Multi-pair signal states in entanglement-based quantum cryptography

Miloslav Dušek[a] and Kamil Brádler[b]

[a]Department of Optics, Palacký University, 17. listopadu 50, 772 00 Olomouc, Czech Republic
[b]Department of Chemical Physics and Optics, Charles University, Ke Karlovu 3, 121 16 Prague 2, Czech Republic

ABSTRACT

Pairs of entangled photons can be employed for quantum key distribution. For each bit exactly one pair of photons is needed. Unfortunately, the quantum states produced by real sources, like a parametric down conversion, contain also terms with more than only one photon pair. We discuss several aspects of the use of such states for quantum key distribution. 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. However, the most important result is that an individual eavesdropping on multi-pair signals increases the error rate. This fact represents the important advantage of the entanglement-based quantum key distribution.

Keywords: Quantum Cryptography, Down Conversion, Entanglement

1. INTRODUCTION

Conventional cryptography knows the only provably secure cipher – the Vernam cipher (or one-time pad).[1] However, this cipher requires both communicating parties to share a secret key of the same length as the message. Secure key distribution had represented a crucial problem that has been solved only on the ground of quantum physics. The first protocol for quantum key distribution (QKD) was devised by Bennett and Brassard[2] (BB84) following Wiesner's ideas.[3] The eavesdropping is detectable because non-orthogonal quantum states are used for communication. Another protocol, inspired by Bell's inequalities, was proposed by Ekert.[4] It relies on nonclassical correlations of two quantum particles. Later this protocol was simplified by Bennett *et al.*[5] in the following way: 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. Both Alice and Bob choose randomly between two conjugated measurement basis, e.g., two linear-polarization basis that are mutually rotated by 45°. When Alice and Bob compare (publicly) the bases they have used they can establish a shared key made up from those signals where the measurement devices gave correlated results. This is the so called sifted key.

The crucial point is the unconditional security of QKD. For ideal systems the proofs of security against collective and joint attacks were given.[6–9] Later, proofs of security of BB84, even in the presence of noise, have been obtained.[10–13] For practical protocols security analysis is in progress.[14–20]

Photon pairs with correlated polarizations can be prepared, e.g., by parametric down conversion of type II[21] or using two down-conversion crystals with phase matching of type I.[22] Quantum states generated by these two methods should be the same in principle. Unfortunately, these techniques never produce exactly a single pair of photons. For concreteness let us look at the system with two non-linear crystals. Orientations of the optical axes of the 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 aiming to Alice, the other to Bob. The first crystal generates beams with horizontal polarizations, the second one beams with vertical polarizations. Quantum state generated by one crystal can be described[23] as

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

where $|n\rangle$ are corresponding number states and ξ and g are constants depending on the details of the preparation process. The total quantum state originating from both the crystals is then

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

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 signal state can jeopardize the security of QKD. An eavesdropper (*Eve*) can "split" these signals and learn something about the key. Similar difficulties implied by the use of weak coherent states in combination with a lossy line has been pointed out earlier.[14–19] A comprehensive analysis of security aspects of practical quantum cryptosystems taking into account the source imperfections were done in Ref..[18] But the role of down-conversion sources was reduced just to the preparation of approximate single photon states there. In the present paper we will go beyond this limitation by considering the entanglement-based QKD (see also[24]).

2. INTRINSIC ERROR RATE

Let us consider the configuration for QKD as in Fig. 1. We will suppose that $g \ll 1$ so that all terms containing more than two pairs can be neglected in Eq. (2):

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

Here we have used notation

$$|m,m,n,n\rangle = |m\rangle_{AV} \, |m\rangle_{BV} \, |n\rangle_{AH} \, |n\rangle_{BH} = \frac{1}{m!n!} \left[\left(\mathsf{a}_{AV}^{\dagger} \mathsf{a}_{BV}^{\dagger} \right)^m \left(\mathsf{a}_{AH}^{\dagger} \mathsf{a}_{BH}^{\dagger} \right)^n \right] |\mathrm{vac}\rangle \tag{5}$$

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

In the diagonal basis "$\times$", represented by the following creation operators

$$\begin{aligned} \mathsf{a}_X^{\dagger} &= (\mathsf{a}_V^{\dagger} + \mathsf{a}_H^{\dagger})/\sqrt{2}, \\ \mathsf{a}_Y^{\dagger} &= (\mathsf{a}_V^{\dagger} - \mathsf{a}_H^{\dagger})/\sqrt{2}, \end{aligned} \tag{6}$$

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).

Loss on the channel and efficiencies of Alice's and Bob's detectors are modelled by beam splitters 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:

$$\mathsf{P}_{\text{no}} = |0\rangle\langle 0| + \sum_{n=1}^{\infty} (1-\eta)^n |n\rangle\langle n| \qquad \text{and} \qquad \mathsf{P}_{\text{yes}} = \sum_{n=1}^{\infty} [1-(1-\eta)^n] |n\rangle\langle n|, \tag{7}$$

where η is a detector efficiency. The noise is neglected.

Our task is to show that if the detector efficiencies are lower than 100 % the use of signal states (4) inevitably causes errors in the sifted key. First, we will calculate the average relative length of the sifted key (with respect to the number of all generated entangled states). Of course, only those measurements contribute to the key when

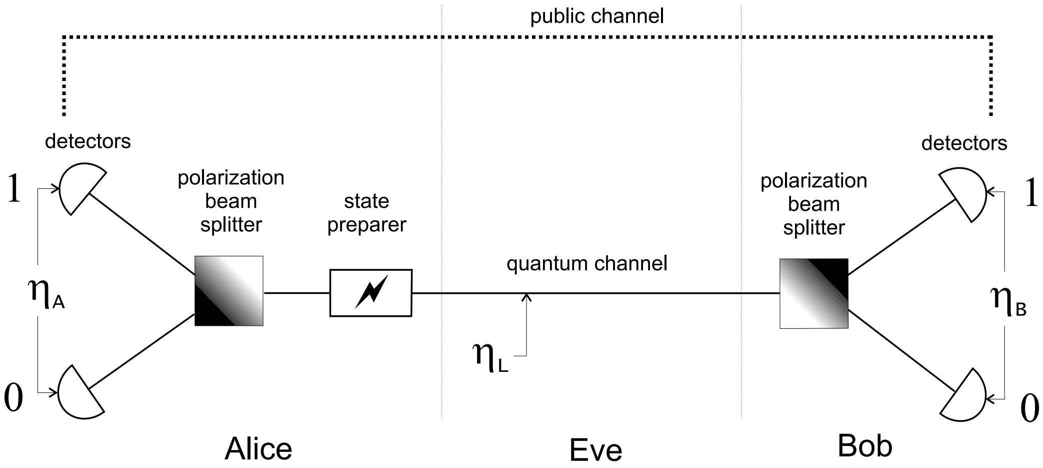

Figure 1. Arrangement for QKD. The signal states are prepared by the source situated at Alice's side. Both Alice and Bob have detectors that cannot distinguish the number of impinging photons and whose detection efficiencies are η_A and η_B, respectively. Alice and Bob change between two orientations of their polarization analyzers: "+" and "×". The both parties are connected by a quantum channel with transmittance η_L. This channel is accessible to Eve. Alice and Bob also communicate through the public channel. Eve can listen there but cannot manipulate it.

Alice and Bob have set the same polarization bases. Further, Alice and Bob include in the key only those events in which *exactly one* detector fires at each side. The average relative length of the sifted key is then given by the formula

$$\begin{aligned} R_{\mathrm{key}} &= \frac{1}{2}\langle\Psi|\,(\mathsf{P}^{AV}_{\mathrm{yes}}\mathsf{P}^{AH}_{\mathrm{no}}\mathsf{P}^{BV}_{\mathrm{yes}}\mathsf{P}^{BH}_{\mathrm{no}} + \mathsf{P}^{AV}_{\mathrm{no}}\mathsf{P}^{AH}_{\mathrm{yes}}\mathsf{P}^{BV}_{\mathrm{no}}\mathsf{P}^{BH}_{\mathrm{yes}} + \mathsf{P}^{AV}_{\mathrm{yes}}\mathsf{P}^{AH}_{\mathrm{no}}\mathsf{P}^{BV}_{\mathrm{no}}\mathsf{P}^{BH}_{\mathrm{yes}} + \mathsf{P}^{AV}_{\mathrm{no}}\mathsf{P}^{AH}_{\mathrm{yes}}\mathsf{P}^{BV}_{\mathrm{yes}}\mathsf{P}^{BH}_{\mathrm{no}})\,|\Psi\rangle \\ &\approx \xi^4 g^2\left\{\eta_A\eta_B\eta_L + g^2\left[1-(1-\eta_A)^2\right]\left[1-(1-\eta_B\eta_L)^2\right] + 2g^2\eta_A(1-\eta_A)\,\eta_B\eta_L(1-\eta_B\eta_L)\right\} \qquad (8) \end{aligned}$$

(indices AV denote Alice's detector for vertical polarization, BH Bob's detector for horizontal polarization, etc.). The first term in 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 $|1,1,1,1\rangle$.

The relative number of errors, i.e. events when Alice gets a bit different from that detected by Bob, is

$$R_{\mathrm{err}} = \frac{1}{2}\langle\Psi|\,(\mathsf{P}^{AV}_{\mathrm{yes}}\mathsf{P}^{AH}_{\mathrm{no}}\mathsf{P}^{BV}_{\mathrm{no}}\mathsf{P}^{BH}_{\mathrm{yes}} + \mathsf{P}^{AV}_{\mathrm{no}}\mathsf{P}^{AH}_{\mathrm{yes}}\mathsf{P}^{BV}_{\mathrm{yes}}\mathsf{P}^{BH}_{\mathrm{no}})\,|\Psi\rangle \approx \xi^4 g^4\eta_A(1-\eta_A)\,\eta_B\eta_L(1-\eta_B\eta_L). \qquad (9)$$

Now we can calculate the error rate:

$$\begin{aligned} \varepsilon &= \frac{R_{\mathrm{err}}}{R_{\mathrm{key}}} \approx \frac{g^2(1-\eta_A-\eta_B\eta_L+\eta_A\eta_B\eta_L)}{1+g^2(6-4\eta_A-4\eta_B\eta_L+3\eta_A\eta_B\eta_L)} \\ &= \frac{(1-\eta_A)(1-\eta_B\eta_L)}{2}\mu + \mathcal{O}(\mu^2). \qquad (10) \end{aligned}$$

If $\eta_L \ll \eta_A, \eta_B$ then $\varepsilon \approx (1-\eta_A)\,\mu/2$.

3. THE AMOUNT OF LEAKED INFORMATION

In this section we will analyze the situation when Eve try to get some information on the key (only) from "multi-particle" (or "multi-pair") signals. 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 (or more) photons. 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 key-generation rate). After Alice and Bob has compared their measurement bases Eve will make a polarization measurement on the stored photons.

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

$$I_E = \sum_i r_i \left[1 + p_i \log_2 p_i + (1-p_i)\log_2(1-p_i)\right], \tag{11}$$

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

In the following we will compare the amount of information that can be obtained by Eve from multi-pair or multi-particle signals (by means of a photon-number-splitting attack) for different cryptographic schemes.

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]

$$R_{\mathrm{exp}} = \frac{1}{2}\left[1 - \exp(-\eta_L\eta_B\mu')\right],$$

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

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

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

$$I_E^{(\mathrm{WCP})} = \begin{cases} 1 & \text{if } R_{\mathrm{exp}} \le R_{\mathrm{multi}}, \\ \dfrac{R_{\mathrm{multi}}}{R_{\mathrm{exp}}} \approx \dfrac{1}{2\eta_L\eta_B}\mu', & \text{otherwise.} \end{cases} \tag{12}$$

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 key-generation rate. Thus, 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 we will calculate what information may leak to Eve if a parametric down-conversion (PDC) source of "single" photons is used instead of a laser (that produces coherent states). 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 states produced by such a down-conversion source are used for BB84 QKD protocol in the same manner as WCS.[18]

The expected average relative length of the sifted key (in proportion to the number of all generated entangled states) is given by the formula

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

The average relative number of “multi-photon” signals reads

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

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 (it can be done exactly but for our purposes the used approximation is good enough)

$$I_E^{\rm (PDC)} = \begin{cases} 1 & \text{if } \; R_{\rm exp} \le R_{\rm multi}, \\ \dfrac{R_{\rm multi}}{R_{\rm exp}} \approx \dfrac{2-\eta_A}{\eta_L \eta_B} \mu'', & \text{otherwise}, \end{cases} \tag{13}$$

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

3.3. Entanglement-based protocol

Finally let us look at the cryptographic scheme fully based on the entanglement of photon polarizations (EPP). Its scheme is in Fig. 1. Signal states are described by Eq. (2). The detectors are of “yes/no” type again; on Alice’s side they have efficiencies η_A, on Bob’s side η_B.

Now the situation is more complex. It becomes important how many photons Eve separates. However, we will confine ourselves only to the simplified case when at most two pairs are present with a reasonable probability [see Eq. (4)]. Then Eve can separate no more than one photon and send remaining one to Bob. In contrast to the two previous cases, here 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 Eq. (8): $R_{\rm exp} = R_{\rm key}$. A portion of two-photon signals leaving Alice’s terminal (those signals that can be read by Eve applying PNS attack) is

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

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 $|1,1,1,1\rangle$.

Applying PNS attack Eve does not learn all bits with certainty now. The reason is that she cannot distinguish the signals stemming from the states $|1,1,1,1\rangle$ from the other two-photon signals. For these particular signals she hits Alice’s bit only with probability 50 % and Bob’s bit values are even always opposite to hers. This must be taken into account when the information leaked to Eve is calculated. Thus Eve’s average information

$$I_j^{\rm (EPP)} \approx \begin{cases} f(p_j) & \text{if } \; R_{\rm exp} \le R_{\rm double}, \\ \dfrac{R_{\rm double}}{R_{\rm exp}} f(p_j) \approx \dfrac{3-2\eta_A}{2\eta_L \eta_B} f(p_j)\, \mu, & \text{otherwise}, \end{cases} \tag{14}$$

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, read

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

If $\eta_A < 1$ the following inequality holds: $I_{EB} < I_{AE} < 1$. Unfortunately, the fact that the maximum Eve’s information is lower than unity does not mean any real advantage because for $R_{\rm exp} \le R_{\rm double}$ the information I_{AE} is equal to the information shared by Alice and Bob, $I_{AB} = 1 + \varepsilon' \log_2 \varepsilon' + (1-\varepsilon')\log_2(1-\varepsilon')$, where ε' is given by Eq. (15).

Let us focus our attention to the error rate now. The very important feature of PNS eavesdropping in EPP systems should be noticed: If Eve applies PNS attack in the way described above, i.e., if she tries to reproduce only the key-generation rate ($R_{\rm exp}$), she *increases* the error rate inevitably. The reason is that she increases the fraction of $|1,1,1,1\rangle$ contributions to the key bits. If Eve has substantially decreased 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

$$R_{\rm err}^{(E)} = \xi^4 g^4 \eta_A (1-\eta_A)/2.$$

Thus due to eavesdropping the error rate grows to

$$\varepsilon' = \begin{cases} \dfrac{R_{\rm err}^{(E)}}{R_{\rm double}} \approx \dfrac{1-\eta_A}{6-4\eta_A}, & \text{if } \ R_{\rm exp} \leq R_{\rm double}, \\[2ex] \dfrac{R_{\rm err}^{(E)}}{R_{\rm exp}} \approx \dfrac{1-\eta_A}{4\eta_B\eta_L}\mu. & \text{otherwise,} \end{cases} \tag{15}$$

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. CONCLUSIONS

We have discussed the effect of the presence of "multi-pair signals" on the security of entanglement-based quantum cryptography. There is an important difference between the quantum-cryptographic setup that uses parametric down conversion just as a "triggered source of photons" and that which employs the entanglement directly for quantum key distribution. In the latter case a nonzero error rate exists even if no eavesdropper is present. This is caused by the joint effect of the occurrence of "multi-pair signals" and of low detection efficiencies. However, the most interesting finding is that the individual eavesdropping on "multi-pair signals" increases the error rate. This feature increases the chance to detect the eavesdropper.

ACKNOWLEDGMENTS

This research was supported by the Ministry of Education of the Czech Republic, projects LN00A015 and RN19982003012.

REFERENCES

1. G.S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Journal of the American Institute of Electrical Engineers* **45**, pp. 109–115, 1926.
2. C.H. Bennett and G. Brassard, "Quantunl cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pp. 175–179, IEEE, New York, 1984.
3. S. Wiesner, "Conjugate coding," *SIGACT News* **15**, p. 78–88, 1983.
4. A.K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.* **67**, pp. 661–663, 1991.
5. C.H. Bennett, G. Brassard, N.D. Mermin, "Quantum cryptography without Bell's theorem," *Phys. Rev. Lett.* **68**, pp. 557–559, 1992.
6. E. Biham and T. Mor, "Security of Quantum Cryptography against Collective Attacks," *Phys. Rev. Lett.* **78**, pp. 2256–2259, 1997.
7. E. Biham and T. Mor, "Bounds on Information and the Security of Quantum Cryptography," *Phys. Rev. Lett.* **79**, pp. 4034–4037, 1997.
8. E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, "Security of Quantum Key Distribution Against All Collective Attacks," Los Alamos e-print archive `quant-ph/9801022`, 1998.
9. E. Biham, M. Boyer, P.O. Boykin, T. Mor, and V. Roychowdhury, "A Proof of the Security of Quantum Key Distribution," Los Alamos e-print archive `quant-ph/9912053`, 1999.

10. D. Mayers, "Quantum Key Distribution and String Oblivious Transfer in Noisy Channels," in: *Advances in Cryptology – Proceedings of Crypto '96*, p. 343, Springer, Berlin, 1996; Los Alamos e-print archive `quant-ph/9606003`, 1996;
11. D. Mayers, "Unconditional Security in Quantum Cryptography," Los Alamos e-print archive `quant-ph/9802025v4`, 1998;
12. H.-K. Lo and H. F. Chau, "Unconditional Security of Quantum Key Distribution over arbitrarily long distances," *Science* **283**, pp. 2050–2056, 1999.
13. P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.* **85**, pp. 441–444, 2000.
14. B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A* **51**, pp. 1863–1869, 1995.
15. H. P. Yuen, "Quantum amplifiers, quantum duplicators and quantum cryptography," *Quantum Semiclassic. Opt.* **8**, pp. 939–949, 1996.
16. M. Dušek, O. Haderka, and M. Hendrych, "Generalized beam-splitting attack in quantum cryptography with dim coherent states," *Opt. Comm.* **169**, pp. 103–108, 1999.
17. N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A* **61**, 052304, 2000.
18. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Senders, "Limitations on Practical Quantum Cryptography," *Phys. Rev. Lett.* **85**, pp. 1330–1333, 2000.
19. M. Dušek, M. Jahma, N. Lütkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," *Phys. Rev. A* **62**, 022306, 2000.
20. H. Inamori, N. Lütkenhaus, D. Mayers, "Unconditional Security of Practical Quantum Key Distribution," Los Alamos e-print archive `quant-ph/0107017`, 2001.
21. P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New High-Intensity Source of Polarization-Entangled Photon Pairs," *Phys. Rev. Lett.* **75**, pp. 4337–4341, 1995.
22. P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, "Ultrabright source of polarization-entangled photons," *Phys. Rev. A* **60**, pp. R773–R776, 1999.
23. D. F. Walls and G. J. Milburn, *Quantum Optics*, p. 84, Springer-Verlag, Heidelberg, 1994.
24. M. Dušek and K. Brádler, "The effect of multi-pair signal states in quantum cryptography with entangled photons," *J. Opt. B: Quantum Semiclass. Opt.* **4**, pp. 109–113, 2002.