Secure Communication with a Publicly Known Key

A. BEIGE[a], B.-G. ENGLERT[a,b], CH. KURTSIEFER[c]
AND H. WEINFURTER[a,c]

[a]Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1
85748 Garching, Germany

[b]Departments of Mathematics and Physics, Texas A & M University
College Station, Texas 77843, U.S.A.

[c]Sektion Physik, Universität München, Schellingstrasse 4
80799 München, Germany

We present a scheme for direct and confidential communication between Alice and Bob, where there is no need for establishing a shared secret key first, and where the key used by Alice even will become known publicly. The communication is based on the exchange of single photons and each and every photon transmits one bit of Alice's message without revealing any information to a potential eavesdropper.

PACS numbers: 03.67.Dd, 42.79.Sz

1. Introduction

It is generally believed that cryptography schemes are only completely secure when the two communicating parties, *Alice* and *Bob*, establish a shared secret key before the transmission of a message. This means they first have to create a random bit sequence, which is not known to anyone else, and which is of the same length as the message. In order to communicate, Alice then multiplies the bits of the message one by one with the key bits. When she announces the result to Bob, or even publicly, then he is the only one who can interpret it and deduce Alice's message.

As shown in a seminal paper by Bennett and Brassard in 1984 [1], Alice and Bob can establish a shared secret key by exchanging single qubits, physically realised by the polarisation of photons, for example. The protocol of the proposed

scheme, that became known as BB84, is as follows. First, Alice prepares a photon in a certain polarisation state, a basis vector in a two-dimensional Hilbert space. Thereby she chooses at random between two complementary bases. Afterwards she forwards the photon to Bob who now performs a measurement on the incoming state. If he chooses the same basis as Alice, which happens with a chance of 50%, they can agree about one key bit. At the end of a transmission they check whether it was secure or not by just comparing some key bits. An eavesdropper can be noticed because his interception causes an error rate of at least 25%.

In 1987 Vaidman, Aharonov and Albert published a paper [2] with the title "How to ascertain the values of σ_x, σ_y, and σ_z of a spin-1/2 particle" and described a paradox that later became known as the *Mean King's Problem* [3]. The quantum-optical version of the king's problem proposed recently [4] suggests a new cryptography scheme, presented in Refs. [5, 6]. In the present paper we focus on a further development, namely a modification that allows Alice to send a message to Bob without the need to establish a shared secret key first.

The protocol of this new scheme has, of course, many similarities to BB84 [1], its later modifications [7–9] and the proposal made by Ekert in 1991 based on entangled photon pairs [10]. But it is much more than just another modification. In contrast to BB84 and its various "analytical continuations", which are *probabilistic*, the scheme we describe here is *deterministic*. Each and every photon sent and detected will eventually contribute a key bit. In addition, and this is another important requirement for direct and confidential communication, no information is revealed to a potential eavesdropper. The only other proposal with deterministic features is the one of Goldenberg and Vaidman [11].

Altogether, the transmission of a message becomes more efficient than in other schemes. The price to be paid for this efficiency raise is that each photon now has to be prepared in a two-qubit state and not only in a single-qubit state. To obtain these states Alice can use, for instance, the spatial binary alternative of a photon with the basis states $|R\rangle$ and $|L\rangle$ and the two polarisations $|v\rangle$ and $|h\rangle$. Here, $|R\rangle$ and $|L\rangle$ describe a photon traveling either in the "right" fiber or in the "left" fiber. How any desired superposition of such two-qubit photon states can be prepared is described in Ref. [4].

In the next section we summarise the basic idea that can be used to construct direct confidential quantum communication schemes. In Sec. 3 we describe concrete proposals for its realisation. The security against eavesdropping attacks of the general intercept-resent kind is addressed in Sec. 4. After discussing a possible experimental setup, we conclude with a summary of our results.

2. The basic idea

In this section we describe the essential ingredients needed for quantum cryptography. The basic protocol that all schemes have in common is the following:

Alice (the sender) exchanges single qubits with Bob (the receiver), each of them prepared in a certain state. As usual she chooses at random between different types of states labeled by n. Here we choose the notation such that states transmitting a "+" bit are denoted by $|n_+\rangle$. In order to transmit a "−" bit Alice prepares the state $|n_-\rangle$. If a photon arrives at Bob's end, he performs a measurement on its state whereat he switches at random between at least two different measurement bases. In the following, there will always be only two different measurements he can choose and we denote the corresponding basis states by $|B_n\rangle$ or $|C_n\rangle$.

As in Refs. [5, 6], let us call the eavesdropper *Evan*. He has full access to all communication channels between the two parties. This means, he can perform any possible quantum mechanical operation on the photons in transmission and he can listen into the classical communication between Alice and Bob. Security of the scheme is assured when Evan's presence leads to a significantly increased error rate in the bit transmission. At the end of a transmission, Alice and Bob compare some of their bits to test whether this rate is above a certain percentage limit or not. If not, Alice announces the encrypted message via a classical communication channel or even publicly.

Up to now, our description applies to any quantum cryptography scheme. If Alice and Bob want to have a scheme to establish a shared secret key, the states $|n_\pm\rangle$, $|B_n\rangle$, and $|C_n\rangle$ only have to fulfill the condition that Bob can, at least in some cases, deduce which bit Alice sent from the knowledge of n and the corresponding outcome of his measurement. In BB84, this applies to 50% of the photons which then provide one key bit each. Whether Evan can gain any knowledge about the bits in transmission or not does not matter. Alice and Bob only use the key sequence they created if they can verify the absence of any eavesdropping attempts.

To obtain a more efficient scheme, Alice and Bob should maximise the rate of photons they can use to establish a key bit. One can even assure that Bob *always* knows whether Alice sent a "+" or a "−" bit by using a four-dimensional Hilbert space [5, 6]. This is the case, when a photon in $|n_+\rangle$ cannot cause the same measurement outcome as a photon in $|n_-\rangle$. For instance, if $n = 3$ and Bob found $|C_2\rangle$ and knows that $|C_2\rangle$ overlaps with the state $|3_+\rangle$, but not with $|3_-\rangle$, then he obtains a "+" bit. Thus every one of Bob's measurements matches with whatever state Alice prepared and the scheme is deterministic.

If Alice and Bob want to communicate directly and confidentially, then there is another condition that has to be fulfilled: Whatever operation Evan performs on the photon state, he should not be able to gain any information about the bit in transmission. Let us assume that Alice uses all state pairs with the same frequency. To find out whether a photon carries a "+" or a "−" bit, Evan has to answer the question whether its state belongs to the subspace spanned by all $|n_+\rangle$ states or to the subspace spanned by all $|n_-\rangle$ states. If

$$\sum_n |n_+\rangle\langle n_+| = \sum_n |n_-\rangle\langle n_-|, \tag{1}$$

then these two subspaces are completely indistinguishable and the bit in transmission is perfectly concealed in the state space.

3. A concrete scheme for direct communication

In this section we present a concrete scheme for direct communication between Alice and Bob. To do so let us assume that

$$|n_+\rangle \equiv |B_n\rangle \quad \text{and} \quad |n_-\rangle \equiv |C_n\rangle. \tag{2}$$

Then the states $|n_+\rangle$ and $|n_-\rangle$, respectively, evenly span the whole Hilbert space and clearly fulfill condition (1). They equal either one or the other measurement basis of Bob. Note that such a coding is different to BB84 and its modifications, where the states $|n_+\rangle$ and $|n_-\rangle$ always belong to the same set of basis states.

To assure that Bob always knows how to interpret his measurement result there should be no overlap between basis states with the same index n, i.e.

$$\langle B_n | C_n \rangle = 0. \tag{3}$$

If Bob finds the photon, for instance, in $|B_m\rangle$ with $m \neq n$, then he knows immediately that Alice prepared it in $|n_-\rangle$. The reason is that a photon in $|n_+\rangle$ cannot cause a "click" at this detector. Otherwise, if n coincides with m, then he knows that he received a "+" bit. This tells him that he measured the same basis as the one used by Alice to prepare the photon state.

The protocol for direct and confidential communication originating from this ansatz is the following: First, Alice creates a random succession of ciphers n that will serve as her cryptographic key. The length of this sequence should coincide with the length of her message. Depending on whether she wants to transmit a "+" bit or a "–" bit next, she prepares the photon either in $|B_n\rangle$ or in $|C_n\rangle$ with n according to the next number of her key and sends it to Bob. Bob measures at random either the B or the C basis on each incoming photon. After Alice and Bob assured each other that the transmission was secure (how well this can be done is discussed in the next section), Alice publicly announces her key. In doing so, she reveals the message to Bob.

Up to now, we have not yet answered the question, what the B and C basis should look like. Let us assume here that Alice and Bob use single photon two-qubit states [4]. Then all states are part of a four-dimensional Hilbert space but our results can also be carried over easily to higher dimensions. Note, that is not possible to find a non-trivial solution to Eqs. (2) and (3) in less than four dimensions, this means a solution for which the states $|C_n\rangle$ are not just a permutation of the states of the B basis.

In the following, we denote the basis transformation that rotates the B basis into the C basis by $\boldsymbol{A}$ and write

$$(|C_1\rangle, |C_2\rangle, |C_3\rangle, |C_4\rangle) = (|B_1\rangle, |B_2\rangle, |B_3\rangle, |B_4\rangle)\boldsymbol{A}. \tag{4}$$

Condition (3) is then fulfilled if the unitary 4×4 matrix $\boldsymbol{A}$ has only vanishing diagonal elements. Besides this, there are no other restrictions on $\boldsymbol{A}$ and there are many choices Alice and Bob can make. For symmetry reasons, let us assume that $\boldsymbol{A}$ is not only unitary but also Hermitian. Then the inverse of the transformation (4) is also furnished by $\boldsymbol{A}$.

It is sufficiently general to consider matrices of the form

$$\boldsymbol{A} = \mathrm{i} \begin{pmatrix} 0 & a_1 & a_2 & a_3 \\ -a_1 & 0 & a_3 & -a_2 \\ -a_2 & -a_3 & 0 & a_1 \\ -a_3 & a_2 & -a_1 & 0 \end{pmatrix} \tag{5}$$

where the parameters a_i are real and fulfill the normalisation constraint

$$a_1^2 + a_2^2 + a_3^2 = 1. \tag{6}$$

Thus, Alice and Bob have two free parameters which they can choose to their liking. Bob's probabilities to find the incoming photon in a certain state are summarised in Table.

TABLE

Bob's probability to find a certain measurement outcome for the scheme corresponding to Eq. (5).

Alice's photon state	Measurement outcome at Bob's end							
	B_1	B_2	B_3	B_4	C_1	C_2	C_3	C_4
1_+	1	0	0	0	0	a_1^2	a_2^2	a_3^2
2_+	0	1	0	0	a_1^2	0	a_3^2	a_2^2
3_+	0	0	1	0	a_2^2	a_3^2	0	a_1^2
4_+	0	0	0	1	a_3^2	a_2^2	a_1^2	0
1_-	0	a_1^2	a_2^2	a_3^2	1	0	0	0
2_-	a_1^2	0	a_3^2	a_2^2	0	1	0	0
3_-	a_2^2	a_3^2	0	a_1^2	0	0	1	0
4_-	a_3^2	a_2^2	a_1^2	0	0	0	0	1

In the next two sections we will see that the fully symmetric choice

$$a_1 = a_2 = a_3 = 1/\sqrt{3} \tag{7}$$

maximises the error rate that a potential eavesdropper introduces in the bit transmission between Alice and Bob. Another solution is to choose

$$a_1 = a_2 = 1/\sqrt{2} \quad \text{and} \quad a_3 = 0. \tag{8}$$

In this case, the experimental implementation of the corresponding scheme is particularly simple, see in Sec. 5 below. To prepare a photon in one of the states of the B and the C basis does not require to produce entanglement between the two

degrees of freedom, the spatial coordinates and the polarisation, of the photon. Nevertheless, the error rate introduced by an eavesdropper is still relatively large.

Finally, we would like to convince ourselves that whatever the parameters a_i are, it is indeed impossible for Evan to gain any information without the knowledge of Alice's key. The reason is that the states $|n_+\rangle$ (and $|n_-\rangle$, respectively) equally span the whole Hilbert space. As long as Alice chooses equally likely between the four possible values of n, she prepares the ensemble of photons with a "+" bit in the mixed state that is given by the (normalised) identity matrix. The same applies to the ensemble of photons that carry a "−" bit. Thus whatever Evan measures, the probability to find the photon in a certain state always equals 1/4 and finding a certain state does not reveal any information to Evan.

4. Security against intercept-resent attacks

The security of the scheme we present here results from the fact that Alice does not reveal her key before she is not convinced that no eavesdropper has been listening in. To test whether this is the case or not, Alice and Bob proceed as follows: Alice intersperses her message with a fair number of control bits at random positions and of random values. Only Alice knows which ones are the control bits and which ones the message bits. After the transmission of all photons, she tells Bob which photons carried control bits and he tells her in which state he found them. If Alice verifies that Bob's findings are consistent with what she sent, then they conclude that the transmission was secure. Otherwise, if the error rate is above a certain percentage level, they should not trust in the security of their communication and Alice should repeat her transmission using a different cryptographic key.

Let us now imagine that Evan is listening in and determine the minimum error rate he causes in case of the setup described in the previous section. By doing so we do not care whether Evan can gain any information in this way or not, once Alice reveals her key. Let us assume, as usual, that Evan intercepts every photon and performs a measurement on it. Afterwards he forwards a replacement to Bob accordingly, namely in the two-qubit state that has the best chance of avoiding wrong detector clicks at Bobs end.

In the following we denote the states of Evan's measurement basis by $|E_k\rangle$. As explained at the end of the previous section, the probability to find the photon in a certain state always equals 1/4 and Evan cannot gain any information from his measurement. For simplicity we consider only the strategy in which Evan forwards the photon in exactly the same state he found it in. In this way he forwards it at least in a state that has some overlap with the state prepared by Alice. More general strategies in which Evan optimises the forwarded state can be analysed as well, but that is technically more demanding, and we are here content with referring the reader to the detailed discussion in [6].

The probability that Alice prepares her photon in $|n_+\rangle$ equals $1/8$ and the probability that Bob measures the B basis is given by $1/2$. In this case, an error occurs if Bob finds the photon in $|B_m\rangle$ with $n \neq m$. The contribution of this case to the total error probability is given by

$$\frac{1}{8} \cdot \frac{1}{2} \sum_k |\langle E_k | n_+ \rangle|^2 \sum_{m \neq n} |\langle E_k | B_m \rangle|^2 = \frac{1}{16} \left(1 - \sum_k |\langle E_k | B_n \rangle|^4 \right), \tag{9}$$

because the probability that Evan measures $|E_k\rangle$ is in this case $|\langle E_k | n_+ \rangle|^2$ whilst $|\langle E_k | B_m \rangle|^2$ is the probability that Bob finds the photon afterwards in $|B_m\rangle$. Analogously, one finds that the contribution to the error rate is given by

$$\frac{1}{16} \sum_k |\langle E_k | n_+ \rangle|^2 |\langle E_k | n_- \rangle|^2 = \frac{1}{16} \sum_k |\langle E_k | B_n \rangle|^2 |\langle E_k | C_n \rangle|^2, \tag{10}$$

if Bob measures the C basis instead of the B basis. In this case an error occurs only if Bob finds the photon in $|n_-\rangle$. Calculating the contributions to the total error rate when Alice prepares the photon in the state $|n_-\rangle$ leads to the same result but with $|B_n\rangle$ replaced by $|C_n\rangle$ and vice versa.

To calculate the total error rate P_{error} one has to sum over all contributions and all possible values of n. Doing so leads to

$$P_{\text{error}} = \sum_n \left[\frac{1}{8} - \frac{1}{16} \sum_k (|\langle E_k | B_n \rangle|^4 + |\langle E_k | C_n \rangle|^4 + 2|\langle E_k | B_n \rangle|^2 |\langle E_k | C_n \rangle|^2) \right]$$

$$= \frac{1}{2} - \frac{1}{16} \sum_n \sum_k \left(|\langle E_k | B_n \rangle|^2 - |\langle E_k | C_n \rangle|^2 \right)^2. \tag{11}$$

Evan's task of minimising the error rate so reduces to the task of minimising this expression. Using the notation

$$|E_k\rangle = \sum_m e_m |m_+\rangle \tag{12}$$

and Eqs. (2–5) we find that

$$P_{\text{error}} \geq \frac{1}{2} - \frac{1}{16} \sum_n (1 + a_1^4 + a_2^4 + a_3^4) \sum_m |e_m|^4 \tag{13}$$

by neglecting all negative terms in the round brackets at the right hand side of Eq. (11), that is the terms that stem from Eq. (10). The state $|E_k\rangle$ is normalised and its coefficients e_m obey the inequality $\sum_m |e_m|^4 \leq \sum_m |e_m|^2 = 1$. This leads to the result

$$P_{\text{error}} \geq \frac{1}{4}(1 - a_1^4 - a_2^4 - a_3^4). \tag{14}$$

For the optimal scheme corresponding to the parameters given in Eq. (7) the right hand side of this equation is $frac16 = 16.67\%$. For the scheme (8), the error rate introduced by Evan in the bit transmission is always above $\frac{1}{8} = 12.5\%$.

As it stands, this calculation applies only to strategies where Evan forwards the photon in the detected state, but not to those where the forwarded states are optimised for minimal error rates. It turns out, however, that these more sophisticated strategies do not yield error rates below these 16.67% or 12.5%, respectively. This is confirmed by the numerical data presented in Fig. 1 which reports error rates for random choices of Evan's measurement basis and forwarded states. The data demonstrate that the right hand side of Eq. (14) is indeed the lower bound of the error rate.
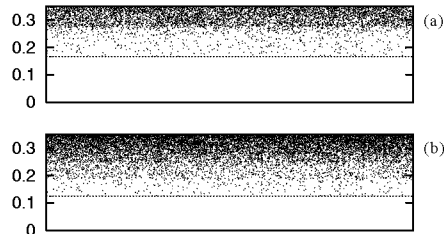
Fig. 1.   Error rate introduced by Evan into the bit transmission between Alice and Bob for the parameters chosen (a) as in Eq. (7), where it is always above 16.67%, and (b) for the parameters as in Eq. (8) where it is always above 12.5%. Each point corresponds to a different intercept-resent strategy whereat Evan's measurement basis and the state in which he forwards the photon to Bob have been acquired completely at random.

To derive Eq. (14) we neglected only terms proportional $|e_k|^2 |e_j|^2$ with $k \neq j$. An optimal strategy for Evan is therefore, for instance, to measure the B basis, i.e. to measure whether the incoming photon is in one of the states $|n_+\rangle$. This strategy also optimises eavesdropping with respect to maximising the information gain of Evan as soon as he gets to know the key. If Alice and Bob fail to notice his presence, he can intercept the whole transmitted message.

5. Proposal for an experimental realisation

We have seen in the previous section that the error rate introduced by an eavesdropper is always above 16.67% for the optimal choice of the parameters (7). This is not much larger than the minimum error rate of 12.5% which was found for the parameter choice of Eq. (8). In this section we discuss how the second scheme could be realised experimentally because its implementation is much simpler, although implementing the optimal scheme is also possible with the methods of [4]. To achieve the same degree of security in the second scheme, Alice and Bob must use about 40% more control bits.

Let us assume now that the vectors of the B basis are given by

$$(|B_1\rangle, |B_2\rangle, |B_3\rangle, |B_4\rangle) = (|Rv\rangle, |Lv\rangle, |Lh\rangle, |Rh\rangle). \tag{15}$$

Then the states of the C basis equal

$$(|C_1\rangle, |C_2\rangle, |C_3\rangle, |C_4\rangle) = i(-|Ls\rangle, |Rs\rangle, |Ra\rangle, -|La\rangle), \tag{16}$$

where

$$|s\rangle \equiv \frac{1}{\sqrt{2}}(|v\rangle + |h\rangle) \quad \text{and} \quad |a\rangle \equiv \frac{1}{\sqrt{2}}(|v\rangle - |h\rangle) \tag{17}$$

are the symmetric and the antisymmetric superposition of the basic polarisation states. Thus, the C basis differs from the states of the B basis only with respect to the possible polarisations of the photons. The phase factors $\pm i$ in Eq. (16) are a consequence of the conventions adopted at (5) and (8) and could as well be omitted. To prepare the states $|n\pm\rangle$, Alice could use any source that produces single photons on demand. For examples of experimental realisations of such sources see for instance Refs. [12–15].

If Alice wants to send a "+" bit to Bob, then she should prepare the photon at random in one of the four states on the right hand side of Eq. (15). To do so she chooses equally likely between the polarisations $|h\rangle$ and $|v\rangle$ and sends the photon either through a "left" or a "right" fiber. To send a "−" bit, Alice can proceed in the same way but should then change the polarisation of the outgoing photon before sending it to Bob. This can be done, for instance with the help of a half-way plate (HWP) that affects the polarisation of a photon such that $|s\rangle$ changes into $|v\rangle$ and $|a\rangle$ changes into $|h\rangle$, or vice versa. For practical realisations, electrically controllable Pockels-cells should be used.

A possible experimental setup for the transmission of "−" bits is sketched in Fig. 2. To deflect vertically polarised photons to one detector and horizontally polarised photons to another detector, Bob uses polarising beam splitters (PBS) whilst he changes the polarisation of a photon, like Alice, with the help of a HWP. In which state Bob finds a photon in case of a "click" is indicated in Fig. 2 by the two letters written next to the corresponding detector. At Bob's end, a beam splitter (BS) reroutes the photon either to a measurement of the B or the C basis.

Instead of using a "left" and a "right" fiber and two polarisation degrees of freedom, Alice and Bob could also utilise other parameters to create single photon two-qubit states. The two fibers can, for instance, be replaced by one fiber and Alice and Bob agree for each photon about two small time windows around a time t_L and a time t_R. If Alice sends the photon around t_L it means that she prepared it in the state $|L\rangle$, otherwise, if she sends the photon around t_R, she prepared it in $|R\rangle$. Alternatively, two degrees of freedom could also be obtained by exploiting different photon frequencies.

The scheme shown in Fig. 2 looks as if it were a combination of two BB84 schemes. But in fact it is not. The scheme is more efficient than what one would get by just combining two BB84 schemes naively. The reason is that the results are interpreted in a completely different way (see Sec. 3 and Table). In contrast to BB84, each and every photon sent by Alice transmits one bit and the scheme is therefore deterministic. In addition, the bit in transmission is concealed in such
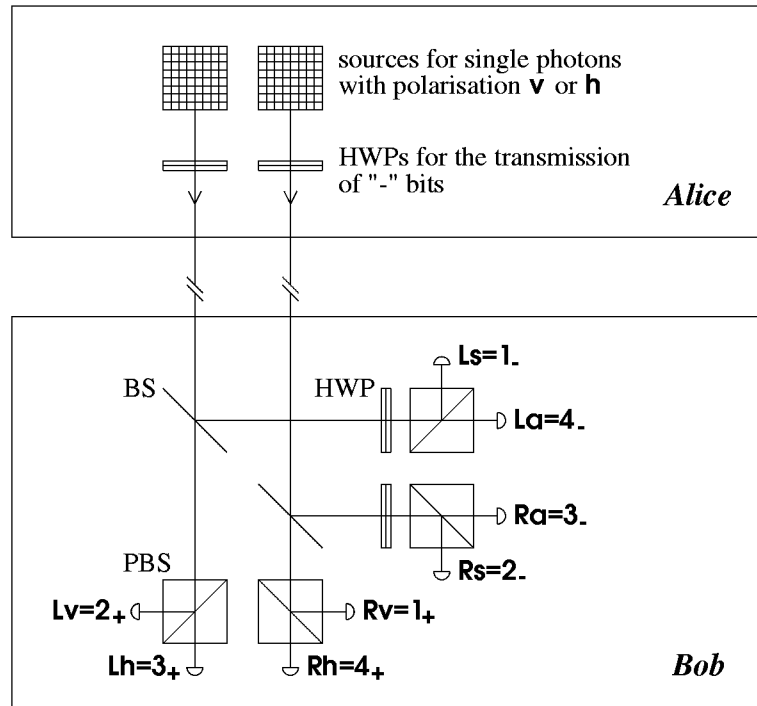
Fig. 2. A feasible experimental setup for the transmission of a "−" bit with single-photon two-qubit states. For an explanation of the optical elements see the text. To transmit "+" bits, the HWPs have to be turned around so that they do not change the polarisation of the outgoing photon. Otherwise, the experimental setup is exactly the same.

a way that an eavesdropper cannot gain any information by performing measurements on the photon state (which cannot be achieved in BB84), and Alice and Bob can communicate directly and confidentially.

6. Conclusions

In summary, we discussed a new scheme for direct and confidential communication between Alice and Bob in detail. While both parties exchange single bits (carried by photons) as in any other quantum cryptography scheme, the purpose of the bit transmission is completely different. Instead of establishing a shared secret key, which can be used later to encrypt a message, Alice can send her message directly. What requirements such schemes have to meet in general has been discussed in Sec. 1.

To encrypt her message, Alice creates a random sequence of ciphers — the cryptographic key. To transmit a "+" bit she prepares the photon in the state

$|n_+\rangle$, to transmit a "$-$" bit she prepares it in $|n_-\rangle$, whereat n always coincides with the next cipher of her key. After Alice and Bob verified that no eavesdropper was listening in, Alice can publicise her key without hesitation. She knows that Bob will be the only one who can decode her message, because he is the only one who received it. In this sense, the scheme realises quantum cryptography with a *publicly known* key.

In Sec. 2 and 3 we presented a concrete protocol based on single-photon two-qubit states and discussed its security against intercept-resent eavesdropping strategies. As in other schemes, security arises from the fact that the presence of an eavesdropper leads to a significantly increased error rate in the bit transmission. This rate can be determined by comparing some control bits with which Alice had interspersed the message before. Only when the measurement outcomes of Bob's side match with the states in which Alice prepared the control qubits, both parties should trust in the security of their communication and Alice can announce her cryptographic key.

By choosing the parameters that characterise the scheme suitably, Alice and Bob can assure that the error rate Evan introduces in the bit transmission is always above 16.67%. Nevertheless, in Sec. 5 we discussed possibilities for the experimental realisation of another scheme, one in which the error rate can be as low as 12.5%. The advantage of this scheme is that its implementation is much simpler, although implementing the optimal scheme is possible too.

Acknowledgment

References

[1] C.H. Bennett, G. Brassard, in: *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, Bangalore*, IEEE, New York 1984, p. 175.

[2] L. Vaidman, Y. Aharonov, D.Z. Albert, *Phys. Rev. Lett.* **58,** 1385 (1987).

[3] Y. Aharonov, B.-G. Englert, *Z. Naturforsch. A* **56,** 16 (2001).

[4] B.-G. Englert, C. Kurtsiefer, H. Weinfurter, *Phys. Rev. A* **63,** 032303 (2001).

[5] A. Beige, B.-G. Englert, C. Kurtsiefer, H. Weinfurter, quant-ph/0101066 (2001).

[6] A. Beige, B.-G. Englert, C. Kurtsiefer, H. Weinfurter, in: *Mathematics of Quantum Computation*, Eds. J.-L. Brylinski, G. Chen, CRC Press, Boca Raton 2002 (in press).

 [7] C.H. Bennett, *Phys. Rev. Lett.* **68,** 3121 (1992).

 [8] D. Bruß, *Phys. Rev. Lett.* **81,** 3018 (1998).

 [9] M. Bourennane, A. Karlsson, G. Björk, *Phys. Rev. A* **64,** 012306 (2001).

[10] A. Ekert, *Phys. Rev. Lett.* **67,** 661 (1991).

[11] L. Goldenberg, L. Vaidman, *Phys. Rev. Lett.* **75,** 1239 (1995).

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

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

[14] M. Hennrich, T. Legero, A. Kuhn, G. Rempe, *Phys. Rev. Lett.* **85,** 4872 (2000).

[15] B. Lounis, W.E. Moerner, *Nature* **407,** 491 (2000).