2 + E_{n,m+1}^2}. \tag{25}$$

From the above expressions, it is clear that $E_{n,m}(z)$, where $n \neq m-1, m, m+1$ can only decrease Eve's collision probability while simultaneously increasing the error rate. Thus, we only need to consider the states $|E_{m-1,m}\rangle$, $|E_{m,m}\rangle$, and $|E_{m+1,m}\rangle$. We relabel these states as $|A_m\rangle$, $|B_m\rangle$, and $|C_m\rangle$, respectively. We similarly define $A_m(z)=\langle z|A_m\rangle$, $B_m(z)=\langle z|B_m\rangle$, $C_m(z)=\langle z|C_m\rangle$. The probability of an error is now given by

$$p_{e|m} = \frac{1}{2} - \frac{1}{2Np(m)}\sum_m (\langle B_m|B_{m+1}\rangle + \langle C_m|A_{m+1}\rangle). \tag{26}$$

We also have the expressions

$$Q_m(z) = B_m(z) + C_m(z), \tag{27}$$

$$P_m(z) = B_m(z) - C_m(z), \tag{28}$$

$$Q_{m+1}(z) = A_{m+1}(z) + B_{m+1}(z), \tag{29}$$

$$P_{m+1}(z) = A_{m+1}(z) - B_{m+1}(z). \tag{30}$$

In Appendix D it is shown that the collision probability is upper bounded by

$$Pc_0 \leq 1 - \frac{1}{8N}\sum_{m,z} (\langle A_m|A_m\rangle + \langle C_{m+1}|C_{m+1}\rangle + \langle Q_m|P_m\rangle + \langle Q_{m+1}|P_{m+1}\rangle + \langle Q_m|P_{m+1}\rangle + \langle Q_{m+1}|P_m\rangle). \tag{31}$$

In Appendix E we show that there is always an optimal attack that satisfies the property that the inner product of the vectors $|A_m\rangle$, $|B_m\rangle$, and $|C_m\rangle$ with any other vector from this set is independent of m. This directly implies that $p(m) = 1/N$ and that the collision probability is independent of m. Thus,

$$Pc_0 \leq 1 - \frac{1}{8}\sum_z (\langle A_0|A_0\rangle + \langle C_1|C_1\rangle + \langle Q_0|P_0\rangle + \langle Q_1|P_1\rangle + \langle Q_0|P_1\rangle + \langle Q_1|P_0\rangle), \tag{32}$$

$$e = \frac{1 - \langle B_0|B_1\rangle - \langle C_0|A_1\rangle}{2}, \tag{33}$$

where e is the bit error rate of the transmission. We must now maximize Eq. (32) subject to the constraint in Eq. (33). This is done in Appendix F, where it is shown that

$$Pc_0 \leq 1 - e^2 - \frac{(1-6e)^2}{2}. \tag{34}$$

The above equation applies when the error rate is in the range $[0, \frac{6}{38}]$. The point $e=\frac{6}{38}$ is the point at which the above equation is maximized. When the error rate exceeds this value the collision probability saturates. There is no attack that allows Eve to have complete information on the key. This is in contrast to BB84 where Eve can steal Alice's photons and send an uncorrelated photon to Bob. After the measurement basis is revealed, Eve learns the bit but simultaneously induces a 50% error rate.

Plugging the expression in Eq. (34) back into Eq. (14), we obtain the following expression for Eve's total collision probability on the k bit string:

$$Pc = Pc_0^{k(1-2\bar{n})}. \tag{35}$$

Using the methods of generalized privacy amplification, the length of the final key should be set to

$$r = -\log_2 Pc - \kappa - s, \tag{36}$$

where κ is the number of bits exchanged during the error correction and s is a security parameter [15]. The final communication rate, defined as $R=\lim_{k\to\infty} r/k$, is given by

$$R_{DPS} = -p_{click}[-(1-2\bar{n})\log_2 Pc_0(e) + f(e)h(e)]. \tag{37}$$

In the above equation p_{click} is the probability where Bob detects a photon, $h(e)=-e\log_2 e-(1-e)\log_2(1-e)$, and $f(e)$ is a function which characterizes how far above the Shannon limit the error correction algorithm is performing [see [17]]. For error correction algorithms working in the Shannon limit, which is the ultimate performance limit of all error correction algorithms, we have $f(e)=1$.

V. COMPARISON OF DPSQKD TO BB84

Having derived a bound on the average collision probability in the previous section, we can now compare DPSQKD to the BB84 protocol. A bound on the collision probability for the BB84 protocol for realistic sources against individual attacks has been previously derived in [17]. In this work, the communication rate was shown to be

$$R_{BB84} = p_{click}\left\{-\beta \log_2\left[\frac{1}{2} + 2\left(\frac{e}{\beta}\right) - 2\left(\frac{e}{\beta}\right)^2\right] - f(e)h(e)\right\}, \tag{38}$$

where

$$\beta = \frac{p_{click} - p_m}{p_{click}}. \tag{39}$$

In the above expression, p_m is the probability that the source emits a multiphoton state into the channel.

Bob's detection events originate from two sources, the photons injected into the channel by Alice and dark counts in Bob's detector. We assume that both the signal and dark count detection probabilities are small, so that multiple detection events can be ignored. Thus,

$$p_{click} = \bar{n}T + d, \tag{40}$$

where $\bar{n}$ is the average number of photons injected into the channel, T is the channel transmission, and d is the detector dark count rate. The error rate e is given by the expression

$$e = \frac{\mu p_{click} + d/2}{p_{click}}, \tag{41}$$

where μ is the baseline error rate of the system due to imperfections in state preparation, channel induced noise, and imperfect detection apparatus.

We compare DPSQKD to the BB84 protocol using both a Poisson photon source and ideal single photon source. For Poisson light sources, $\bar{n}$ is freely adjustable and $p_m \leq \bar{n}^2/2$. In contrast, an ideal single photon source is characterized by $\bar{n}=1$ and $p_m=0$. The detector dark count rate is an important parameter in the simulation. For telecom wavelengths, one of the most promising photon detectors is based on an upconversion of 1.5 μ photons to visible wavelengths, where they can be detected using conventional silicon avalanche photodiodes [18]. Such detectors have already been used to experimentally demonstrate DPSQKD in the telecom wavelengths, allowing communication distances over 100 km of fiber [19]. The experimentally measured dark count rate for these detectors is 10 kHz per detector. The APDs have a temporal resolution of 0.5 ns. If the signal is windowed to this resolution level, the dark count rate per pulse is 5×10^{-6} dark counts per detector. Since DPSQKD uses two detectors, the overall dark count rate is 10^{-5}. In contrast, BB84 with passive modulation [11] use four detectors giving a dark count rate of 2×10^{-5}. The baseline error rate is set to $\mu=0.01$. The parameter $\bar{n}$ is freely adjustable for BB84 with Poisson light, as well as for DPSQKD. In the simulations, the value of $\bar{n}$ is numerically optimized for each value of the channel loss.

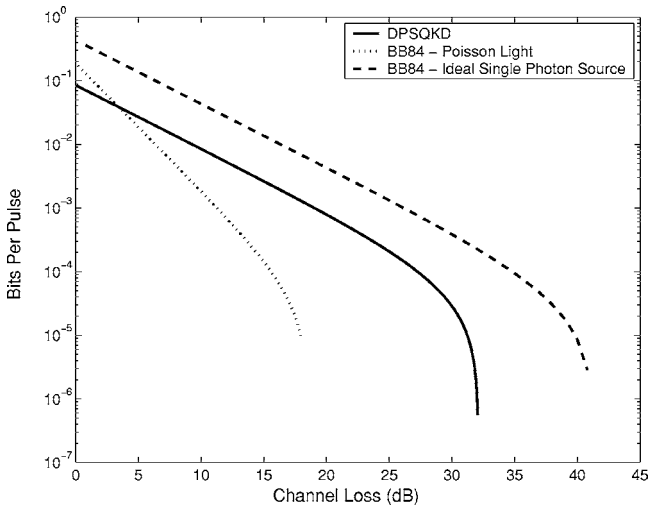

FIG. 3. Communication rate vs channel loss for DPSQKD and BB84.

The results of the simulation are shown in Fig. 3. The communication rate is plotted vs the channel loss in units of dB. One can see that all three curves feature an exponential decay for a period of time, after which the communication rate quickly drops to 0. This sharp cutoff is caused by the dark counts in Bob's detectors. The curve for BB84 with Poisson light decays as a faster exponential than both the DPSQKD and BB84 protocol with an ideal single photon source. This is due to photon splitting attacks, which require us to lower $\bar{n}$ with increasing channel loss. DPSQKD does not suffer from these types of attacks, therefore it follows more closely the curve for the BB84 protocol with an ideal single photon source. This is a very important conclusion, because DPSQKD can be implemented with conventional lasers, detectors, and linear optics, in contrast to the engineering of ideal single photon sources for BB84.

VI. SEQUENTIAL ATTACKS

In the previous two sections we investigated the security of DPSQKD against individual attacks. The fundamental assumption in this analysis was that Eve measures each photon independently, and does not use the measurement results of some of the photons to refine the measurement of the remaining photons. However, in DPSQKD there are certain attacks which do not satisfy this assumption, but which are conceptually very simple. One such attack is the sequential attack.

In a sequential attack, Eve uses a detection apparatus equivalent to Bob's setup, which she places in the quantum channel very close to Alice. Eve then waits for k consecutive clicks on her detection apparatus. Whenever such an event occurs, Eve can reconstruct a $k+1$ time slot state. This states induces an error rate of

$$\epsilon_{seq} = \frac{1}{2(k+1)}. \tag{42}$$

Of course, the probability of observing k consecutive clicks decreases exponentially with k. If $\bar{n}$ is the average number of

photons per pulse, then the probability of k consecutive clicks is $\bar{n}^k$. This probability must be at least as large as Bob's detection probability in order for Eve to conserve the overall detection rate. Thus, we must have $\bar{n}^k \geqslant \bar{n}T$, which imposes an upper bound on k.

The collision probability for sequential attacks is very easy to calculate. When Bob detects a photon in any time slot other than slots 1 or $k+2$, Eve knows the value of Alice's key. This happens with the probability $k/(k+1)$. If Bob detects a photon in slots 1 or $k+2$, then Eve knows nothing about Alice's key, so her collision probability is $\frac{1}{2}$. If Eve performs M sequential attacks, her collision probability is given by

$$P_{c0} = \frac{1}{2^{M/k+1}}. \tag{43}$$

From the condition $\bar{n}^k = \bar{n}T$ we obtain that

$$k = \log_{\bar{n}} T + 1. \tag{44}$$

This condition ensures that there are enough sequential clicks to conserve the communication rate. However, even if the number of sequential clicks is sufficient, Eve may not be able to perform an attack on every bit of the key, because she cannot exceed the natural system error rate which we define as ϵ_s. She can only perform a sequential attack on a fraction $\epsilon_s/\epsilon_{seq}$ of the bits, and must leave the remainder of the string undisturbed to conserve the error rate. Thus, if N is the number of bits in Alice's string, then

$$M = \frac{N\epsilon_s}{\epsilon_{seq}} = N(k+1)\epsilon_s. \tag{45}$$

Plugging the above equation into Eq. (43), and using Eq. (36), we obtain the communication rate

$$R_{seq} = p_{click}[1 - 2\epsilon_s(\log_{\bar{n}} T + 1) - f(e)h(e)]. \tag{46}$$

We compare this communication rate to that of DPSQKD calculated in the previous section. Using the same values for the dark count and error rate, we plot the communication rate for sequential attacks and individual attacks in Fig. 4. For individual attacks, the average photon number $\bar{n}$ is once again optimized for each value of the channel loss. We then use the same optimal $\bar{n}$ to evaluate the rate for sequential attacks, so that we may compare the effectiveness of individual and sequential attacks under the same operating condition. One can see that the communication rate for individual attacks is always lower than sequential attacks, indicating that in the operating regime we are considering it is more advantageous for Eve to perform individual instead of sequential attacks. This means that security against individual attacks already implies security against sequential attacks as well.

Of course, we do not know if the sequential attacks are optimal, or if a more clever scheme could produce better results for Eve. To answer this question, a more general proof of security is needed.

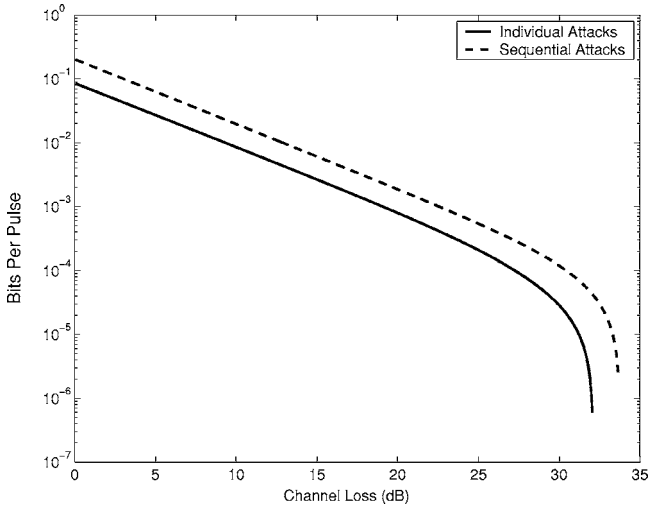

FIG. 4. Comparison of individual attacks to sequential attacks in DPSQKD.

VII. CONCLUSION

In conclusion, we have derived a proof of security for DPSQKD with realistic sources against individual attacks. This proof allows us to directly calculate the communication rate after privacy amplification. We showed that, in contrast to the BB84 protocol, the DPSQKD does not suffer from photon splitting attacks even when implemented with attenuated lasers. We compared the communication rate as a function of channel loss for DPSQKD to the BB84 protocol using both an attenuated laser and an ideal single photon source. DPSQKD allows us to achieve communication rates close to the BB84 protocol with an ideal single photon source, making it an outstanding candidate for practical long distance quantum cryptography. We then compared individual attacks to sequential attacks in DPSQKD and showed that individual attacks are more powerful in our operating regime. Thus, security against individual attacks already ensures security against sequential attacks as well.

ACKNOWLEDGMENTS

Financial support for this work was provided by the MURI Center for photonic quantum information systems (ARO/ARDA Program No. DAAD19-03-1-0199), as well as by a DCI Grant.

APPENDIX A: EXPRESSION FOR COLLISION PROBABILITY

Here we derive the expression for the collision probability given in Eq. (15). We start with Eq. (13), and use the Bayes rule to rewrite it as

$$Pc_0 = \sum_m p(m) \sum_z \frac{p^2(z|0,m)p^2(0|m) + p^2(z|1,m)p^2(1|m)}{p(z|m)}. \tag{A1}$$

By completing the square, we can rewrite the above expression as

$$Pc_0 = \sum_m p(m)\left(1 - 2\sum_z \frac{p(0)p(1)p(z,m|0)p(z,m|1)}{p(z,m)p(m)}\right). \tag{A2}$$

Using the fact that $p(0)=p(\pi)=\frac{1}{2}$ directly leads to the result stated in Eq. (15).

APPENDIX B: DERIVATION OF THE ERROR RATE

In this section we show that Eve's attack strategy leads to an error rate given by Eq. (20). We start with the obvious relation $p_{e,m}=(p_{e,m|0}+p_{e,m|1})/2$. We define the states $|M_+\rangle = |J_m\rangle + |J_{m+1}\rangle$ and $|M_-\rangle = |J_m\rangle - |J_{m+1}\rangle$. We define $E_{\phi_1,\ldots,\phi_k}[A]$ as the average of expression A over the possible values of $\phi_1,\ldots,\phi_k$. It is straightforward to show that

$$p(m) = \frac{1}{4N}E_{\phi_1,\ldots,\phi_k}[\langle M_-|M_-\rangle + \langle M_+|M_+\rangle]$$

$$= \frac{1}{2N}\sum_n \langle E_{n,m}|E_{n,m}\rangle + \langle E_{n,m+1}|E_{n,m+1}\rangle.$$

Now,

$$p_{e,m|0} = \sum_{\phi_1,\ldots,\phi_k} p_{e,m|0,\phi_1,\ldots,\phi_k} \prod_{j\neq m+1} p(\phi_j)$$

$$= \sum_{\phi_1,\ldots,\phi_k} p_{e,m|0,\phi_1,\ldots,\phi_k} 2^{-(k-1)}$$

$$= \sum_{\phi_1,\ldots,\phi_k} \langle M_-|M_-\rangle 2^{-(k-1)}$$

$$= \frac{1}{4N}\sum_{n\neq m,m+1} \big||E_{n,m}\rangle - |E_{n,m+1}\rangle\big|^2 + \big|(|E_{m,m}\rangle - |E_{m+1,m+1}\rangle) + (|E_{m+1,m}\rangle - |E_{m,m+1}\rangle)\big|^2.$$

The exact same argument leads to

$$p_{e,m|1} = \frac{1}{4N}\sum_{n\neq m,m+1} \big||E_{n,m}\rangle - |E_{n,m+1}\rangle\big|^2 + \big|(|E_{m,m}\rangle - |E_{m+1,m+1}\rangle) - (|E_{m+1,m}\rangle - |E_{m,m+1}\rangle)\big|^2.$$

Using the above two expressions we have

$$p_{e,m} = \frac{1}{2}\left[p(m) - \frac{1}{N}(\langle E_{m,m}|E_{m+1,m+1}\rangle + \langle E_{m+1,m}|E_{m,m+1}\rangle)\right].$$

Dividing the above expression by $p(m)$ directly leads to the expression in Eq. (20).

APPENDIX C: EXPRESSION FOR COLLISION PROBABILITY

Here we derive the expression in Eq. (25). We start with the expression in Eq. (15). Using the same definition for $E_{\phi_1\ldots\phi_k}[A]$ that we did in Appendix B, we have

$$p(z,m|0) = \frac{1}{4N}E_{\phi_1,\ldots,\phi_k}[|(\langle z|J_m\rangle + \langle z|J_{m+1}\rangle)|0_m\rangle + (\langle z|J_m\rangle - \langle z|J_{m+1}\rangle)|1_m\rangle|^2]$$

$$= \frac{1}{4N}\left[(E_{m,m}(z) + E_{m+1,m}(z))^2 + [E_{m,m+1}(z) + E_{m+1,m+1(z)}]^2 + \sum_{n\neq m,m+1} E_{n,m}^2 + E_{n,m+1}^2\right).$$

Similarly we can derive

$$p(z,m|1) = \frac{1}{4N}\left[[E_{m,m}(z) - E_{m+1,m}]^2 + [E_{m,m+1}(z) - E_{m+1,m+1}]^2 + \sum_{n\neq m,m+1} E_{n,m}^2 + E_{n,m+1}^2\right].$$

Using the fact that $p(z,m)=[p(z,m|0)+p(z,m|1)]/2$, and plugging the above two expressions into Eq. (15) directly leads to the expression given in Eq. (25).

APPENDIX D: UPPER BOUND ON COLLISION PROBABILITY

We start with Eq. (25), and use the form of the Cauchy inequality which was first proposed by Lutkenhaus for the bound on the collision probability in BB84 (see Appendix A of [11]). Specifically if $\psi(z)=\langle z|\psi\rangle$ and $\phi(z)=\langle z|\phi\rangle$, then the Cauchy inequality tells us that

$$\sum_z \frac{\psi^2(z)\phi^2(z)}{A_m^2(z) + A_{m+1}^2(z) + B_m^2(z) + B_{m+1}^2(z) + C_m^2(z) + C_{m+1}^2(z)} \geqslant \frac{\langle\phi|\psi\rangle}{2p(m)}. \tag{D1}$$

We expand the product terms in Eq. (25), and apply the above bound. Also, we can assume that $|A_m\rangle$ and $|C_{m+1}\rangle$ are orthogonal to all other vectors, because this maximizes the collision probability without affecting the error rate. This leads directly to the expression given in Eq. (31).

APPENDIX E: SYMMETRIZATION OF COLLISION PROBABILITY

We have so far shown that the collision probability and error rate depend on the interference between state vectors at times m and $m+1$. This means that our optimization problem has a symmetry of circular permutation. Specifically, if we apply the following transformation:

$$|A_m\rangle \rightarrow |A_{m+1 \bmod k}\rangle,$$

$$|B_m\rangle \rightarrow |B_{m+1 \bmod k}\rangle,$$

$$|C_m\rangle \rightarrow |C_{m+1 \bmod k}\rangle,$$

we do not affect the error rate or Eve's collision probability. Now, let us suppose that an optimal attack exists which is

given by the state vectors $|A_m\rangle$, $|B_m\rangle$, and $|C_m\rangle$. We can form a new set of state vectors $|A'_m\rangle$, $|B'_m\rangle$, and $|C'_m\rangle$ as follows:

$$|A'_m\rangle = \frac{1}{\sqrt{k}}\sum_{j=0}^{k-1} |A_{m+j \bmod k}\rangle j,$$

$$|B'_m\rangle = \frac{1}{\sqrt{k}}\sum_{j=0}^{k-1} |B_{m+j \bmod k}\rangle j,$$

$$|C'_m\rangle = \frac{1}{\sqrt{k}}\sum_{j=0}^{k-1} |C_{m+j \bmod k}\rangle j.$$

In the above equations, $|j\rangle$ represent an orthogonal basis which keeps track of which circular permutation has been chosen. The collision probability can now be written as

$$P_{c0} = \sum_{x,z,m,j} p^2(x|z,m,j)p(z,m,j)$$

$$= \sum_j p(j) \sum_{x,z,m} p^2(x|z,m,j)p(z,m|j)$$

$$= \sum_j p(j) P_{c0|j}.$$

The expression $P_{c0|j}$ is simply the average collision probability given the value of the measurement on the states $|j\rangle$. However, because the different values of j represent different circular permutations and the collision probability is invariant under circular permutation, we have $P_{c0|j}=P_{c0}$. Thus, the symmetrized probes $|A'_m\rangle$, $|B'_m\rangle$, and $|C'_m\rangle$ have the same collision probability as the unsymmetrized ones. It is easy to verify that these symmetrized probes satisfy the property that their inner products with each other is independent of m.

APPENDIX F: OPTIMIZATION OF THE COLLISION PROBABILITY

We define $a=\langle A_0|A_0\rangle=\langle A_1|A_1\rangle$, $b=\langle B_0|B_0\rangle=\langle B_1|B_1\rangle$, and $c=\langle C_0|C_0\rangle=\langle C_1|C_1\rangle$. Normalization imposes the constraint $a+b+c=1$. We define the angles ϕ_1 and ϕ_2 as

$$\langle B_1|B_0\rangle = b\cos\phi_1,$$

$$\langle A_1|C_0\rangle = \sqrt{ac}\cos\phi 2.$$

Straightforward manipulation of the bound on P_{c0} leads to the expression

$$P_{c0} \leqslant 1 - \tfrac{1}{8}\{a^2 + c^2 + (b-c)^2 + (b-a)^2 + 2[b\cos\phi_1 - \sqrt{(ac)}\cos\phi_2]\}.$$

We also use the fact that

$$(b\cos\phi_1 - \sqrt{ac}\cos\phi_2) = (1-2e)^2 - 4b\sqrt{ac}\cos\phi_1\cos\phi_2.$$

Using the above expression, it is easy to show that the collision probability is maximized and the error rate is minimized when $\cos\phi_1=\cos\phi_2=1$.

Now we set

$$a = (1-b)\cos\theta,$$

$$c = (1-b)\sin\theta.$$

Plugging into the expression for the collision probability, it is straightforward to show that the collision probability achieves a maximum when $\theta=\pi/4$, and that this condition also minimizes the error rate. Thus, the optimal attack strategy occurs when $a=c$. This condition implies that

$$e = \frac{x}{2},$$

$$P_{c0} \leqslant 1 - \tfrac{1}{4}[x^2 + 2(1-3x)^2].$$

Substituting the expression for e into P_{c0} directly leads to the expression in Eq. (34).

[1] C. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[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] M. Koashi and N. Imoto, Phys. Rev. Lett. **79**, 2383 (1997).
[6] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[7] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[8] D. Mayers, J. Am. Chem. Soc. **48**, 351 (2001).
[9] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[10] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).
[11] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
[12] C. A. Fuchs, N. Gisin, R. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[13] B. A. Slutsky, R. Rao, P. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).
[14] K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. A **67**, 032310 (2003).
[15] C. Bennett, G. Brassard, C. Crpeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[16] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).
[17] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[18] C. Langrock *et al.*, Opt. Lett. **30**, 1725 (2005).
[19] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. Fejer, K. Inoue, and Y. Yamamoto, e-print quant-ph/0507110.