Security of quantum key distribution with entangled photons against individual attacks

Edo Waks, Assaf Zeevi, and Yoshihisa Yamamoto*
Quantum Entanglement Project, ICORP, JST, E.L. Ginzton Laboratory, Stanford University, Stanford, California 94305
(Received 10 January 2001; revised manuscript received 20 September 2001; published 25 April 2002)

We investigate the security of quantum key distribution with entangled photons, focusing on the two-photon variation of the Bennett-Brassard 1984 (BB84) protocol proposed in 1992 by Bennett, Brasard, and Mermin (BBM92). We present a proof of security which applies to realistic sources, and to untrustable sources which can be placed outside the labs of the two receivers. The proof is restricted to individual eavesdropping attacks, and assumes that the detection apparatus is trustable. We find that the average collision probability for the BBM92 protocol is the same as that of the BB84 protocol with an ideal single-photon source. This indicates that there is no analog in BBM92 to photon splitting attacks, and that the source can be placed between the two receivers without changing the form of the collision probability. We then compare the communication rate of both protocols as a function of distance, and show that BBM92 has potential for much longer communication distances, up to 170 km, in the presence of realistic experimental imperfections. Finally, we propose a scheme based on entanglement swapping that can lead to even longer distance communication. The limiting factor in this scheme is the channel loss, which imposes very slow communication rates at longer distances.

DOI: 10.1103/PhysRevA.65.052310 PACS number(s): 03.67.Dd, 03.65.Ud, 03.67.−a

I. INTRODUCTION

The field of quantum-information theory has brought the potential to accomplish feats considered impossible by purely classical methods. One of these is the ability to transmit an unconditionally secure message between two parties, known as quantum cryptography. The first full protocol for quantum cryptography was proposed in 1984 by Bennett and Brassard using four nonorthogonal states of a quantum system [1], and has since been known as BB84. Following the discovery of the BB84 protocol, other protocols based on nonorthogonal quantum states have been proposed [2,3]. The security of all of these protocols relies on the impossibility of measuring the wave function of a quantum system without imposing a backaction on the state. This backaction will usually result in an increase in errors across the communication channel.

In 1991 it was proposed by Ekert that quantum key distribution could also be implemented using entanglement between quantum systems [4]. Two entangled quantum systems cannot lead to violations of Bell's inequality if they are also correlated to a local variable, which an eavesdropper can observe. A test of Bell's inequality could then provide a statement of security against eavesdropping. The idea of using entangled photons for quantum cryptography was extended by Bennett, Brassard, and Mermin [5] to the two-photon variant of BB84. In this protocol, which we refer to as BBM92, both receivers measure their respective photons randomly in two non-orthogonal bases. An eavesdropper cannot maintain perfect correlations simultaneously in those two incompatible bases while still learning information about the measurement results.

The experimental effort to perform quantum key distribution evolved simultaneously as the theory was being formed. Several groups reported implementations of the BB84 protocol and other single-photon schemes [6–10]. Long distance violations of Bell's inequality have been demonstrated in [11], and recently several proof-of-principle experiments using entangled photons have also been performed [12–14]. Any practical systems which implement quantum key distribution have a baseline error rate which cannot be distinguished from tampering. A complete analysis of such systems must relate this finite error rate to the security of the transmission. Furthermore, practical systems handle errors by public discussion through two additional steps, error correction and privacy amplification. The error correction step serves the dual purpose of correcting all erroneously received bits and giving an estimate of the error rate. Privacy amplification is then used to distill a shorter key which can be made as secure as desired. A security analysis should consider the effect of these two steps.

The security of quantum key distribution is a complex subject with several open questions still remaining. Most theoretical studies of security have dealt with the BB84 protocol. Early work showed security against several restricted types of attacks [15,16]. Later, security was proved for the most general individual attacks [17–19], and these proofs were extended to practical photon sources in [20]. In an individual attack the eavesdropper is restricted to measuring each quantum transmission independently, but is allowed to use any measurement which is not forbidden by quantum mechanics. A more general attack allows collective measurements which make use of the correlations introduced during error correction and privacy amplification by exchange of block parties. This information can be used to refine an eavesdropper's quantum measurement. Security against these more general attacks has been shown in [21]. The most general type of attack is known as a joint attack where the eavesdropper treats the entire quantum transmission as one system which she entangles with a probe of very large dimensional-

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

ity. There are currently several proofs of security against this most general scenario [22–24].

Entangled photon protocols have not been studied as thoroughly as the BB84 protocol. Several proofs of security exist for entanglement-based protocols against enemies with unlimited computational power. Some of these proofs require that the receivers process their qubits through some form of quantum computer [25,26]. Others apply to more standard entangled photon protocols but require that the source generate only one photon for each receiver [27]. Although these proofs represent important progress in the security of entangled photon protocols, they cannot yet be used directly to analyze the security of practical systems.

In order to treat practical entangled photon systems a proof of security must be extended to realistic sources. Furthermore, in most of these systems the source can be located in between the two receivers and is not trustable. An eavesdropper can replace it with a different source that may provide more information without changing the error rate. In the worst case one must also consider the detection apparatus to be untrustable, so that an eavesdropper can in some way modify the measurements made by the two communicating parties. The issue of untrustable source and detection apparatus has previously been investigated by Mayers and Yao [28,29]. Mayers and Yao present a protocol in which two receiving parties measure their respective signals randomly in one of three nonorthogonal bases. It is proven that if the probabilities of the measurement results are consistent with those produced by a Bell state, then the security of the communication channel is ensured. An eavesdropper cannot simulate these probabilities while learning a non-negligible amount of information about the secret key, even if she is allowed to modify or control all aspects of the source and detection apparatus (i.e., number of particles per pulse, measurement bases, losses). This proof has the potential to guarantee security for realistic systems with virtually no assumptions. However, at this point the proof considers only the idealized limit where the probabilities are perfect, so it cannot be applied to practical systems either. The extension of this proof to imperfect probabilities due to effects such as imperfect state preparation and channel losses remains an important but difficult question.

In this paper we provide a proof of security for an entangled photon protocol which can be applied to practical systems. This is done by extending the proof of Lütkenhaus for the BB84 protocol with realistic sources [20] to apply to BBM92, the EPR variant of the BB84 protocol. The proof of security relies on two assumptions. The first is that all eavesdropping is restricted to individual attacks. The second assumption is that the detection apparatus is trustable. This means that we consider a specific model for the behavior of the detection apparatus, which includes losses, and assume that the eavesdropper cannot modify the measurement apparatus beyond this model. With these restrictions, we find a quantitative relationship between the security of the final key and experimentally measurable quantities such as the error rate. This is achieved by finding an upper bound on the average collision probability, which is an important quantity in the analysis of privacy amplification. The proof works for realistic sources, and allows the source to be placed outside the labs of the two receivers. Although our proof makes assumptions about the eavesdropper and the detection units, we believe these assumptions to be realistic under many experimental conditions. Because the technology to perform collective and joint measurements does not exist, and may not for quite some time, the assumption of individual attacks is realistic for current systems. The assumption that the measurement apparatus is reliable may also be argued as reasonable because the measurement systems are located in the labs of the receivers. They can therefore be tested to make sure they are operating according to expectation, and cannot be physically manipulated by the eavesdropper. This is in contrast to the source which is located somewhere between the two receivers and can easily be modified.

Deriving a bound on the collision probability allows us to make several interesting quantitative observations about the BBM92 protocol. We show that the collision probability for this protocol is the same as BB84 with an ideal single photon source. This has two interesting implications. First, there is no analog in BBM92 to the photon splitting attacks which can be a severe security risk for the BB84 protocol. Second, there is no advantage to keeping the source in the labs of one of the receivers. The source can be put in between the two receivers without changing the form of the collision probability. We then show that there is actually a big advantage to putting the source midway between the two receivers. Such a configuration is significantly more robust in the presence of optical losses and detector dark counts, which leads potentially to much longer communication distances. Since the proof applies to any source of entangled photons we can extend our analysis to more sophisticated methods of generating entangled pairs, such as those based on entanglement swapping. In the final section we analyze a system based on a series of entanglement swaps using only linear optics. We show that this system can be even less sensitive to detector dark counts and channel losses, which may lead to even longer communication distances. The limiting factor in this scheme is the channel loss which imposes unreasonably slow communication rates at longer distances.

In Sec. II, we describe the BBM92 protocol and review the general theory behind quantum key distribution. We restate some important information theoretic results on error correction, and privacy amplification. We then derive a method for handling the side information leaked during error correction. This method allows us to account for the effect of error correction on the length of the final key. In Sec. III, we derive a proof of security for the BBM92 protocol, and use it to calculate expected communication rates under practical experimental conditions. These rates are compared to the BB84 protocol with ideal and Poissonian sources. Finally, in Sec. IV, we investigate an experimental configuration based on entanglement swapping, which can be more robust to channel loss and detector dark counts.

II. PRELIMINARIES

In this section we provide a review of important concepts in quantum key distribution (QKD). We also derive some

preliminary results which we will use in the upcoming sections. The standard participants in QKD are Alice, Bob, and Eve. Alice would like to exchange a secret key with Bob, which can later be used to encode the actual message. To do this she uses both a quantum channel and a public channel. The enemy, Eve, can listen in on the public channel, but is assumed incapable of altering the messages being exchanged. Eve is also allowed to make any measurements she can on the quantum channel.

The secret key is formed in three steps. The first is the raw quantum transmission, which uses both the quantum and public channel simultaneously. The next two steps, error correction and privacy amplification, make use of only the public channel. After privacy amplification Alice and Bob each possess a copy of the secret key, about which Eve knows only a negligibly small amount of information.

A. Quantum transmission

In the BBM92 protocol Alice and Bob share a pair of photons from a source presumed to be somewhere in between both parties. In the ideal case the photon pair is in a quantum-mechanically entangled state such as

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|xx\rangle + |yy\rangle), \tag{1}$$

where x and y are two orthoganol states of the photon wave function. For definiteness we assume that x and y are polarization states, but alternate implementations can usually be treated in a completely analogous way. The above state implies that if both receivers measure their photon in the x-y basis, their measurement results will be completely correlated. However, we can define the alternate basis

$$|u\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle),$$

$$|v\rangle = \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle).$$

Using this basis one can rewrite the above state in the equivalent form

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|uu\rangle + |vv\rangle). \tag{2}$$

Thus, if both receivers choose to measure in the u-v instead of the x-y basis their measurement results will remain correlated. In BBM92 each receiver measures their respective photon randomly in either the x-y or u-v basis. Later they agree to keep only the instances in which the measurement bases were the same, forming the ''sifted'' key.

B. Error correction

In any realistic communication system errors are bound to occur, and some form of error correction is required. In quantum cryptography the errors typically arise from technological imperfections in the optics and detectors, but can also come from eavesdropping. In order to achieve noise-free communication these errors must be corrected, and this can be done through public discussion.

Following the raw quantum transmission Alice, Bob, and Eve each possess the strings X, Y, and Z, respectively. In order to correct the errors, Alice and Bob exchange an additional message U such that knowledge of string Y and U leave very little uncertainty about string X. One way to mathematically express this is to use the Shannon entropy function [30]

$$H(X) = -\sum_x p(x)\log_2 p(x). \tag{3}$$

The conditional entropy function $H(X|Y=y)$ is defined as above using the conditional probability distribution $p(x|Y=y)$. The average conditional entropy $H(X|Y)$ is simply defined as

$$H(X|Y) = \sum_y p(y)H(X|Y=y). \tag{4}$$

The message U should provide Bob with enough information so that $H(X|YU)\approx 0$. Since string U is publicly disclosed, Eve may learn additional information as well, but good error correction algorithm will reduce this information leakage to a minimum. Unfortunately, given the error rate e, a lower bound exists on the minimum number of bits in U. This limit, which is a variant of the Shannon noiseless coding theorem can be stated as

$$\lim_{n\to\infty}\frac{\kappa}{n} \geqslant h(e), \tag{5}$$

where n is the length of the string, κ is the number of bits in message U, and $h(e)$ is the conditional entropy of a single bit over a binary symmetric channel which is given by

$$h(e) = -e\log_2 e - (1-e)\log_2(1-e). \tag{6}$$

An error correction algorithm should ideally operate very close to this limit. At the same time the algorithm should be computationally efficient or the execution time may become prohibitively long.

Error correction algorithms can usually be divided into two classes, unidirectional and bidirectional. In a unidirectional algorithm information flows only from Alice to Bob. Alice provides Bob with an additional string U which he then uses to try to find his errors. This makes it difficult to design algorithms which are both computationally efficient and operate near the Shannon limit [19,31]. In a bidirectional algorithm information can flow both ways, and Alice can use the feedback from Bob to determine what additional information she should provide him. This makes it easier to approach the Shannon limit. These two classes can be further subdivided into two subclasses, one for algorithms which discard errors and one for those which correct them. Discarding errors is usually done in order to prevent additional side

information from leaking to Eve. By correcting the errors one allows for this additional flow of side information, which can be accounted for during privacy amplification. Since privacy amplification is typically a very efficient process, algorithms which correct the errors tends to perform better.

Although our proof of security is independent of the type of error correction which is done, the communication rate in QKD strongly depends on this. For our calculations we will work with the algorithm given in [31], which is bidirectional and corrects the errors. This algorithm works within about 15–35% of the Shannon limit, even with rather substantial error rates.

C. Privacy amplification

After error correction, Alice and Bob share an error-free string X. Eve has also potentially obtained at least partial information about this string from attacks on the raw quantum transmission and side information leaked during error correction. Thus, X cannot by itself be used as a key. However, through the method of generalized privacy amplification [32], the string X can be compressed to a shorter string K over which any eavesdropper has only a negligible amount of information. The amount of compression needed depends on how much information may have been compromised during the previous phases of the transmission.

To do privacy amplification Alice picks a function g out of a universal class of functions $\mathcal{G}$ which map all n bit strings to r bit strings where $r<n$ (see [32] for more details). Once g has been picked and publicly announced both parties calculate the string $K=g(X)$, which serves as the final key. This key is considered secure if Eve's mutual information on K, defined as [30]

$$I_E(K;GV)=H(K)-H(K|GV), \tag{7}$$

is negligibly small, where G is the random variable corresponding to the choice of function g and V is all the information available to Eve.

An important quantity in the analysis of privacy amplification is the collision probability defined as

$$P_c(X)=\sum_x p^2(x). \tag{8}$$

One can show that the conditional entropy $H(K|G)$ is bounded by ([32] theorem 3)

$$H(K|G)\geqslant r-\frac{2^r}{\ln 2}P_c(X). \tag{9}$$

This theorem can be applied to conditional distributions as well, which leads to

$$H(K|G,Z=z)\geqslant r-\frac{2^r}{\ln 2}P_c(X|Z=z), \tag{10}$$

where $P_c(X|Z=z)$ is just the collision probability of the distribution $p(x|Z=z)$. By averaging both sides of the above equation we get

$$H(K|GZ)\geqslant r-\frac{2^r}{\ln 2}\langle P_c(X|Z=z)\rangle_z, \tag{11}$$

where

$$\langle P_c(X|Z=z)\rangle_z=\sum_z p(z)P_c(X|Z=z) \tag{12}$$

is the average collision probability. This is a quantity of central importance in privacy amplification. In the case of individual attacks, the ith bit in Z depends only on the ith bit in X. Under these circumstances the average collision probability factors into the product of the average collision probability of each bit. Thus,

$$\langle P_c(X|Z=z)\rangle_z=(p_c)^n, \tag{13}$$

where n is the number of bits in string X and

$$p_c=\sum_{\alpha=0,1}\sum_{\beta=1}^{k}\frac{p^2(\alpha,\beta)}{p(\beta)}. \tag{14}$$

In the above expression α sums over the possible values of a single bit in Alice's string and β sums over the possible measurement outcomes of the probe, which are enumerated from 1 to k. Suppose that we are able to come up with a bound of the form $-\log_2\langle P_c(X|Z=z)\rangle_z\geqslant c$. If we set $r=c-s$, where s is a security parameter chosen by Alice and Bob, then Eq. (11) leads to

$$I_E(X;Z)\leqslant 2^{-s}/\ln 2. \tag{15}$$

Thus, a bound on the average collision probability allows the two parties to make Eve's mutual information exponentially small in s.

D. Handling side information from error correction

If the only information available to Eve comes from string Z, which is obtained from attacks on the quantum transmission, then the discussion in the previous section is sufficient. But if Alice and Bob do error corrections Eve will also learn an additional string U which gives her more information about Alice's key. This side information must also be included in the calculation. We can apply the bound in Eq. (9) to the conditional distribution $p(x|U=u,Z=z)$, which leads to

$$H(K|G,U=u,Z=z)\geqslant r-\frac{2^r}{\ln 2}P_c(X|U=u,Z=z). \tag{17}$$

We can then try to average both sides of the above expression but doing this introduces additional complications. The random variable U introduces correlations between different bits in strings X and Z. Because of this the average collision probability no longer factors into the product of individual bits, as in Eq. (13). This makes the problem of finding a bound on the average collision probability significantly more difficult. This problem has been previously investigated in

[33], where several bounds on the collision probability $P_c(X|Z=z,U=u)$ were derived as a function of $P_c(X|Z=z)$. The extension of this work to the average collision probability involves a few subtleties, which we deal with in Appendix A. In this appendix we show that if we set

$$r = n\tau - \kappa - t - s, \tag{18}$$

where

$$\tau = -\log_2 p_c, \tag{19}$$

κ is the number of bits in message U, n is the length of the error corrected key, and both s and t are security parameters chosen by Alice and Bob, then

$$I_E \leqslant 2^{-t} r + \frac{2^{-s}}{\ln 2}. \tag{20}$$

This bound on Eve's information is still exponentially small in the security parameters, and only involves the collision probability averaged over her measurements on the quantum transmission.

III. SECURITY OF THE BBM92 PROTOCOL

In this section we give a proof of security for the BBM92 protocol. As shown in the previous section, this involves finding an upper bound on p_c given in Eq. (14) using the laws of quantum mechanics. We then calculate the communication rate in the presence of detector dark counts and channel losses for both an ideal source which creates exactly one entangled pair per clock cycle, as well as a more practical source based on parametric down conversion.

A. Proof of security against individual attacks

In the BBM92 protocol Alice, Bob, and Eve observe orthogonal Hilbert spaces H_A, H_B, and H_E respectively. In the most general case Eve can control which density matrix ρ_{abe} over the space $H_A \otimes H_B \otimes H_E$ she will share with Alice and Bob. This density matrix can span all the photon number states of the two receivers, and Eve's measurable subspace which can have any number of dimensions. In practice Eve can do this by blocking out the original source and substituting her own source which generates the desired state that maximizes her information on the final key. We derive a bound on the optimal density matrix, which serves as an upper bound, even if Eve is incapable of generating it in practice.

As mentioned previously, our proof assumes that Eve is restricted to individual attacks and that Alice and Bob's detection apparatus is trustable. A trustable detection apparatus is one whose components behave according to a known model which cannot be modified by Eve. In order to define this model we first have to specify the physical implementation of the detection apparatus, which is shown in Fig. 1. In this detection scheme, a 50/50 beam splitter modulates the measurement basis by partitioning the photons and sending them into one of the two polarizing beam splitters. This modulation technique is known as passive modulation, as opposed to active modulation where the measurement basis for each receiver is switched using a rapid phase modulator. We work with a passive modulation scheme because it simplifies the proof of security and is easier to implement in practice.

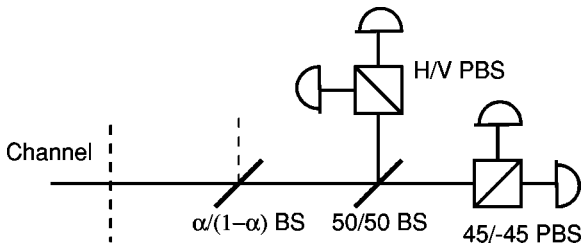

FIG. 1. Detection unit used by Alice and Bob.

In order to account for optical losses we place a beam splitter in front of the detection apparatus which reflects off a specified fraction of the light into a loss mode. All losses are lumped into this beam splitter and the subsequent optical components can be regarded as lossless. This model is realistic under two conditions. First, the use of a beam-splitter model is valid if the loss is linear. A linear beam splitter cannot effectively model loss due to nonlinear effects such as two-photon absorption. To incorporate such effects a more complicated loss model is required. However, in real system multiphoton absorption is typically many orders of magnitude weaker than linear absorption, so a beam-splitter approximation is extremely good. Second, placing the beam splitter in front of the detection apparatus requires that the losses to each detector are equal. This is an important point in passive modulation. A passive modulation scheme must be constructed in such a way that a photon has the same probability of being detected regardless of which path it takes. If, for example, one detector has higher quantum efficiency than the other three, additional loss should be placed in front of it to make sure that the above property is satisfied.

Having modeled the loss, we can now define the operation of the lossless components. For each detection unit we define $E^{(0)}$ as the projector onto vacuum and E^n_ψ as the projector onto the state which has n photons with polarization ψ, where $\psi \in \{x,y,u,v\}$. The detection apparatus performs a positive operator valued measurement (POVM) whose elements corresponds to different combinations of detection events from four photon counters. The elements of this POVM can be broken up into F_{vac}, F_ψ, and F_D which correspond to no detections, one detection corresponding to polarization ψ, and more than one detection, respectively. These operators are given by [19]

$$F_{vac} = E^0, \tag{21}$$

$$F_\psi = \sum_{n=1}^{\infty} \left(\frac{1}{2}\right)^n E^n_\psi, \tag{22}$$

$$F_D = \sum_{n=2}^{\infty} \left\{ \left[\frac{1}{2} - \left(\frac{1}{2}\right)^n\right] \sum_\psi E^n_\psi \right\} + \frac{1}{2} \sum_{n,m=1}^{\infty} E^n_x E^m_y + E^n_u E^m_v. \tag{23}$$

Multiple detection events, corresponding to the operator F_D, are possible if more than one photon is incident on the detection apparatus. These events should not be discarded, because keeping track of them can prevent certain security loopholes. By incorporating the multiple detection events in the proof of security for the BB84 protocol, one can make it disadvantageous for Eve to add additional photons to Alice's signal [19]. We will show that monitoring these events can also significantly simplify the proof of security for the BBM92 protocol. In order to incorporate multiple detection events into the proof of security we will use the disturbance parameter ϵ introduced in [19]. This parameter is given by

$$\epsilon = \frac{n_{err} + w_D n_D}{n_{rec}} \tag{24}$$

where n_{err}, n_D, and n_{rec} are the number of error bits, dual fire events, and number of bits that entered the error-corrected key, respectively, and w_D is a weighting parameter chosen by Alice and Bob. As part of the proof we will show that $w_D = 1/2$ is a sufficient number to ensure security for the BBM92 protocol, just as it was for BB84 [19]. Note that in the limit that the dual fire rates are negligibly small the disturbance parameter simplifies to the bit error rate.

Eve is allowed to pick any density matrix ρ_{abe} which represents some entangled state of her observable Hilbert space and the signals transmitted to Alice and Bob. She can send any number of photons she wishes, or a coherent superposition of photon numbers. Our first step is to show that the most general density matrix ρ_{abe} can be written as

$$\rho_{abe} = \sum_{i,j=1}^{\infty} \rho_{abe}^{(ij)}, \tag{25}$$

where $\rho_{abe}^{(ij)}$ is the density operator over the subspace where Alice received i photons and Bob received j photons. This is due to the fact that the detection units consist of only passive linear optics with vacuum auxiliary modes and single-photon counters. As can be seen by Eqs. (21)–(23), a detection event is represented by a projection operator which is diagonal in the photon number basis. We define E_a^i as the projector onto Alice's i photon subspace, and E_b^j as the projector onto Bob's j photon subspace. Suppose that F_a and F_b are positive operators which represent a measurement corresponding to any combination of detection events for Alice and Bob, respectively. Because these operators are diagonal in the photon number basis they can be written equivalently as

$$F_a = \sum_i E_a^i F_a^i E_a^i, \tag{26}$$

$$F_b = \sum_j E_b^j F_b^j E_b^j. \tag{27}$$

Let F_e be the positive operator corresponding to Eve's measurement result on her own subspace. The joint probability $p(a,b,e)$ can be written as

$$\begin{aligned} p(a,b,e) &= \mathrm{Tr}\{\rho_{abe} F_a F_b F_e\} \\ &= \sum_{ij} \mathrm{Tr}\{\rho_{abe} E_a^i E_b^j F_a F_b E_a^i E_b^j F_e\} \\ &= \sum_{ij} \mathrm{Tr}\{E_a^i E_b^j \rho_{abe} E_a^i E_b^j F_a F_b F_e\}. \end{aligned}$$

The last step comes from the fact that the projectors commute with Eve's measurement operator and the invariance of the trace under cyclic permutation. If we define $\rho_{abe}^{(ij)} = E_a^i E_b^j \rho_{abe} E_a^i E_b^j$ we see that the joint probability does not change if we select a density matrix of the form given in Eq. (25).

The main consequence of the above result is that Eve can keep track of the number of photons she is sending to Alice and Bob without changing the measurement results. Thus, her collision probability can be broken up into different photon number contributions as

$$p_c = \sum_{i,j=1}^{\infty} \frac{p_{rec}^{(ij)}}{p_{rec}} p_c^{(ij)}, \tag{28}$$

where

$$p_c^{(ij)} = \sum_{m \in M^{(ij)}, \psi} \frac{1}{p_{rec}^{(ij)}} \frac{p^2(\psi,m)}{p(m)}. \tag{29}$$

The set $M^{(ij)}$ is defined as the set of all measurement results on Eve's probe if she sent i photons to Alice and j to Bob, and $p_{rec}^{(ij)}$ is the probability that the signal component $\rho_{abe}^{(ij)}$ enters the error-corrected key. We can similarly define $p_{err}^{(ij)}$ and $p_D^{(ij)}$ as the probability that this signal component enters the sifted key as an error or causes a dual fire event, respectively. Using Eq. (24) we can break up the disturbance measure ϵ into different photon number contributions as

$$\epsilon = \sum_{ij} \frac{p_{rec}^{(ij)}}{p_{rec}} \frac{p_{err}^{(ij)} + w_D p_D^{(ij)}}{p_{rec}^{(ij)}} = \sum_{ij} \frac{p_{rec}^{(ij)}}{p_{rec}} \epsilon^{(ij)}. \tag{30}$$

Our next step is to investigate the term $p_c^{(11)}$ which is the component corresponding to Alice and Bob each receiving one photon. Instead of directly finding a bound on Eve's collision probability from this component, we show that any bounds derived for the BB84 protocol on single photon states can also be applied to BBM92 when Alice and Bob each receive one photon. In the BB84 protocol Alice sends a photon in one of four nonorthogonal states to Bob. Eve performs a measurement on the photon and the backaction noise on the state can be described by a complete positive mapping (CP map)

$$\rho_b = \sum_k A_k \rho_a A_k^\dagger \tag{31}$$

where ρ_a is the density matrix prepared by Alice, and ρ_b is the density matrix which Bob receives. The only restriction on the operators A_k is that they satisfy the condition

$$\sum_k A_k^\dagger A_k = I. \tag{32}$$

In the BBM92 protocol Alice does not directly send Bob a density matrix. In the ideal case where both receivers share a pure entangled pair, if Alice's measurement corresponds to the operator F_a she prepares Bob's density matrix in the state $F_a^T/\mathrm{Tr}\{F_a\}$. If one could show that, given Alice observes F_a, any eavesdropping strategy incorporated by Eve could once again be described by a CP map

$$\rho_b = \sum_k A_k \frac{F_a^T}{\mathrm{Tr}\{F_a\}} A_k^\dagger, \tag{33}$$

then this seemingly different situation is equivalent to the BB84 protocol attack. Unfortunately, in the BBM92 protocol there are many eavesdropping strategies which cannot be described by such a mathematical formalism. However, in Appendix B we show that there is always an optimal attack which can be described by a CP map. Thus, any bounds which have been derived for the BB84 protocol using a POVM formalism on single-photon states can be directly applied to BBM92 protocol when one photon is sent to each receiver. Several such bounds have already been derived [17–19]. Since we are interested in the average collision probability, and since we are assuming the use of a bidirectional error-correction algorithm which corrects rather than discards errors, we can use the bound derived by Lütkenhaus ([19], Appendix D). This bound is given by

$$p_c^{(11)} \leqslant \frac{1}{2} + 2\epsilon^{(11)} - 2(\epsilon^{(11)})^2. \tag{34}$$

In order to account for the components with more than one photon for either receiver we show in Appendix C that, if the weighting parameter w_D in Eq. (24) is set to 1/2, Eve's optimal strategy is to only send one photon to Alice and Bob. This argument follows the same line as that given for the BB84 protocol in [19]. Given that this is the optimal strategy one is led directly to the result

$$p_c \leqslant \tfrac{1}{2} + 2\epsilon - 2\epsilon^2, \tag{35}$$

which is exactly the same as the collision probability for the BB84 protocol using a single-photon source.

The above result highlights two important points. First, one does not have to confine the source to either Alice's or Bob's lab. Allowing Eve to have total control of the source does not effect the form of the collision probability. Second, there is no analog to the photon splitting attack for the BBM92 protocol since the collision probability bound was derived without assumptions on the source. The error rate and dual fire rate are sufficient to determine how much privacy amplification is necessary.

B. Ideal entangled photon source

In this section we will calculate the expected communication rate for an ideal entangled photon source. This source creates exactly one pair of photons per clock cycle, whose quantum state is given by

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}(|xx\rangle + |yy\rangle). \tag{36}$$

Although proposals for creating such a source exist [34], we do not know of any successful implementations of such proposals to date. Nevertheless, this simplified analysis will set the groundwork for the analysis of practical sources based on parametric down conversion.

When doing two-photon experiments one is interested in coincidence events where the two receivers simultaneously detect a photon. In all our calculations we will assume that the dual fire rate is negligibly small, thus the disturbance parameter simplifies to the error rate. The channel is assumed to be an exponentially decaying function of distance. Thus, the channel transmission T_F can be written as

$$T_F = 10^{-(\sigma L/10)}, \tag{37}$$

where σ is the loss coefficient. We combine all losses to each receiver from the channel, detectors, and optics into one beam splitter with transmission

$$\alpha_L = \eta T_F(L), \tag{38}$$

where η accounts for all distance independent losses in the system. We separate the coincidence probability into two parts, p_{true} is the probability of a true coincidence from a pair of entangled photons, and p_{false} is the probability of a false coincidence which, for an ideal source, can only occur from a photon and dark count or two dark counts. In the limit of negligible dual fire events we have

$$p_{coin} = p_{true} + p_{false}. \tag{39}$$

We need to decide where to put the source. Setting the source a distance x from Alice and $L-x$ from Bob we have

$$p_{true} = \alpha_x \alpha_{L-x} = \eta \alpha_L,$$

and

$$p_{false} = 4\alpha_x d + 4\alpha_{L-x} d + 16 d^2, \tag{40}$$

keeping only terms which are second order in α_x and d. It can be seen that the probability of a true coincidence does not change with x, but the false coincidence rate does. A simple optimization shows that the false coincidence rate achieves a minimum halfway between Alice and Bob, which is given by

$$p_{false} = 8\alpha_{L/2} d + 16 d^2. \tag{41}$$

We define n_{tot} as the total number of signal pulses sent to the receivers, and n_{rec} as the length of the error corrected key. Thus,

TABLE I. Benchmark performance of error correction algorithm.

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

$$n_{rec}=\frac{n_{tot}p_{click}}{2}. \tag{42}$$

The error rate e is

$$e=\frac{p_{false}/2+\mu p_{true}}{p_{coin}}, \tag{43}$$

where μ is the baseline error rate of the signal. Using Eq. (18) we have

$$r=n_{rec}\left(\tau(e)-\frac{\kappa}{n_{rec}}\right)-t-s. \tag{44}$$

We define the asymptotic communication rate as

$$R=\lim_{n_{tot}\to\infty}\frac{r}{n_{tot}}. \tag{45}$$

In order to incorporate the effect of the error-correction algorithm we define the function $f(e)$ in the same way as was done in [20]. This function determines how far off from the Shannon limit the algorithm is performing. An algorithm can be tested to determine the value of $f(e)$. For example, the values given in Table I are for the error-correction algorithm given in [31]. Using this definition we have

$$\lim_{n_{rec}\to\infty}\frac{\kappa}{n_{rec}}=-f(e)[e\log_2(e)+(1-e)\log_2(1-e)]. \tag{46}$$

If we fix the value of Eve's information on the final key given by Eq. (20), then s is a constant and t varies roughly logarithmically with n_{tot}, so both terms drop out in the limit of large strings. This leads to an expression for the communication rate

$$R=\frac{p_{coin}}{2}\{\tau(e)+f(e)[e\log_2 e+(1-e)\log_2(1-e)]\}. \tag{47}$$

The values of p_{coin} and e can be calculated from Eqs. (39) and (43).

C. Entangled photons from parametric down conversion

A more practical way of generating entangled photons is to use the spontaneous emission of a nondegenerate parametric amplifier. This technique, known as parametric down conversion, is extensively used to generate entanglement in polarization as well as other degrees of freedom such as energy and momentum. Parametric amplifiers exploit the second-order nonlinearities of noncentrosymmetric materials. These nonlinearities couple three different modes of an electromagnetic field via the interaction Hamiltonian [35]

$$H_I=i\hbar\chi^{(2)}Ve^{i(\omega-\omega_a-\omega_b)t}\hat{a}^\dagger\hat{b}^\dagger+\mathrm{H.c.},$$

where modes a and b are treated quantum mechanically while the third mode $Ve^{i\omega t}$ is considered sufficiently strong to be treated classically. The state of the field after the nonlinear interaction is given by

$$|\psi\rangle=\exp\left[\frac{1}{i\hbar}\int_0^T H_I(t)dt\right]|0\rangle.$$

We assume the energy conservation condition, $\omega=\omega_a+\omega_b$, which leads directly to

$$|\psi\rangle=e^{\chi(\hat{a}^\dagger\hat{b}^\dagger-\hat{a}\hat{b})}|0\rangle,$$

where the parameter χ depends on several factors including the nonlinear coefficient $\chi^{(2)}$, the pump energy, and the interaction time. Using the operator identity [35]

$$e^{\chi(\hat{a}^\dagger\hat{b}^\dagger-\hat{a}\hat{b})}=e^{\Gamma\hat{a}^\dagger\hat{b}^\dagger}e^{-g(\hat{a}^\dagger\hat{a}+\hat{b}^\dagger\hat{b}+1)}e^{-\Gamma\hat{a}\hat{b}}, \tag{48}$$

where

$$\Gamma=\tanh\chi,$$

$$g=\ln\cosh\chi,$$

directly leads to the relation

$$|\psi\rangle=\frac{1}{\cosh\chi}\sum_{n=0}^{\infty}\tanh^n\chi|n\rangle_a|n\rangle_b. \tag{49}$$

The above equation makes it clear that whenever a photon is detected in one mode, the conjugate mode must also contain a photon. In order to generate entanglement in polarization one needs to create a correlation between the polarization of these two modes. This is typically done using noncollinear Type II phase matching [36], which leads to the slightly more complicated interaction

$$H_I=i\hbar\chi^{(2)}Ae^{i\omega t}(\hat{a}_x^\dagger\hat{b}_y^\dagger+\hat{a}_y^\dagger\hat{b}_x^\dagger)+\mathrm{H.c.},$$

where x and y refer to the polarization of the photon. Since all creation operators in the Hamiltonian commute, we can apply Eq. (48) to both mode pairs which directly leads to

$$|\psi\rangle=\frac{e^{\tanh\chi(\hat{a}_x^\dagger\hat{b}_y^\dagger+\hat{a}_y^\dagger\hat{b}_x^\dagger)}}{\cosh^2\chi}|0\rangle. \tag{50}$$

If χ is sufficiently small that the above expression can be kept only to first order then a parametric down converter creates a Bell state. But χ cannot be made small without sacrificing the rate of down conversion.

We want to calculate the probability p_{coin} and the error rate e as a function of the parameter χ, as well as the optical losses and dark counts of the detectors. We begin by defining the field operator

$$\hat{\psi}=\frac{e^{\tanh\chi(\hat{a}_x^\dagger\hat{b}_y^\dagger+\hat{a}_y^\dagger\hat{b}_x^\dagger)}}{\cosh^2\chi}. \tag{51}$$

The beam-splitter model that we have introduced previously to account for the losses becomes very useful here. The beam splitters perform a unitary operation on the modes which is given by

$$\hat{a}_\sigma\rightarrow\sqrt{\alpha_{L/2}}\hat{a}_\sigma+\sqrt{1-\alpha_{L/2}}\hat{c}_\sigma,$$

$$\hat{b}_\sigma\rightarrow\sqrt{\alpha_{L/2}}\hat{b}_\sigma+\sqrt{1-\alpha_{L/2}}\hat{d}_\sigma,$$

where σ represents polarization and the modes c and d are the reflected modes of the beam splitters. To determine the state of the photons after the loss we first apply this beam-splitter transformation. To simplify the notation we define another field operator

$$\psi_{\rho\phi}=\hat{\rho}_x^\dagger\hat{\phi}_y^\dagger+\hat{\rho}_y^\dagger\hat{\phi}_x^\dagger,$$

where ρ and ϕ are any two independent modes. Using this definition, Eq. (51) is transformed by the two beam splitters into

$$\hat{\psi}=\frac{1}{\cosh^2\chi}\exp[\tanh\chi(\alpha_{L/2}\psi_{ab}+\sqrt{\alpha_{L/2}(1-\alpha_{L/2})}\times(\psi_{ad}+\psi_{bc})+(1-\alpha_{L/2})\psi_{cd})].$$

We can expand this expression in terms of $\hat{a}^\dagger$ and $\hat{b}^\dagger$ as

$$\hat{\psi}=\frac{1}{\cosh^2\chi}\exp[\tanh\chi(1-\alpha_{L/2})\psi_{cd}]\times\{1+\tanh\chi\sqrt{\alpha_{L/2}(1-\alpha_{L/2})}[\psi_{ad}+\psi_{cd}]+\tanh\chi\psi_{ab}+\tanh^2\chi\alpha_{L/2}(1-\alpha_{L/2})\psi_{ab}\psi_{cd}+\psi_D\}$$

where ψ_D is the wave operator which contains all the terms that create more than one photon in either modes. It is now necessary to operate on the vacuum and trace out over modes c and d to get the final density matrix. As shown in Sec. III A we can ignore any off-diagonal terms that couple different photon number states because they do not contribute to the signal. We define the density-matrix ρ_{ψ_+} as the two-photon density matrix in which the photons are in the entangled state $|\psi_+\rangle$ given in Eq. (36). The matrices ρ_0^a and ρ_0^b represent a zero-photon vacuum state in mode a and b, respectively. Finally we define the matrices ρ_u^a and ρ_u^b as

$$\rho_u^{a,b}=\frac{I}{2}, \tag{52}$$

where I is the identity matrix. The above matrices correspond to an unpolarized photon in mode a or b, respectively. After tracing out loss modes c and d and ignoring the coherence between different photon number states, the density matrix becomes

$$\rho_{AB}=A\rho_{\psi_+}+B\rho_0^a\otimes\rho_0^b+C(\rho_u^a\otimes\rho_0^b+\rho_0^a\otimes\rho_u^b)+D\rho_u^a\otimes\rho_u^b+(1-A-B-2C-D)\rho_D, \tag{53}$$

where ρ_D is the matrix which represents all the possible states in which more than one photon is in either mode a and b after the losses. The coefficients A, B, C, and D are

$$A=\frac{1}{\cosh^4\chi}\frac{2\alpha_{L/2}^2\tanh^2\chi}{(1-\tanh^2\chi(1-\alpha_{L/2})^2)^4}, \tag{54}$$

$$B=\frac{1}{\cosh^4\chi}\frac{1}{(1-\tanh^2\chi(1-\alpha_{L/2})^2)^2}, \tag{55}$$

$$C=\frac{1}{\cosh^4\chi}\frac{2\alpha_{L/2}(1-\alpha_{L/2})\tanh^2\chi}{(1-\tanh^2\chi(1-\alpha_{L/2})^2)^3}, \tag{56}$$

$$D=\frac{1}{\cosh^4\chi}\frac{4\alpha_{L/2}^2(1-\alpha_{L/2})^2\tanh^4\chi}{(1-\tanh^2\chi(1-\alpha_{L/2})^2)^4}. \tag{57}$$

In the above expression, A is the probability that Alice and Bob share an entangled pair of photons. This component on the signal will be defined as a true coincidence, because it leads to error-free transmission. The coefficient B is then the probability that neither receiver gets a photon, either because the source failed to generate a pair or because all photons were lost. Similarly, C is the probability that one of the two receivers gets a photon but the other does not. In order for these signals to be factored into the key they must be accompanied by dark counts. Coefficient D is the probability that both receivers get a photon, but these photons are unpolarized and uncorrelated. Note that D is at least fourth order in $\tanh\chi$, indicating that at least two pairs must be created in order for it to exist. The intuitive explanation for the presence of this unpolarized component is that when higher-order number states are created, and some of these photons are lost, the loss modes c and d play a similar role to Eve. The photons in this mode can potentially carry some information about the quantum state of the other photons, and will thus result in decoherence. Since this component of the signal causes a 50% error, we can lump it into the definition of a false coincidence. Hence,

$$p_{true}=A,$$

$$p_{false}=16d^2B+8dC+D.$$

The communication rate can be calculated by simply plugging these expressions into Eqs. (39), (43), and (47).

D. Calculations

We now use the previously derived equation to calculate the rate of communication using the BBM92 protocol. We would also like to compare these rates to those of the BB84 protocol with ideal and realistic sources. The equations for

the communication rate of the BB84 protocol against individual attacks are given by [20]

$$R_{\mathrm{BB84}}=\frac{p_{click}}{2}\{\beta\tau(e/\beta)+f(e)[e\log_2 e+(1-e)\log_2(1-e)]\}. \tag{58}$$

The factor τ is again defined as Eq. (19). The parameter β accounts for the photon splitting attacks due to multiphoton states emitted by the source, and is given by

$$\beta=\frac{p_{click}-p_m}{p_{click}}. \tag{59}$$

In the above equation p_m is the probability the source emits a multiphoton state, and p_{click} is the probability that Bob detects a photon. For an ideal source $p_m=0$, while for a Poissonian light source it is given by

$$p_m=1-(1+\overline{n})e^{-\overline{n}}, \tag{60}$$

where $\overline{n}$ is the average number of photons per pulse. Bob's probability of detection can be broken up into a signal and dark count component as

$$p_{click}=p_{signal}+p_{dark}, \tag{61}$$

where we again ignore simultaneous signal and dark count events. These components are given by

$$p_{signal}=\alpha_L\overline{n} \tag{62}$$

$$p_{dark}=4d. \tag{63}$$

For an ideal source $\overline{n}=1$, but for a Poissonian source it becomes a free variable which should be optimized. Note that the loss coefficient in (62) is now α_L instead of $\alpha_{L/2}$. This is because in the BB84 protocol the photon starts in Alice's lab and must travel all the way to Bob, in contrast to the BBM92 protocol where the photons start half way in between. The error rate is given by

$$e=\frac{p_{dark}/2+\mu p_{signal}}{p_{click}}. \tag{64}$$

We perform simulations for fiber optical and free-space key distribution experiments. For the fiber-optical simulation we look at the 1.5 μm telecommunication window, while for free space communication we focus on the visible wavelengths where single-photon counters tend to perform best. In free space communication the channel loss is no longer an exponential function of distance. Instead, it is a complicated function which results from atmospheric effects, beam diffraction, and beam steering problems. Thus, for free space we are more interested in the rate as a function of the total loss rather than distance.

Figure 2 shows the calculation results for both BB84 and BBM92 protocols with ideal and realistic sources. In plot (a) of the figure we show results for fiber optical channels. Using experimental values from [10] we set the detector quantum efficiency to 0.18, $d=5\times10^{-5}$, and the channel loss $\sigma=0.2$ dB/km. We also set the baseline error rate $\mu=0.01$, and add an extra 1 dB of loss to account for losses in the receiver unit. The curves corresponding to the BBM92 protocol plot the distance from Alice to Bob, with the source assumed halfway in between. Plot (b) shows calculations for free space quantum key distribution. The communication rate is plotted as a function of the total loss, including the detector quantum efficiency. In the free-space curves for the BBM92 protocol we again put the source halfway between Alice and Bob and plot the rate as a function of the total loss in both arms. The dark counts of the detectors are set to 5×10^{-8}. In the curve for the BB84 protocol with a Poisson light source the average photon number $\overline{n}$ is a free adjustable parameter. Similarly with parametric down conversion we are free to adjust χ. For both cases we numerically optimize the communication rate at each point with respect to the adjustable parameter.

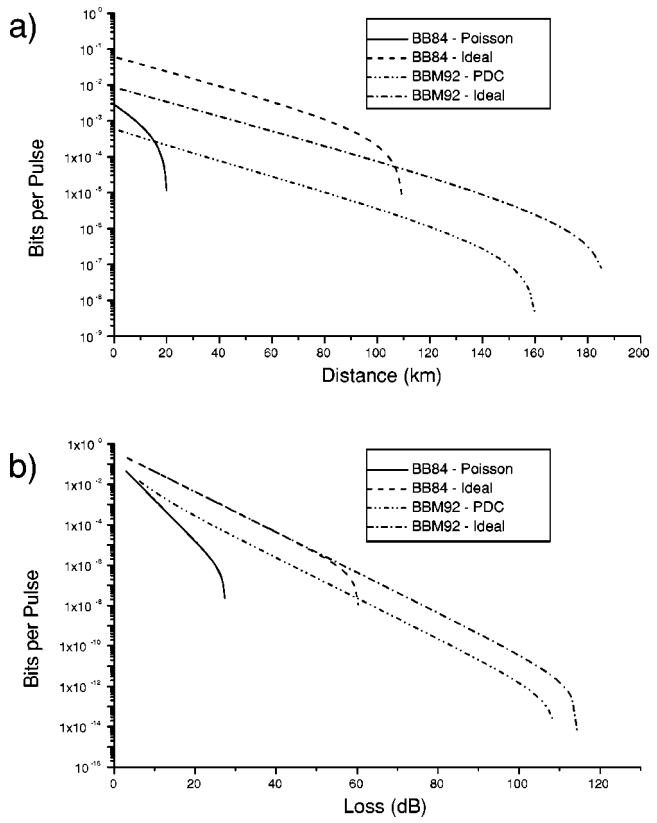

FIG. 2. Comparison of communication rate for the BB84 and BBM92 protocols. Plot (a) is for 1.5 μm fiber optical communication experiment. In this wavelength $\eta=0.18$, $d=5\times10^{-5}$, and the channel loss σ is set to 0.2 dB/km. For the Ekert protocol the distance is the total separation between Alice and Bob. Plot (b) shows calculated values for free-space quantum key distribution with visible photons. The rate is plotted as a function of the total loss, including detector quantum efficiency. The detectors are assumed to have a dark count rate of $d=5\times10^{-8}$. For the Ekert protocol the loss is the total loss in both arms.

Each curve features a cutoff distance where the communication rate quickly drops to zero. This cutoff is due to the dark counts, which begin to make a non-negligible contribu-

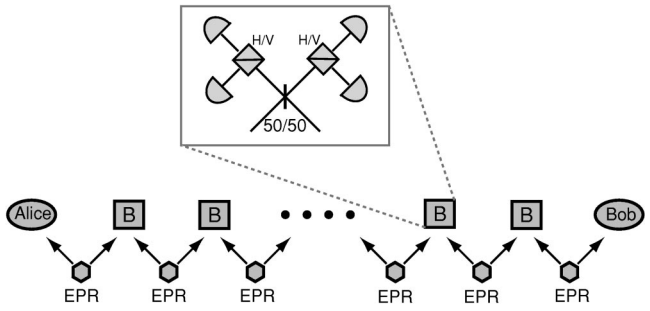

FIG. 3. Experimental setup for quantum key distribution with entanglement swaps.

tion to the signal at some point. However the two curves for BBM92 feature a much longer cutoff distance than their BB84 counterparts. This is due partially to the absence of the photon splitting attacks. But even when performing the BB84 protocol with ideal single-photon sources, which do not suffer from photon splitting attacks either, the cutoff distance for BBM92 is still significantly longer. This is because in BBM92 a dark count alone cannot produce an error. It must be accompanied by a photon or another dark count, so it is much less likely to contribute to the signal. The difference in rates between the ideal entangled photon source and the parametric down converter can be attributed to the interplay between coefficient A in Eq. (55), and coefficient D in Eq. (57). Term A is the probability of a real coincidence, and increases with χ. Term D on the other hand contributes to false coincidences and increases with χ as well, but is of higher order. One cannot make A arbitrarily large without getting an increased contribution from D. This leads to an optimum value for χ which is less than one.

IV. ENTANGLEMENT SWAPPING

In this section we analyze a more complicated scheme based on entanglement swapping. Figure 3 gives a diagram of the proposed configuration. A series of entangled photon sources, which we assume to be ideal sources, are spread out an equal distance apart from Alice to Bob. The sources are clocked to simultaneously emit a single pair of entangled photons. Each of the pair is sent to a corresponding Bell state analyzer, whose actions are to perform an entanglement swap. If all the swaps have been successfully performed, Alice and Bob will share a pair of entangled photons. Experimental demonstrations of a single entanglement swap can be found in [37]. Entanglement swapping is a key element for quantum repeaters, which use entanglement purification protocols to reliably exchange quantum correlated photons between two parties [38]. We show that even without such protocols, using only linear optical elements, photon counters, and a clocked source of entangled photons, swapping can enhance the communication distance.

The key element to the scheme is the Bell analyzer. Since we restrict ourselves to passive linear elements and vacuum auxiliary states we cannot achieve a complete Bell measurement. It has recently been shown that Bell analyzers based on only these components cannot have better than a 50% efficiency [39]. One scheme which achieves this maximum is shown in the inset of Fig. 3. This scheme will distinguish between the states

$$|\psi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|xy\rangle \pm |yx\rangle), \tag{65}$$

but will register an inconclusive result if sent the states

$$|\phi_{\pm}\rangle = \frac{1}{\sqrt{2}}(|xx\rangle \pm |yy\rangle). \tag{66}$$

The state generated by the entangled photon sources is assumed to be $|\psi_{+}\rangle$. Considering only a single swap, we can write

$$|\psi_{+}\rangle_{12}|\psi_{+}\rangle_{34} = \frac{1}{2}[|\psi_{+}\rangle_{23}|\psi_{+}\rangle_{14} - |\psi_{-}\rangle_{23}|\psi_{-}\rangle_{14} + |\phi_{+}\rangle_{23}|\psi_{+}\rangle_{14} - |\phi_{-}\rangle_{23}|\phi_{-}\rangle_{14}]. \tag{67}$$

The above expression makes it clear that a Bell measurement on photons 2 and 3 leaves photons 1 and 4 in an entangled state, and the measurement result tells which one. After N such Bell measurements photon 1 and $2N$ will be entangled, and the N Bell measurement results will allow Alice and Bob to know which entangled state they share. Knowledge of this state allows them to perform the BBM92 protocol and interpret their data correctly. Since our Bell analyzer has an efficiency of only 50%, in the best possible case we will pay a price of 2^{-N} in communication rate.

Consider the single swap. We will define α to be the detection probability for each photon. The probability that both photons 2 and 3 reach the Bell analyzer and are successfully projected is

$$p_{swap}^{true} = \tfrac{1}{2}\alpha^2. \tag{68}$$

If a photon is lost in the fiber or due to detector inefficiency the Bell analyzer may still indicate that a Bell measurement has been performed due to detector dark counts. The probability of this happening is

$$p_{swap}^{false} = 6\alpha d + 12d^2. \tag{69}$$

Defining the factor

$$g = \frac{p_{swap}^{true}}{p_{swap}^{true} + p_{swap}^{false}}, \tag{70}$$

it is straightforward to show that, given the Bell analyzer registered a successful Bell measurement, the density matrix of photons 1 and 4 is given by

$$\rho_{14} = g\rho_{\psi_{\pm}} + (1-g)\frac{I}{4}, \tag{71}$$

where $\rho_{\psi_{\pm}}$ is the pure state $|\psi_{+}\rangle$ or $|\psi_{-}\rangle$ depending on the measurement result.

For the case of N entanglement swaps the detection probability for each photon is

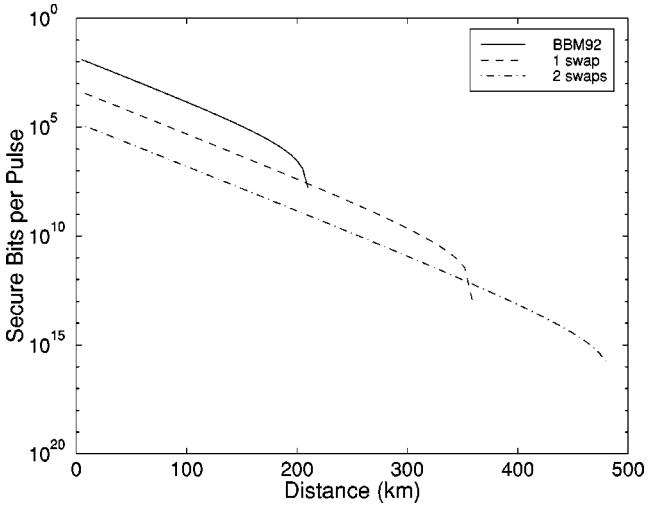

FIG. 4. Comparison of BBM92 protocol with regulated EPR source, one swap scheme, and two swap schemes. Fibers and detectors are taken for the 1.5 μm window.

$$\alpha = \eta 10^{-\left(\frac{\sigma L}{10(2N+2)}\right)}, \tag{72}$$

where L is the distance from Alice to Bob. It is again straightforward to show that after N swaps, the state of photons 1 and $2N$ is

$$\rho_{1,2N} = g^N \rho_{\psi_\pm} + (1-g^N)\frac{I}{4}, \tag{73}$$

and the probability that all N bell measurements registered a successful result is

$$p_{\text{Bell}} = (p_{swap}^{true} + p_{swap}^{false})^N. \tag{74}$$

We then have

$$p_{true} = p_{\text{Bell}} g^N \alpha^2,$$

$$p_{false} = p_{\text{Bell}}(8\alpha d + 16d^2 + (1-g^N)\alpha^2).$$

These can be plugged into Eqs. (43) and (47) to get the final communication rate.

In Fig. 4 we show a comparison between the BBM92 protocol with an ideal entangled photon source, a one-swap scheme, and a two-swap scheme using a fiber optic channel at 1.5 μm. The swaps result in a longer cutoff distance which can lead to longer communication ranges. It should be noted however that at these distances the natural fiber loss is substantial and will lead to very slow communication rates. It is unclear whether swapping will lead to a practical form of quantum key distribution, but a single swap could be useful for very long distance QKD.

V. DISCUSSION

In this paper we provided a proof of security for quantum key distribution with the entangled photon protocol proposed by Bennett, Brassard, and Mermin [5], referred to as BBM92. This proof is based on the assumptions that Eve is restricted to individual attacks and that the detection apparatus is trustable. With these assumptions a bound was derived on Eve's average collision probability, and hence on her mutual information as a function of the final key length.

Using the above results we compared the performance of this protocol to the BB84 protocol for both ideal and practical sources. We investigated fiber-optic as well as free-space key distribution scenarios. The BBM92 protocol was shown to have significantly better performance at longer distance provided that the source can be placed midway between the two communicating parties. This opens up the possibility for communication lengths of up to 170 km.

Finally, we analyzed a more complicated scheme based on entanglement swaps using only linear optical components, photon counters, and a clocked source of entangled photons. Entanglement swapping can allow for even longer distance secure communication, but at some point the natural loss of the fiber becomes so severe that the communication rate is prohibitively slow.

ACKNOWLEDGMENTS

The authors would like to thank Norbert Lütkenhaus and Dominic Mayers for their many helpful comments and suggestions.

APPENDIX A: INFORMATION BOUNDS ON EAVESDROPPING

In this appendix we show how to bound Eve's expected information $I_E(K;GUZ)$ by the average collision probability

$$\langle p_c(x|z)\rangle_z = \sum_z p(z) P_c(X|Z=z), \tag{A1}$$

where

$$P_c(X|Z=z) = \sum_x p^2(x|z). \tag{A2}$$

Let U and Z be arbitrary, possibly correlated, random variables over alphabets $\mathcal{U}$ and $\mathcal{Z}$, respectively. Let $|\cdot|$ denote the cardinality of a given set. Let $t>0$ be a security parameter chosen by Alice and Bob and define set A as

$$A = \left\{ (u,z) \in (\mathcal{U},\mathcal{Z}) : p(u|z) \geqslant \frac{2^{-t}}{|\mathcal{U}|} \right\}. \tag{A3}$$

Defining A^c as the complement of set A we have

$$P(A^c) = \sum_{(u,z)\in A^c} p(u,z) = \sum_{(u,z)\in A^c} p(u|z)p(z)$$

$$\leqslant \frac{2^{-t}}{|\mathcal{U}|} \sum_{u\in\mathcal{U}, z\in\mathcal{Z}} p(z) = 2^{-t}.$$

Thus with probability of at least $1-2^{-t}$ the combined string (U, Z) take a value in A. Then for another random variable X,

$$\begin{aligned}\langle P_c(X|Z=z)\rangle_z &= \sum_{z\in\mathcal{Z}} p(z)\sum_x p^2(x|z)\\ &= \sum_{z\in\mathcal{Z}} p(z)\sum_x \left(\sum_{u\in\mathcal{U}} p(u|z)p(x|uz)\right)^2\\ &\geqslant \sum_{z\in\mathcal{Z}} p(z)\sum_x \sum_{u\in\mathcal{U}} p^2(u|z)p^2(x|uz)\\ &= \sum_{z\in\mathcal{Z},u\in\mathcal{U}} p(u,z)p(u|z)\sum_x p^2(x|uz)\\ &\geqslant \sum_{(z,u)\in A} p(u|z)p(u,z)\sum_x p^2(x|uz)\\ &\geqslant \frac{2^{-t}}{|\mathcal{U}|}\sum_{(z,u)\in\mathcal{A}} p(u,z)P_c(X|U=z,Z=z).\end{aligned}$$

Thus

$$\sum_{(z,u)\in A} p(u,z)P_c(X|U=z,Z=z)\leqslant 2^t|\mathcal{U}|\langle P_c(X|Z=z)\rangle_z. \tag{A4}$$

We can now use this result to bound $H(K|GUZ)$ as follows:

$$\begin{aligned}H(K|GUZ) &= \sum_{u,z} p(u,z)H(K|G,U=u,Z=z)\\ &= \sum_{(u,z)\in A} p(u,z)H(K|G,U=u,Z=z)\\ &\quad + \sum_{(u,z)\in A^c} p(u,z)H(K|G,U=u,Z=z)\\ &\geqslant \sum_{(u,z)\in A} p(u,z)H(K|G,U=u,Z=z),\end{aligned}$$

using the positivity of the conditional entropy functions, and the fact that U and Z are independent of G. Plugging Eq. (17) into the above inequality leads to

$$\begin{aligned}H(K|GUZ) &\geqslant \sum_{(u,z)\in A} p(u,z)\\ &\quad\times\left(r-\frac{2^r}{\ln 2}p_c(X|U=u,Z=z)\right)\\ &\geqslant (1-2^{-t})r-\frac{2^r}{\ln 2}2^t|\mathcal{U}|\langle p_c(X|Z=z)\rangle_z\\ &= (1-2^{-t})r-2^{r+t+\log_2|\mathcal{U}|+\log_2\langle p_c(X|Z=z)\rangle_z},\end{aligned}$$

as follows from Eq. (A4). We can then set

$$r=-\log_2\langle p_c(X|Z=z)\rangle_z-t-\kappa-s, \tag{A5}$$

where $\kappa=\log_2|\mathcal{U}|$ is the number of bits in message U and s is another security parameter. This leads to the bound

$$H(K|GUZ)\geqslant(1-2^{-t})r-\frac{2^{-s}}{\ln 2}. \tag{A6}$$

Eve's mutual information can now be bounded by

$$I_E(K;GUZ)=H(K)-H(K|GUZ)\leqslant 2^{-t}r+\frac{2^{-s}}{\ln 2}.$$

Plugging Eqs. (13) into (A5) leads directly to

$$r=n\tau-t-\kappa-s, \tag{A7}$$

where $\tau=-\log_2 p_c$.

APPENDIX B: ONE-PHOTON CONTRIBUTION

In this appendix we show that there is always an optimal eavesdropping strategy for the contribution from $\rho_{abe}^{(11)}$ which can be described by a set of complete projectors A_k. These complete projectors may depend on the measurement basis used by Alice and Bob.

First consider the POVM which Alice performs on her photon. Since we only look at the subspace where she receives exactly one photon, there can only be one detection event. The four detectors map out to the four operators

$$F_x=\tfrac{1}{2}|x\rangle\langle x|, \tag{B1}$$

$$F_y=\tfrac{1}{2}|y\rangle\langle y|, \tag{B2}$$

$$F_u=\tfrac{1}{2}|u\rangle\langle u|, \tag{B3}$$

$$F_v=\tfrac{1}{2}|v\rangle\langle v|, \tag{B4}$$

where we use the shorthand notation $|x\rangle$, $|y\rangle$, $|u\rangle$, and $|v\rangle$ to indicate one photon polarized along the direction indicated by the state. Note that for the above four operators $F_a^T/\mathrm{Tr}\{F_a\}$ are the same as the density matrices prepared by Alice in the BB84 protocol.

Eve is allowed to choose any density-matrix $\rho_{abe}^{(11)}$. We can assume without loss of generality that $\rho_{abe}^{(11)}$ is a pure state because any mixed state can be generated by a pure state with a probe of higher dimensions by ignoring some of its degrees of freedom. Discarding information cannot enhance Eve's knowledge on the final key. The most general pure state can be written as

$$|\psi_{abe}\rangle=|xx\rangle|P_{xx}\rangle+|yy\rangle|P_{yy}\rangle+|xy\rangle|P_{xy}+|yx\rangle|P_{yx}\rangle, \tag{B5}$$

where $|P_{xx}\rangle$, $|P_{yy}\rangle$, $|P_{xy}\rangle$, and $|P_{yx}\rangle$ are states of Eve's probe and are not assumed to be normalized or orthogonal. Alternatively we can write this wave function in the u-v basis as

$$|\psi_{abe}\rangle=|uu\rangle|P_{uu}\rangle+|vv\rangle|P_{vv}\rangle+|uv\rangle|P_{uv}\rangle+|vu\rangle|P_{vu}\rangle, \tag{B6}$$

where Eve's probe states in the u-v are given by

$$|P_{uu}\rangle=\tfrac{1}{2}(|P_{xx}\rangle+|P_{yy}\rangle+|P_{xy}\rangle+|P_{yx}\rangle), \tag{B7}$$

$$|P_{vv}\rangle=\tfrac{1}{2}(|P_{xx}\rangle+|P_{yy}\rangle-|P_{xy}\rangle-|P_{yx}\rangle), \tag{B8}$$

$$|P_{uv}\rangle=\tfrac{1}{2}(|P_{xx}\rangle-|P_{yy}\rangle-|P_{xy}\rangle+|P_{yx}\rangle), \tag{B9}$$

$$|P_{vu}\rangle=\tfrac{1}{2}(|P_{xx}\rangle-|P_{yy}\rangle+|P_{xy}\rangle-|P_{yx}\rangle). \tag{B10}$$

Throughout this discussion we will use dirac notation interchangeably with the matrix notation

$$|x\rangle=\begin{bmatrix}1\\0\end{bmatrix},$$

$$|y\rangle=\begin{bmatrix}0\\1\end{bmatrix}.$$

Suppose that Alice measures the positive operator F_a with the general form

$$F_a=\begin{bmatrix}a & b\\ b^* & c\end{bmatrix}. \tag{B11}$$

Then

$$\rho_b=\frac{\mathrm{Tr}_{ae}\{|\psi_{abe}\rangle\langle\psi_{abe}|F_a\}}{\mathrm{Tr}\{|\psi_{abe}\rangle\langle\psi_{abe}|F_a\}}. \tag{B12}$$

If we define the operator

$$A_k=\sqrt{\frac{\mathrm{Tr}\{F_a\}}{\mathrm{Tr}\{|\psi_{abe}\rangle\langle\psi_{abe}|F_a\}}}\begin{bmatrix}\langle k|P_{xx}\rangle & \langle k|P_{yx}\rangle\\ \langle k|P_{xy}\rangle & \langle k|P_{yy}\rangle\end{bmatrix},$$

then one can verify that

$$\rho_b=\sum_k A_k\frac{F_a^T}{\mathrm{Tr}\{F_a\}}A_k^\dagger.$$

In the ideal case, where Alice and Bob share a maximally entangled pair of photons, we have

$$\rho_b=\frac{F_a^T}{\mathrm{Tr}\{F_a\}}.$$

The operators A_k map the ideal channel to the noisy channel.

We are not done yet. We must still show that the operators satisfy the completeness relation

$$\sum_k A_k^\dagger A_k=I, \tag{B13}$$

and that they do not depend on F_a. In the BB84 protocol these conditions come naturally because Eve's interaction with the signal must be unitary. In the BBM92 protocol there are attacks which do not satisfy these conditions and thus cannot be described by a CP map. However, we will show that there is always an optimal attack which does satisfy these two conditions, and can thus be characterized by such a map.

Without loss of generality we can assume that the operators A_k are real matrices. If this is not true than one can write A_k as

$$A_k=R_k+iI_k,$$

where R_k and I_k are real matrices. The joint probability that Alice measures F_a and Eve measures A_k is

$$\mathrm{Tr}\{A_kF_aA_k^\dagger\}=\mathrm{Tr}\{R_kF_aR_k^T\}+\mathrm{Tr}\{I_kF_aI_k^T\}.$$

Since there is no mixing between the real and imaginary parts Eve could break up A_k into two real operators R_k and I_k by adding one more dimension to her probe. This type of probability split can only enhance her final collision probability ([40], Appendix E).

Starting with Eq. (B13) we sum over k to get

$$\sum_k A_k^\dagger A_k=\frac{\mathrm{Tr}\{F_a\}}{\mathrm{Tr}\{|\psi_{abe}\rangle\langle\psi_{abe}|F_a\}}\times\begin{bmatrix}\langle P_{xx}|P_{xx}\rangle+\langle P_{xy}|P_{xy}\rangle & \langle P_{xx}|P_{yx}\rangle+\langle P_{xy}|P_{yy}\rangle\\ \langle P_{yx}|P_{xx}\rangle+\langle P_{yy}|P_{xy}\rangle & \langle P_{yy}|P_{yy}\rangle+\langle P_{yx}|P_{yx}\rangle\end{bmatrix}. \tag{B14}$$

We now show that there is always an optimal attack which satisfies the following symmetry conditions:

$$\langle P_{xx}|P_{xx}\rangle=\langle P_{yy}|P_{yy}\rangle, \tag{B15}$$

$$\langle P_{xy}|P_{xy}\rangle=\langle P_{yx}|P_{yx}\rangle, \tag{B16}$$

$$\langle P_{uu}|P_{uu}\rangle=\langle P_{uu}|P_{uu}\rangle, \tag{B17}$$

$$\langle P_{uv}|P_{uv}\rangle=\langle P_{vu}|P_{vu}\rangle. \tag{B18}$$

Suppose that the wave function (B5) does not satisfy these conditions. Eve can apply the following transformation to both Alice and Bob's photon

$$|x\rangle\mapsto|y\rangle,|y\rangle\mapsto|x\rangle, \tag{B19}$$

and it can be shown that this does not effect the error rate or collision probability. She can also apply the transformation

$$|x\rangle\mapsto|x\rangle,|y\rangle\mapsto-|y\rangle, \tag{B20}$$

which is the same as flipping $|u\rangle$ with $|v\rangle$. This does not effect the collision probability or the error rate either. Thus, Eve can send any one of the four states below without changing anything

(1) $|xx\rangle|P_{xx}\rangle+|yy\rangle|P_{yy}\rangle+|xy\rangle|P_{xy}\rangle+|yx\rangle|P_{yx}\rangle$,

(2) $|xx\rangle|P_{yy}\rangle+|yy\rangle|P_{xx}\rangle+|xy\rangle|P_{yx}\rangle+|yx\rangle|P_{xy}\rangle$,

(3) $|xx\rangle|P_{xx}\rangle+|yy\rangle|P_{yy}\rangle-|xy\rangle|P_{xy}\rangle-|yx\rangle|P_{yx}\rangle$,

(4) $|xx\rangle|P_{yy}\rangle+|yy\rangle|P_{xx}\rangle-|xy\rangle|P_{yx}\rangle-|yx\rangle|P_{xy}\rangle$.

The second state is obtained by applying Eq. (B19) to the first state. The third state is obtained by applying Eq. (B20) to the first state, and the fourth state is obtained by first applying Eq. (B19), then Eq. (B20). Eve could send an equal mixture of all four states without altering the error rate or collision probability, and one can verify that this equal mixture would satisfy the desired symmetry conditions.

Condition (B16), along with the fact that, Eq. (B5) must be normalized, amounts to

$$\langle P_{xx}|P_{xx}\rangle+\langle P_{xy}|P_{xy}\rangle=\langle P_{yy}|P_{yy}\rangle+\langle P_{yx}|P_{yx}\rangle=1/2. \tag{B21}$$

Knowing that A_k is a real matrix, we then have from condition (B18),

$$\langle P_{xx}|P_{yx}\rangle+\langle P_{xy}|P_{yy}\rangle=0. \tag{B22}$$

These two relations immediately imply that

$$\mathrm{Tr}\{|\psi_{abe}\rangle\langle\psi_{abe}|F_a\}=\frac{\mathrm{Tr}\{F_a\}}{2},$$

which means that

$$A_k=\sqrt{2}\begin{bmatrix}\langle k|P_{xx}\rangle & \langle k|P_{yx}\rangle\\ \langle k|P_{xy}\rangle & \langle k|P_{yy}\rangle\end{bmatrix}.$$

So A_k are independent from F_a and the completeness relation (B13) comes directly from Eqs. (B21) and (B22).

APPENDIX C: HIGHER-ORDER NUMBER STATE CONTRIBUTIONS

Higher-order number states are taken into account by setting w_D sufficiently large so that Eve's optimal strategy is to only use the $\rho_{abe}^{(11)}$ component. First suppose Eve sends one photon to Alice and j photons to Bob, where $j>1$. Then

$$p_D^{(1j)}\geqslant 2\left[\frac{1}{2}-\left(\frac{1}{2}\right)^j\right]\mathrm{Tr}\{\rho_{abe}^{(1j)}\}, \tag{C1}$$

$$p_{rec}^{(1j)}\leqslant 2\left(\frac{1}{2}\right)^j\mathrm{Tr}\{\rho_{abe}^{(1j)}\}, \tag{C2}$$

which leads to

$$\frac{p_D^{(1j)}}{p_{rec}^{(1j)}}\geqslant\frac{\left[\frac{1}{2}-\left(\frac{1}{2}\right)^j\right]}{\left(\frac{1}{2}\right)^j}\geqslant 1. \tag{C3}$$

The argument is completely equivalent if Eve sends j photons to Alice and one photon to Bob. Now if Eve sends i photons to Alice and j photons to Bob, where $i,j>1$, then

$$p_D^{(ij)}\geqslant 2\left[\frac{1}{2}-\left(\frac{1}{2}\right)^i\right]\left[\frac{1}{2}-\left(\frac{1}{2}\right)^j\right]\mathrm{Tr}\{\rho_{abe}^{(ij)}\}, \tag{C4}$$

$$p_{rec}^{(ij)}\leqslant 2\left(\frac{1}{2}\right)^i\left(\frac{1}{2}\right)^j\mathrm{Tr}\{\rho_{abe}^{(ij)}\}, \tag{C5}$$

which leads to

$$\frac{p_D^{(ij)}}{p_{rec}^{(ij)}}\geqslant\frac{\left[\frac{1}{2}-\left(\frac{1}{2}\right)^i\right]}{\left(\frac{1}{2}\right)^i}\frac{\left[\frac{1}{2}-\left(\frac{1}{2}\right)^j\right]}{\left(\frac{1}{2}\right)^j}\geqslant 1. \tag{C6}$$

A disturbance of 1/2 already implies that Eve can obtain the entire string. So setting w_D to 1/2 means that Eve can do at least as good by sending only $\rho_{abe}^{(11)}$. Thus

$$p_c\geqslant\tfrac{1}{2}+2\epsilon-2\epsilon^2. \tag{C7}$$

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[3] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[6] 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).
[7] P. D. Townsend, IEEE Photonics Technol. Lett. **10**, 1048 (1998).
[8] C. Marand and P. T. Townsend, Opt. Lett. **20**, 1695 (1995).
[9] G. Rigbordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, J. Mod. Opt. **47**, 517 (2000).
[10] M. Bourennane, F. Gibson, A. Karlsson, A. Hening, P. Johnson, T. Tsegaye, D. Ljunggren, and E. Sundberg, Opt. Express **4**, 383 (1999).
[11] W. Tittel, J. Brendel, N. Gisin, and H. Zbinden, Phys. Rev. A **59**, 4150 (1999).
[12] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).
[13] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[14] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglung, and P. G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000).
[15] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
[16] B. Huttner and A. K. Ekert, J. Mod. Opt. **41**, 2455 (1994).
[17] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[18] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).
[19] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
[20] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[21] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).

[22] D. Mayers, J. ACM **48**, 351 (2001).
[23] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowder, *Proceedings of the 32nd Annual ACS Symposium of Theory of Computing* (ACM Press, New York, 2000), pp. 715–724.
[24] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[25] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[26] H. Aschauer and J. Briegel, e-print quant-ph/0008051.
[27] H. Inamori, e-print quant-ph/0008064.
[28] D. Mayers and A. Yao, e-print quant-ph/0007058.
[29] D. Mayers (unpublished).
[30] T. M. Cover, *Elements of Information Theory* (Wiley, New York, 1991).
[31] G. Brassard and L. Salvail, in *Advances in Cryptology-EUROCRYPT'93*, Vol. 765 of Lecture Notes in Computer Science, edited by T. Hellseth (Springer, Berlin, 1994), pp. 410–423.
[32] C. H. Bennett, G. Brassard, C. Crpeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[33] C. Cachin and U. M. Maurer, J. Cryptology **10**, 97 (1997).
[34] O. Benson, C. Santori, M. Pelton, and Y. Yamamoto, Phys. Rev. Lett. **84**, 2513 (2000).
[35] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, Berlin, 1994).
[36] P. G. Kwiat, K. Mattle, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **75**, 4337 (1995).
[37] J. W. Pan, D. Bouwmeester, H. Weifurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998).
[38] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **81**, 5932 (1998).
[39] J. Calsamiglia and N. Lutkenhaus, e-print quant-ph/0007058.
[40] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).