INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF OPTICS B: QUANTUM AND SEMICLASSICAL OPTICS

J. Opt. B: Quantum Semiclass. Opt. **4** (2002) 109–113 PII: S1464-4266(02)30945-5

The effect of multi-pair signal states in quantum cryptography with entangled photons

Miloslav Dušek[1] **and Kamil Brádler**[2]

[1] Department of Optics, Palacký University, 17 listopadu 50, 772 00 Olomouc, Czech Republic

[2] Department of Chemical Physics and Optics, Charles University, Ke Karlovu 3, 121 16 Prague 2, Czech Republic

Received 19 November 2001, in final form 29 January 2002
Published 5 February 2002
Online at stacks.iop.org/JOptB/4/109

Abstract

Real sources of entangled photon pairs (such as parametric down conversion) are not perfect. They produce quantum states that contain more than only one photon pair with some probability. Several aspects of the use of such states for the purpose of quantum key distribution are discussed. It is shown that the presence of 'multi-pair' signals (together with low detection efficiencies) causes errors in transmission even in the absence of an eavesdropper. Moreover, it is shown that even the eavesdropping, that draws information only from these 'multi-pair' signals, increases the error rate. This fact represents the important advantage of entanglement-based quantum key distribution. Information, that can be obtained by an eavesdropper from the 'multi-pair' signals, is also calculated.

Keywords: Quantum cryptography, down conversion

1. Introduction

The only provably secure method of communication with guaranteed privacy is Vernam cipher (or one-time pad) [1]. It requires both communicating parties to share a secret key of the same length as the message. The problem was how to distribute this key securely. The solution has been found on the ground of quantum physics. Quantum key distribution (QKD) is a technique to provide two parties with such a secure, secret and shared key. The first protocol for QKD was given by Bennett and Brassard [2] (BB84) following Wiesner's ideas [3]. The essence of this protocol is that if non-orthogonal quantum states are used for communication and a channel transmits them perfectly then eavesdropping is detectable. Later a different protocol, inspired by Bell's inequalities, was proposed by Ekert [4]. It relies on nonclassical correlations or entanglement of two quantum particles. Its simplified ('BB84-like') version works as follows [5]: let us suppose two communicating parties, *Alice* and *Bob*, share a set of entangled pairs $(|V\rangle_A|V\rangle_B + |H\rangle_A|H\rangle_B)/\sqrt{2}$, where $|V\rangle$ and $|H\rangle$ are two orthonormal states of each particle—e.g., vertical and horizontal linear polarizations of photons. Alice and Bob choose randomly and independently between two conjugated polarization bases—e.g., between basis $\{V, H\}$ (+) and the 'diagonal' basis (×) which are mutually rotated by 45°. Following a public discussion about the choice of the basis of measurement apparatuses, Alice and Bob can obtain a shared key made up from those signals where the measurement devices give correlated results. This is the so-called sifted key.

For ideal systems proofs of security against collective and joint attacks were given [6–9]. Finally, proofs of security of BB84, even in the presence of noise, have been obtained [10–13]. For practical protocols security analysis is in its initial stage [14–19].

Photon pairs with correlated polarizations can be prepared, e.g., by parametric down conversion of type II [20] or using two down-conversion crystals with phase matching of type I [21]. Unfortunately, these techniques never produce exactly a single pair of photons. Quantum states generated by the above-mentioned down-conversion methods should be the same in principle. However, the system with two nonlinear crystals is perhaps more illustrative for our purposes. Orientations of optical axes of two identical crystals are mutually perpendicular. With a vertically (horizontally) polarized pump beam down conversion will only occur in the first (second) crystal, respectively. A 45°-polarized pump photon will be equally likely to down convert in either crystal. Let us suppose two spatial modes with two fixed frequencies fulfilling phase-matching conditions. One is aimed at Alice, the other at Bob. The first crystal generates beams with horizontal polarizations, the second one beams with vertical polarizations. The quantum state generated by one crystal can be described [22] as[1]

$$|\psi\rangle = \xi \sum_{n=0}^{\infty} g^n |n\rangle_A |n\rangle_B, \tag{1}$$

where $|n\rangle$ are corresponding number states, $\xi = (\cosh \chi t)^{-1} = \sqrt{1-g^2}$ and $g = \tanh \chi t$ with χ being proportional to the nonlinear susceptibility and pump power and t denoting the interaction time[2]. The total quantum state originating from both the crystals is then[3]

$$\begin{aligned}|\Psi\rangle &= |\psi\rangle_1 |\psi\rangle_2 \\ &= \xi^2 \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} g^{m+n} |m\rangle_{AV} |m\rangle_{BV} |n\rangle_{AH} |n\rangle_{BH},\end{aligned} \tag{2}$$

where the subscripts V and H denote modes with vertical polarization (produced by the first crystal) and horizontal polarization (coming from the second crystal), respectively. The mean number of pairs is

$$\mu = \xi^4 \sum_{m,n} (m+n) g^{2(m+n)} = \frac{2g^2}{1-g^2}. \tag{3}$$

The presence of more than one pair in the signals (or more than one photon in the case of 'single-photon' protocols) may enable eavesdropper (*Eve*) to obtain information about the cryptographic key without causing any error. Thus she could learn something about the key and simultaneously stay undisclosed. Similar difficulties implied by the use of weak coherent states in combination with lossy lines were pointed out earlier [14–19]. A comprehensive analysis of the security aspects of practical quantum cryptosystems taking into account the source imperfections was performed in [18]. However, the role of down-conversion sources was reduced just to the preparation of approximate single-photon states there. In this paper we want to go beyond this limitation by considering the entanglement-based QKD.

This paper is organized as follows. In section 2 we explain, on a simplified signal state containing at most two pairs of photons, why errors appear in QKD. Imperfect detection efficiency and losses on the transmission line are taken into account while detector dark counts are neglected. Section 3 contains the comparison of the amount of information that can be obtained by Eve from multi-pair or multi-particle signals (by means of photon-number-splitting attack [18]) for different cryptographic schemes. Particularly for quantum cryptography using entangled photons, weak coherent states, and down-conversion 'single-photon' sources. In section 4 we briefly discuss restrictions on Eve's activity stemming from monitoring both the data rate and the 'double-click' rate (both detectors corresponding to logical 1 and 0 fire together). Section 5 concludes the paper with a short summary.

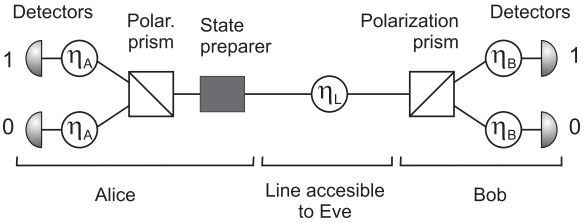

Figure 1. Arrangement for QKD. State preparer, situated at Alice's side, generates signal states (2). Both Alice and Bob have detectors that cannot distinguish the number of impinging photons and whose detection efficiencies are η_A and η_B, respectively (this is indicated by circles in the figure). Alice and Bob change between two orientations of their polarization analysers: + and ×. Both communicating parties are connected by a quantum channel with transmittance η_L. This channel is accessible to Eve.

2. Errors in QKD due to imperfect signal states

Consider the configuration for QKD as in figure 1. Let us suppose that $g \ll 1$ so that in equation (2) we can neglect all terms containing more than two pairs:

$$\begin{aligned}|\Psi\rangle = \xi^2 [&|0,0,0,0\rangle + g(|0,0,1,1\rangle + |1,1,0,0\rangle) \\ &+ g^2(|0,0,2,2\rangle + |2,2,0,0\rangle + |1,1,1,1\rangle) + \mathcal{O}(g^3)].\end{aligned} \tag{4}$$

Here we have used the notation

$$\begin{aligned}|m,m,n,n\rangle &= |m\rangle_{AV} |m\rangle_{BV} |n\rangle_{AH} |n\rangle_{BH} \\ &= \frac{1}{m!n!} [(\mathsf{a}^\dagger_{AV} \mathsf{a}^\dagger_{BV})^m (\mathsf{a}^\dagger_{AH} \mathsf{a}^\dagger_{BH})^n] |\text{vac}\rangle\end{aligned} \tag{5}$$

with $\mathsf{a}^\dagger$ denoting creation operators in corresponding modes.

In the diagonal basis ×, represented by the following creation operators:

$$\begin{aligned}\mathsf{a}^\dagger_X &= (\mathsf{a}^\dagger_V + \mathsf{a}^\dagger_H)/\sqrt{2}, \\ \mathsf{a}^\dagger_Y &= (\mathsf{a}^\dagger_V - \mathsf{a}^\dagger_H)/\sqrt{2},\end{aligned} \tag{6}$$

state (4) does *not change* its form. It can be shown that even the full state (2) is invariant under such transformations of bases (the same transformation at both sides).

Losses on the channel and non-perfect efficiency of Alice's and Bob's detectors are modelled by beamsplitters with intensity transmittances η_L, η_A and η_B, respectively. All detectors are assumed to be 'yes/no' detectors, which either fire or do not fire—they cannot distinguish the number of impinging photons. They can be described by the pair of POVM operators $\mathsf{P}_{no} = |0\rangle\langle 0| + \sum_{n=1}^{\infty} (1-\eta)^n |n\rangle\langle n|$ and $\mathsf{P}_{yes} = \sum_{n=1}^{\infty} [1 - (1-\eta)^n] |n\rangle\langle n|$, where η is a detector efficiency. We neglect noise.

We intend to show that if the detector efficiencies are lower than 100% the use of signal states (4) inevitably causes errors in the sifted key. Therefore we are interested only in those cases when Alice and Bob have set the same polarization bases. Of course, Alice and Bob include in the key only those events

[1] Of course, this is just an approximation because more than only two modes are always present in real cases. If the number of signal or idler modes is effectively infinite then the total number of photons in signal or idler beam, respectively, obeys Poissonian statistics.

[2] It has a good physical meaning only for a pulse-pumped down conversion. Then it may be limited to infinity.

[3] We neglect a slight decrease of the pump power behind the first crystal.

in which *exactly one* detector fires at each side. The average relative length of the sifted key (with respect to the number of all generated entangled states) is then given by the formula[4]

$$\begin{aligned} R_{key} &= \tfrac{1}{2}\langle\Psi(\mathsf{P}^{AV}_{yes}\mathsf{P}^{AH}_{no}\mathsf{P}^{BV}_{yes}\mathsf{P}^{BH}_{no} + \mathsf{P}^{AV}_{no}\mathsf{P}^{AH}_{yes}\mathsf{P}^{BV}_{no}\mathsf{P}^{BH}_{yes} \\ &\quad + \mathsf{P}^{AV}_{yes}\mathsf{P}^{AH}_{no}\mathsf{P}^{BV}_{no}\mathsf{P}^{BH}_{yes} + \mathsf{P}^{AV}_{no}\mathsf{P}^{AH}_{yes}\mathsf{P}^{BV}_{yes}\mathsf{P}^{BH}_{no})|\Psi\rangle \\ &\approx \xi^4 g^2\{\eta_A\eta_B\eta_L + g^2[1-(1-\eta_A)^2][1-(1-\eta_B\eta_L)^2] \\ &\quad + 2g^2\eta_A(1-\eta_A)\eta_B\eta_L(1-\eta_B\eta_L)\}. \end{aligned} \tag{7}$$

Indices AV denote Alice's detector monitoring vertical polarization, BH denote Bob's detector monitoring horizontal polarization, etc. The first term on the right-hand side comes from the entangled state $|0,0,1,1\rangle + |1,1,0,0\rangle$, i.e. it represents a contribution from a single pair. The second term is a correction stemming from the state $|0,0,2,2\rangle + |2,2,0,0\rangle$ and the third one a correction from the state $|1,1,1,1\rangle$.

On the other hand, the relative number of errors (i.e. events when Alice gets a bit different from that detected by Bob) is

$$\begin{aligned} R_{err} &= \tfrac{1}{2}\langle\Psi(\mathsf{P}^{AV}_{yes}\mathsf{P}^{AH}_{no}\mathsf{P}^{BV}_{no}\mathsf{P}^{BH}_{yes} + \mathsf{P}^{AV}_{no}\mathsf{P}^{AH}_{yes}\mathsf{P}^{BV}_{yes}\mathsf{P}^{BH}_{no})|\Psi\rangle \\ &\approx \xi^4 g^4\eta_A(1-\eta_A)\eta_B\eta_L(1-\eta_B\eta_L). \end{aligned} \tag{8}$$

Thus the error rate reads

$$\begin{aligned} \varepsilon = \frac{R_{err}}{R_{key}} &\approx \frac{g^2(1-\eta_A-\eta_B\eta_L+\eta_A\eta_B\eta_L)}{1+g^2(6-4\eta_A-4\eta_B\eta_L+3\eta_A\eta_B\eta_L)} \\ &= \frac{(1-\eta_A)(1-\eta_B\eta_L)}{2}\mu + \mathcal{O}(\mu^2). \end{aligned} \tag{9}$$

Clearly, if $\eta_A \to 1$ then $\varepsilon \to 0$ for all mean pair numbers μ. So Alice should have as good detectors as possible. At Bob's side the crucial limitation is usually represented by a low line transmission η_L for real systems. If $\eta_L \ll \eta_A, \eta_B$ then $\varepsilon \approx (1-\eta_A)\mu/2$.

3. Information leaked to Eve

Let us assume now that Eve will try to get some information on the key only from 'multi-particle' (or 'multi-pair') signals in order to avoid errors in transmission. She will be allowed to use the most efficient individual attack of this kind—the photon-number-splitting (PNS) attack [18]: she substitutes a lossy channel by a lossless one. Then she measures the total number of photons in incoming signals. If this number is higher than one she extracts and stores one photon (or more). The rest is sent to Bob. It is also supposed that she can control Bob's detection efficiency, so that Bob always receives these signals. If the number of incoming photons is equal to one she either blocks the signal or passes it without other changes to Bob (in order not to decrease the data rate). After the public comparison of Alice's and Bob's bases she makes a polarization measurement on the stored photons.

The average Eve's information about sifted-key bits is

$$I_E = \sum_i r_i[1 + p_i\log_2 p_i + (1-p_i)\log_2(1-p_i)], \tag{10}$$

where r_i is the portion of bits that Eve knows with probability p_i; $\sum_i r_i = 1$. If Eve knows r percent bits for certain, and she has no idea about the others then simply $I_E = r$.

3.1. Weak coherent states

First let us look at the case of quantum cryptography with weak coherent states (WCS). The signals are represented by the states (of corresponding polarization modes)

$$|\alpha\rangle = \exp(-|\alpha|^2/2)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle,$$

where $|n\rangle$ are Fock states. A mean photon number in a signal state is $\mu' = |\alpha|^2$.

The expected average relative length of the sifted key (in proportion to the number of all sent signals) is [16, 18]

$$R_{exp} = \tfrac{1}{2}[1 - \exp(-\eta_L\eta_B\mu')],$$

where η_B denotes Bob's detector efficiency. The average relative number of 'multi-photon' signals is given by the formula

$$R_{multi} = \tfrac{1}{2}\sum_{n=2}^{\infty}|\langle\alpha|n\rangle|^2 = \tfrac{1}{2}[1-(1+\mu')\exp(-\mu')].$$

Eve can determine all the bits stemming from these 'multi-photon' signals with certainty. Thus the information leaked to Eve reads

$$I_E^{(WCP)} = \begin{cases} 1 & \text{if } R_{exp} \leqslant R_{multi}, \\ \dfrac{R_{multi}}{R_{exp}} \approx \dfrac{1}{2\eta_L\eta_B}\mu', & \text{otherwise.} \end{cases} \tag{11}$$

If the number of 'multi-photon' signals is lower than the expected number of sifted-key bits Eve must pass some 'single-photon' signals in order to reproduce the data rate. So, Eve knows the part of the key bits with certainty but she knows nothing about the rest (corresponding to the passed 'single-photon' signals).

3.2. Parametric down conversion

Now, what information may leak to Eve if a parametric down-conversion (PDC) source of 'single' photons is used instead of laser-producing coherent states? Generated signal states (with fixed polarizations) are used for BB84 QKD protocol in exactly the same manner as WCS [18]. The source consists of a single down-conversion crystal generating state (1) and a 'yes/no' detector (with an efficiency η_A) placed in one of the two output modes. A click on this detector means that the signal state has been prepared in the other mode. The expected average relative length of the sifted key (in proportion to the number of all generated entangled states) is given by the formula

$$R_{exp} = \frac{\xi^2}{2}\sum_{n=0}^{\infty} g^{2n}[1-(1-\eta_A)^n][1-(1-\eta_L\eta_B)^n].$$

The average relative number of 'multi-photon' signals reads

$$R_{multi} = \frac{\xi^2}{2}\sum_{n=2}^{\infty} g^{2n}[1-(1-\eta_A)^n].$$

[4] It is taken into account that only about one half of all transmitted signals are included into the sifted key because only one half of Alice's and Bob's bases coincide on average.

Again, Eve can learn all the bits carried by the 'multi-photon' signals with certainty. After some straightforward calculations one can find the amount of information leaked to her[5]:

$$I_E^{(PDC)} = \begin{cases} 1 & \text{if } R_{exp} \leqslant R_{multi}, \\ \dfrac{R_{multi}}{R_{exp}} \approx \dfrac{2-\eta_A}{\eta_L \eta_B}\mu', & \text{otherwise,} \end{cases} \tag{12}$$

where we have used the fact that in the case under consideration the mean number of pairs in each generated entangled state is $\mu' = g^2/(1-g^2)$.

3.3. Entangled photons

Finally let us look at the cryptographic scheme fully based on the entanglement of photon polarizations (EPP); see figure 1. Signal states are described by equation (2). All detectors are of 'yes/no' type again; on Alice's side they have efficiencies η_A, on Bob's side η_B.

Here the situation is more complex. It becomes important how many photons Eve separates. However, we will confine ourselves only to the simplified situation when at most two pairs are present with a reasonable probability (see equation (4)). Then Eve can separate no more than one photon and send the remaining one to Bob. In contrast to two previous cases, now the information I_{AE} that Eve shares with Alice is *different* from the information I_{EB} that she shares with Bob. This is related to the occurrence of errors in the transmission.

The expected rate of sifted-key generation is given by equation (7): $R_{exp} = R_{key}$. A portion of two-photon signals leaving Alice's terminal—those signals that can be read by Eve applying PNS attack—is

$$R_{double} = \xi^4 g^4 \{[1-(1-\eta_A)^2] + \eta_A(1-\eta_A)\}.$$

The first term represents contributions from the states $|0,0,2,2\rangle$ and $|2,2,0,0\rangle$, while the second term that from the state $|1,1,1,1\rangle$. (It is taken into account that the bit is accepted to the key only if there is exactly one click of Alice's detector.)

When calculating information it must be taken into account that Eve does not know all measured bits with certainty. She cannot distinguish the signals stemming from states $|1,1,1,1\rangle$ from the other two-photon signals. And for these particular signals she hits Alice's bit only with probability 50% and Bob's bit values are even always opposite to hers. Thus Eve's average information is

$$I_j^{(EPP)} \approx \begin{cases} f(p_j) & \text{if } R_{exp} \leqslant R_{double}, \\ \dfrac{R_{double}}{R_{exp}} f(p_j) \approx \dfrac{3-2\eta_A}{2\eta_L\eta_B} f(p_j)\mu, & \text{otherwise,} \end{cases} \tag{13}$$

where $j = AE, EB$ and $f(p_j) = 1 + p_j \log_2 p_j + (1-p_j)\log_2(1-p_j)$. Probabilities that Eve has the same bit as Alice or Bob, respectively, correspond to the ratios of successful results to all results:

$$p_{AE} = \frac{5-3\eta_A}{6-4\eta_A}, \qquad p_{EB} = \frac{2-\eta_A}{3-2\eta_A}.$$

Clearly, $f(p_{EB}) < f(p_{AE}) < 1$ for $\eta_A < 1$ and then also $I_{EB} < I_{AE} < 1$. Unfortunately, the fact that the maximum Eve's information (see equation (13)) is lower than unity (if $\eta_A < 1$) does not represent any real advantage because for $R_{exp} \leqslant R_{double}$ information I_{AE} is equal to information shared by Alice and Bob, $I_{AB} = 1 + \varepsilon' \log_2 \varepsilon' + (1-\varepsilon')\log_2(1-\varepsilon')$, where ε' is given by equation (14).

However, notice the very important feature of PNS eavesdropping in EPP systems which reminds 'single-particle' attacks: if Eve applies PNS attack in the way described above, i.e. if she tries to reproduce only the transmission rate (R_{exp}), she *increases* the error rate. The reason is that she increases the fraction of $|1,1,1,1\rangle$ contributions to the key bits: if Eve substantially decreases original technological losses on the line but simulates them henceforth by the selective cancellation of the single-pair signals only she inevitably increases the fraction of multi-pair signals that will contribute to the key and therefore she also increases the number of $|1,1,1,1\rangle$ contributions that are responsible for errors. The relative number of erroneous bits stemming from these contributions is $R_{err}^{(E)} = \xi^4 g^4 \eta_A (1-\eta_A)/2$. Thus due to eavesdropping the error rate grows to

$$\varepsilon' = \begin{cases} \dfrac{R_{err}^{(E)}}{R_{double}} \approx \dfrac{1-\eta_A}{6-4\eta_A}, & \text{if } R_{exp} \leqslant R_{double}, \\ \dfrac{R_{err}^{(E)}}{R_{exp}} \approx \dfrac{1-\eta_A}{4\eta_B\eta_L}\mu, & \text{otherwise.} \end{cases} \tag{14}$$

The increase of the error rate can help to detect an eavesdropper which is impossible in the analogous situation (PNS attack) in WCS and PDC systems.

4. How to restrict Eve's activity

In the previous section Eve was restricted by the demand to reproduce the transmission rate (the average number of sifted-key bits) only. However, it is not the only quantity which could be monitored by Bob. In all the mentioned techniques Bob can also measure the double-click rate in those events when he used a different basis from Alice. In the case of EPP Bob can even monitor the double-click rate in situations with coincident bases (and, of course, he can monitor the error rate). Clearly Bob's activities pose other important restrictions to Eve [19]. Even more possibilities are offered by a passive arrangement, when Alice and Bob do not change bases actively (see, e.g., [23, 24]). However, the calculations of double-click rates in the case of eavesdropping needs to include three-pair contributions at least.

5. Conclusions

The effect of the presence of 'multi-pair signals' on the security of quantum cryptography was discussed. The 'multi-pair signals' inevitably appear in any system with a parametric-down-conversion source. We have shown that there is an important difference between the quantum-cryptographic set-up that uses such a source just as 'the triggered source of photons' and that which employs the entanglement of generated signal pairs directly for QKD. In the latter case there is a nonzero error rate even if there is no eavesdropper.

[5] It can be done exactly but for our purposes the used approximation is good enough.

This is caused by the joint effect of the occurrence of 'multi-pair signals' and of low detection efficiencies. However, the most important result is that in the latter set-up an individual eavesdropping on 'multi-pair signals' increases the error rate in the transmission.

Acknowledgments

MD acknowledges discussions with Zachary Walton. This work has been supported under the project LN00A015 and Research Plan CEZ:J14 'Wave and Particle Optics' of the Ministry of Education of the Czech Republic and project 19982003012 of the Czech National Security Authority.

References

[1] Vernam G S 1926 *AIEE* **45** 109

[2] Bennett C H and Brassard G *Proc. IEEE International Conference on Computers, Systems, and Signal Processing (Bangalore, India, 1984)* (New York: IEEE) pp 175–9

[3] Wiesner S 1983 *SIGACT News* **15** 78

[4] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[5] Bennett C H, Brassard G and Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

[6] Biham E and Mor T 1997 *Phys. Rev. Lett.* **78** 2256

[7] Biham E and Mor T 1997 *Phys. Rev. Lett.* **79** 4034

[8] Biham E, Boyer M, Brassard G, van de Graaf J and Mor T 1998 *Security of Quantum Key Distribution Against All Collective Attacks (Los Alamos e-print archive)* quant-ph/9801022

[9] Biham E, Boyer M, Boykin P O, Mor T and Roychowdhury V 1999 *A Proof of the Security of Quantum Key Distribution (Los Alamos e-print archive)* quant-ph/9912053

[10] Mayers D 1996 *Advances in Cryptology, Proc. Crypto '96* (Berlin: Springer) p 343 (*Los Alamos e-print archive* quant-ph/9606003)

[11] Mayers D 1998 *Unconditional security in Quantum Cryptography (Los Alamos e-print archive)* quant-ph/9802025v4

[12] Lo H-K and Chau H F 1999 *Science* **283** 2050

[13] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[14] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863

[15] Yuen H P 1996 *Quantum Semiclass. Opt.* **8** 939

[16] Dušek M, Haderka O and Hendrych M 1999 *Opt. Commun.* **169** 103

[17] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304

[18] Brassard G, Lütkenhaus N, Mor T and Senders B C 2000 *Phys. Rev. Lett.* **85** 1330

[19] Dušek M, Jahma M and Lütkenhaus N 2000 *Phys. Rev.* A **62** 022306

[20] Kwiat P G, Mattle K, Weinfurter H, Zeilinger A, Sergienko A V and Shih Y 1995 *Phys. Rev. Lett.* **75** 4337

[21] Kwiat P G, Waks E, White A G, Appelbaum I and Eberhard P H 1999 *Phys. Rev.* A **60** R773

[22] Walls D F and Milburn G J 1994 *Quantum Optics* (Heidelberg: Springer) p 84

[23] Rarity J G, Owens P C M and Tapster P R 1994 *J. Mod. Opt.* **41** 2435

[24] Ribordy G, Brendel J, Gautier J-D, Gisin N and Zbinden H 2001 *Phys. Rev.* A **63** 012309