Quantum cryptography using larger alphabets

H. Bechmann-Pasquinucci and W. Tittel
Group of Applied Physics, University of Geneva, CH-1211 Geneva 4, Switzerland
(Received 1 November 1999; published 16 May 2000)

Like all of quantum information theory, quantum cryptography is traditionally based on two-level quantum systems. In this paper, a protocol for quantum key distribution based on higher-dimensional systems is presented. An experimental realization using an interferometric setup is also proposed. Analyzing this protocol from the practical side, one finds an increased key creation rate while keeping the initial laser pulse rate constant. Analyzing it for the case of intercept/resend eavesdropping strategy, an increased error rate is found compared to two-dimensional systems, hence an advantage for the legitimate users to detect an eavesdropper.

PACS number(s): 03.67.Dd

I. INTRODUCTION

Reliable transfer of confidential information is becoming more and more important. The only means, mathematically proven to be secure, is the one time pad [1], in which the sender, Alice, and the receiver, Bob, need to share a common secret key. This key is used to en- and decode the secret message. Quantum key distribution (QKD) is known to provide the one time pad with the required secret key [2]. Based on the nonclassical features of quantum mechanics, it provides the distribution of the key in a way that guarantees the detection of any eavesdropping. Roughly speaking, since it is not possible to measure an unknown quantum system without modifying it, an eavesdropper manifests itself by introducing errors in the transmission data. After the final transmission, a suitable subset of data is used to estimate the error rate. If the error rate is found to be below a certain threshold, Alice and Bob can proceed using the remaining data to establish a secret key by means of error correction and privacy amplification [3]. Otherwise, they will decide that the data are not secure and start a new data transmission.

During the last years several quantum key distribution protocols based on two-level systems (qubits) have been published [4,5]. The connection between the quantum bit error rate (QBER) and the maximum amount of information the eavesdropper might have attained has been investigated both in the case of incoherent and coherent (joint measurement of more qubits) eavesdropping attacks [5,6], and the shortening of the raw key due to error correction and privacy amplification has been calculated [7]. There is one interesting thing to note: all work, not only in the case of quantum key distribution but in quantum information theory in general, has thus far mainly been based on qubits (for exceptions, see, e.g., [8]). It should be mentioned that the use of variables with continuous spectrum has been investigated intensively in the last years, see, e.g., [9]. Here we are, however, only concerned with variables taking discrete values. The reason why higher discrete alphabets have not been considered up to now is probably easy but not very scientific: classical information theory is based on bits. Indeed, the enlargement to higher alphabets is of no interest in the classical case, since it does not hold any advantage.

From the experimental side, a number of prototypes, based on qubits, have been developed, demonstrating that QKD not only works inside the laboratory, but outside, under real conditions, as well [10]. Thus, quantum key distribution, together with the one time pad, could already today provide an alternative to the traditional public key systems where security is based on computational complexity, which may turn out to be insecure. However, using present technology, the prototypes, especially those, adapted to ''long'' transmission distances of tens of kilometers, still suffer from low key creation rates of some hundred Hz. This could be improved by a factor of 10 by sending single-photon Fock states instead of faint laser pulses (containing only 0.1 photon per pulse), and by increasing the initial pulse rate; however, the drawback is more and more severe technical demands.

In this paper, we propose a QKD protocol using a larger alphabet and analyze it in terms of key creation rate and security against eavesdropping. Surprisingly and in opposition to the classical treatment of information, we find some important differences when passing from the two- to the higher-dimensional case. Since each photon carries more information, we find an increase of the flux of information between Alice and Bob while keeping the initial pulse rate constant. Beyond and even more important, a first eavesdropping analysis considering the strategy of intercept/resend shows advantages of this protocol with respect to protocols based on qubits.

The paper is arranged in the following way: In Sec. II, we introduce our proposal and investigate it in terms of security against eavesdropping. After this theoretical part, we present an experimental realization (Sec. III) and discuss some further extensions of our idea (Sec. IV). Finally, a short conclusion is given in Sec. V.

II. QUANTUM KEY DISTRIBUTION USING LARGER ALPHABETS

Higher-dimensional quantum systems have already been investigated in order to generalize tests of local realism or in the context of the Kochen-Specker theorem ([11,12] and references therein). However, up to now, like its classical counterpart, quantum information theory has essentially been based on bits (qubits).

Here we investigate the use of higher spins for QKD. One can imagine a whole variety of new protocols; for example, using n nonorthogonal states, where n is the dimension of the

 ©2000 The American Physical Society

space. However, the state identification becomes more and more difficult since it has to be done with positive operator valued measure (POVM) measurements [13]. Another possibility is using m different bases, each with n orthogonal states, where n is the dimension of the space. In this first approach we will limit ourselves to a protocol, using two bases and four orthogonal states per basis.

A. QKD: The Bennett-Brassard 1984 protocol (BB84) in four dimensions

The protocol known as the BB84 was originally intended for two bases, each one with two orthogonal states (qubits), but it may without difficulty be extended to a four-level system or the so-called quantum quarts (qu-quarts). As in the qubit case, Alice first chooses in which of two bases she wants to prepare her state, and second she has to decide which state to send. In the qu-quart case Alice has to choose between four different states, whereas in the qubit case she has to choose between two different states. Each of the two bases are chosen with equal probability, and each state is again chosen with equal probability. In other words, in the four-dimensional case, each of the possible eight states appear with probability $\frac{1}{8}$, whereas in the traditional two-dimensional case, the probability is $\frac{1}{4}$.

The first basis can always be chosen arbitrarily as

$$|\psi_\alpha\rangle, |\psi_\beta\rangle, |\psi_\gamma\rangle, |\psi_\delta\rangle, \tag{1}$$

where the states satisfy $|\langle\psi_i|\psi_j\rangle| = \delta_{ij}$. The second basis has to fulfill a certain requirement with respect to the first basis, namely, that $|\langle\psi_i|\phi_j\rangle| = \frac{1}{2}$. This requirement makes the protocol symmetric which insures that the eavesdropper is not given any advantage. There are several choices of bases which may fulfill this requirement, but in the following the basis is assumed to be

$$\begin{aligned}
|\phi_\alpha\rangle &= \tfrac{1}{2}(|\psi_\alpha\rangle + |\psi_\beta\rangle + |\psi_\gamma\rangle + |\psi_\delta\rangle),\\
|\phi_\beta\rangle &= \tfrac{1}{2}(|\psi_\alpha\rangle - |\psi_\beta\rangle + |\psi_\gamma\rangle - |\psi_\delta\rangle),\\
|\phi_\gamma\rangle &= \tfrac{1}{2}(|\psi_\alpha\rangle - |\psi_\beta\rangle - |\psi_\gamma\rangle + |\psi_\delta\rangle),\\
|\phi_\delta\rangle &= \tfrac{1}{2}(|\psi_\alpha\rangle + |\psi_\beta\rangle - |\psi_\gamma\rangle - |\psi_\delta\rangle).
\end{aligned} \tag{2}$$

These states satisfy $|\langle\phi_i|\phi_j\rangle| = \delta_{ij}$. Furthermore, the overlap between any state from the first (ψ-) basis with any state from the second (ϕ-) basis is seen to be $\frac{1}{2}$ as required.

Bob will every time he receives a state choose to measure either in the ψ- or the ϕ- basis. At the end of all the transmissions Alice and Bob will, as in the qubit case, have a public discussion where they single out the transmission where they have used the same basis. Since they both make random choices, on average $\frac{1}{2}$ of the transmission has to be discarded. If no eavesdropper is present Alice and Bob will now share a random string of α, β, γ, and δ's, where the various letters are taken to be the subscript of the states, i.e., $|\psi_\alpha\rangle$ and $|\phi_\alpha\rangle$ are identified as the letter "α," etc. Thus, if Bob initially made n detections, he ends up with $n/2$ quarts, which is, in terms of information contents, equivalent to n bits. This key can now directly be used to encode a secret message using the one time pad. Note that the one time pad is not restricted to bits, but that any alphabet can be used; see, e.g., [1].

B. Eavesdropping: Intercept/resend

During the public discussion Alice and Bob extract a subset of data which is compared in public. This discussion leads to an estimate of the error rate induced by the presence of an eavesdropper. The data revealed during the discussion is afterwards discarded.

The simplest possible eavesdropping strategy is the intercept/resend strategy, in which Eve (the eavesdropper) intercepts the transmissions from Alice to Bob, performs a measurement and, according to the outcome of her measurement, she prepares a new state and sends it on to Bob. In the following only the cases where Alice and Bob use the same basis are considered, since the ones where they use different bases are discarded during the public discussion.

Suppose Alice sends the state $|\psi_\alpha\rangle$. If Eve performs her measurement in the ψ basis she will find the state $|\psi_\alpha\rangle$ and she will prepare a new $|\psi_\alpha\rangle$ state and send it to Bob. Hence, Eve introduces no errors and Bob finds the correct state. If instead Eve measures in the ϕ basis, she will with equal probability, $\frac{1}{4}$, find one of the four different ϕ states and pass it on to Bob. For any of the ϕ states Bob will only find the correct state, $|\psi_\alpha\rangle$, with probability $\frac{1}{4}$, which means that with probability $\frac{3}{4}$ he will get the wrong state, hence an error.

For the following discussions it is convenient to introduce a more formal measure of information. The relevant information measure here is Shannon information [14], which by tradition is measured in terms of bits. The Shannon information is for qubits bounded between 0 and 1 bit, since each qubit can carry one bit of information. However, for the qu-quarts, the Shannon information is bounded between 0 and 2 bits, since each qu-quart can carry 2 bits of information. To obtain 0 bits of course means obtaining no information, and 1 bit or 2 bits, respectively, means having full information. The general form of the Shannon information is

$$I_S = \begin{cases} 1 + H(p_1, \ldots, p_n) & \text{for qubits} \\ 2 + H(p_1, \ldots, p_n) & \text{for qu-quarts,} \end{cases} \tag{3}$$

where $H(p_1, \ldots, p_n)$ is the entropy function defined as $H(p_1, \ldots, p_n) = p_1 \log_2 p_1 + \cdots + p_n \log_2 p_n$, and $p_1, \ldots, p_n$ is the probability distribution of the possible outcomes $1, \ldots, n$.

Above it was argued that the eavesdropper learns correctly half of the transmissions when using the intercept/resend strategy. The formal definition of Shannon information leads for the qu-quart case to

$$\begin{aligned}
I_S^4 &= \tfrac{1}{2}[2 + 1\log_2 1 + 0\log_2 0 + 0\log_2 0 + 0\log_2 0\\
&\quad + \tfrac{1}{2}[2 + \tfrac{1}{4}\log_2\tfrac{1}{4} + \tfrac{1}{4}\log_2\tfrac{1}{4} + \tfrac{1}{4}\log_2\tfrac{1}{4} + \tfrac{1}{4}\log_2\tfrac{1}{4}]\\
&= 1
\end{aligned} \tag{4}$$

as expected, since half of the times Eve learns 2 bits and half of the times she learns 0 bits, leading to an average of 1 bit, which is $\frac{1}{2}$ half of the transferred information.

Calculating Eve's amount of Shannon information for the qubit case leads to

$$I_S^2=\tfrac{1}{2}[1+1\log_2 1+0\log_2 0]+\tfrac{1}{2}[1+\tfrac{1}{2}\log_2\tfrac{1}{2}+\tfrac{1}{2}\log_2\tfrac{1}{2}]$$
$$=\tfrac{1}{2}. \tag{5}$$

This means that also in the qubit case the eavesdropper learns on average only $\frac{1}{2}$ of the transfered information; however, she will introduce a smaller error rate of only one out of four transmissions [3]. To conclude, the eavesdropper gains the same fraction of information whether using qu-quarts or qubits; however, the qu-quarts do hold an advantage for Alice and Bob, since the eavesdropper introduces a higher error rate, $\frac{3}{8}$ compared to $\frac{1}{4}$, in order to obtain the same amount of information [15]. From now on, we will refer to the quantum error rate in the general case as quantum transmission error rate QTER.

The intermediate basis

As in the qubit case Eve may also choose to perform her measurement in what is known as the intermediate basis, instead of using the same bases as Alice and Bob [3]. Eavesdropping in the intermediate basis is the simplest example of an eavesdropping strategy which gives the eavesdropper probabilistic information.

In the extended BB84 protocol the intermediate θ basis is defined with the following requirements:

$$|\langle\theta_i|\psi_i\rangle|=|\langle\theta_i|\phi_i\rangle|=\text{maximum value,}$$
$$|\langle\theta_i|\psi_j\rangle|=|\langle\theta_i|\phi_j\rangle|=\text{minimum value, for all}\quad i\neq j. \tag{6}$$

The two vectors $|\psi_i\rangle$ and $|\phi_i\rangle$ define a plane. The vector which gives the same maximum overlap, is the one with the same minimum distance to both of them, which is

$$|\theta_i\rangle=N(|\psi_i\rangle+|\phi_i\rangle), \tag{7}$$

where N is the normalization constant. This argument leads to the following intermediate basis:

$$|\theta_\alpha\rangle=\frac{1}{2\sqrt{3}}(3|\psi_\alpha\rangle+|\psi_\beta\rangle+|\psi_\gamma\rangle+|\psi_\delta\rangle),$$
$$|\theta_\beta\rangle=\frac{1}{2\sqrt{3}}(|\psi_\alpha\rangle-3|\psi_\beta\rangle+|\psi_\gamma\rangle-|\psi_\delta\rangle),$$
$$|\theta_\gamma\rangle=\frac{1}{2\sqrt{3}}(|\psi_\alpha\rangle-|\psi_\beta\rangle-3|\psi_\gamma\rangle+|\psi_\delta\rangle), \tag{8}$$
$$|\theta_\delta\rangle=\frac{1}{2\sqrt{3}}(|\psi_\alpha\rangle+|\psi_\beta\rangle-|\psi_\gamma\rangle-3|\psi_\delta\rangle),$$

which satisfies $|\langle\theta_i|\theta_j\rangle|=\delta_{ij}$ and which has the following overlaps:

$$|\langle\theta_i|\psi_i\rangle|=|\langle\theta_i|\phi_i\rangle|=\frac{3}{2\sqrt{3}},$$
$$|\langle\theta_i|\psi_j\rangle|=|\langle\theta_i|\phi_j\rangle|=\frac{1}{2\sqrt{3}}. \tag{9}$$

Assume that Alice sends the state $|\psi_\alpha\rangle$ and Eve measures in the intermediate basis, i.e., the θ basis, then she will find the following outcomes with the corresponding probabilities: $P(\theta_\alpha)=\frac{3}{4}$ and $P(\theta_\beta)=P(\theta_\gamma)=P(\theta_\delta)=\frac{1}{12}$. These probabilities give Eve the following Shannon information:

$$I_S^4=(2+\tfrac{3}{4}\log_2\tfrac{3}{4}+3\tfrac{1}{12}\log_2\tfrac{1}{12})\approx 0.792, \tag{10}$$

and she will give rise to the following error rate: with probability $\frac{3}{4}$ Eve will send to Bob the state $|\theta_\alpha\rangle$ and with probability $\frac{1}{12}$ she will send him $|\theta_\beta\rangle$, $|\theta_\gamma\rangle$, or $|\theta_\delta\rangle$. This gives Bob the following probability of finding the correct state (remember that Alice sent $|\psi_\alpha\rangle$, and it is assumed that Bob measures in the ψ basis) $\frac{3}{4}\frac{3}{4}+3(\frac{1}{12}\frac{1}{12})=\frac{5}{8}$. This means that even if Eve measures in the intermediate basis, she will introduce the same error rate, namely, $\frac{3}{8}$.

Comparing this strategy on the qu-quarts with the equivalent strategy on qubits: In the qubit case Eve has probability $P(s)=(2-\sqrt{2})/4\approx 0.146$ for successfully identifying the state, leading to an amount of Shannon information of

$$I_S^2=\left[1+\left(\frac{2-\sqrt{2}}{4}\right)\log_2\left(\frac{2-\sqrt{2}}{4}\right)\right.$$
$$\left.+\left(1-\frac{2-\sqrt{2}}{4}\right)\log_2\left(1-\frac{2-\sqrt{2}}{4}\right)\right]\approx 0.399 \tag{11}$$

and a QBER of $\frac{1}{4}$. To compare the information gained by the eavesdropper in the two cases, we have to consider how much information she has on the whole string. Suppose that Alice has sent n qu-quarts, then Eve has $0.792n$ bits of information on the whole string. In order to transmit the same amount of information to Bob using qubits, Alice has to send $2n$ qubits since each qubit carries half the amount of information of a qu-quart. This means that in the qubit case Eve would obtain $2n\times 0.399=0.798n$ bits of information. Again this shows that in the case of a larger alphabet the eavesdropper will introduce a higher error rate, the same as in the case treated before in Sec. II B, in order to get a comparable amount of information. The issue of optimal eavesdropping on the higher alphabet will be discussed in a future publication [16].

C. Mapping onto a two-dimensional key

Classically a larger alphabet like the one used here may simply be viewed as an encoding of bits, for example, $\alpha=00$, $\beta=01$, $\gamma=10$, and $\delta=11$. Alice and Bob can also in this case choose to view the higher alphabet as a simple encoding of bits. However, the following example shows that they have to be careful about when they perform the translation. Suppose that the eavesdropper has used the intermediate basis,[1] then she will have obtained each quart correctly with probability $\frac{3}{4}$. This means that on average Eve will have three out of four quarts correctly; however, she

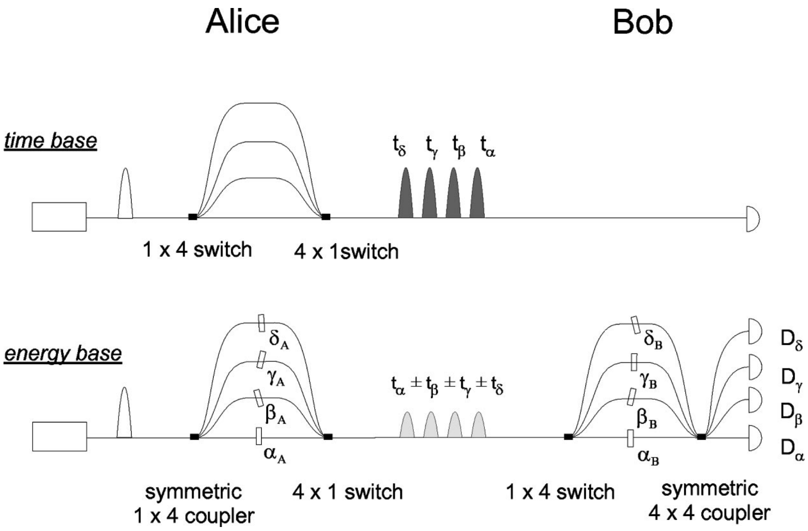

FIG. 1. Schematical setup for four-letter quantum key distribution. See text for a detailed description.

does not know which ones she has correctly and which ones are wrong. Now suppose that Alice has sent the following string of α, β, γ, and δ:

$$\text{Alice:} \quad \alpha\delta\beta\alpha\gamma\delta\delta\beta\gamma\alpha\beta\delta\ldots,$$

but that Eve has the string

$$\text{Eve:} \quad \alpha\delta\boldsymbol{\gamma}\alpha\gamma\boldsymbol{\beta}\delta\beta\gamma\alpha\boldsymbol{\alpha}\delta\ldots \quad .$$

It is easily seen that 3 out of 12 are wrong in Eve's string or that she has $\frac{9}{12}=\frac{3}{4}$ correct.

Assume now that Alice and Bob want to map the four-dimensional key onto a binary one. Using the above given example, Alice's new string reads

Alice: 00 11 01 00 10 11 11 01 10 00 01 11 . . . .

Doing the same with her sequence of quarts, Eve ends up with

Eve: 00 11 **10** 00 10 **0**1 11 01 10 00 0**0** 11 . . . .

Notice that here Eve has $\frac{4}{24}=\frac{1}{6}$ bits wrong, or five out of six bits correct. This is due to the fact that the errors occurring in Eve's string are no longer independent, but depend on each other in the respective blocks. Beyond, this the processes of error correction and privacy amplification do not apply to this case. This means that Alice and Bob have to perform this process in the higher alphabet, and only perform the translation to bits at the very end when the eavesdropper has no information on the string shared between them.

It is important to realize that Alice and Bob should not even discuss how the translation should be done until after error correction and privacy amplification, since this information may give an advantage to the eavesdropper. Assume that Alice and Bob before starting the transmissions of ququarts have decided for the bit-encoding that is given above. In designing the optimal eavesdropping strategy, Eve may use this knowledge to give different weight to the various states. Suppose, for example, Alice sends an α. Eve will with the highest possible probability try to identify that Alice sent an α, since in that case she has learned both bits correctly. Failing to make the correct identification, and instead obtaining β or γ will however still give her one bit correct, whereas finding δ gives her only errors. As a consequence Eve will give more weight to β and γ, than to δ. However, this is very different from eavesdropping on the higher alphabet, where obtaining α is correct, but any other letter β, γ, or δ is equally wrong.

III. EXPERIMENTAL REALIZATION

In the following, the given states are given physical meaning and a possible experimental realization for a four-letter alphabet is presented. It is important to notice that generalization to arbitrarily large alphabets is in principle possible.

Alice is in possession of an apparatus (see Fig. 1) that allows her to route an incoming photon (or faint laser pulse) emitted at time t_0 to one of four different delay lines. This task can be accomplished by using an optical switch. Using another switch, the light traveling via the chosen delay line is then injected (at times $t_\alpha, \ldots, t_\delta$) into the output port of the device. This apparatus thus allows Alice to create single photons in four different time slots, which we identify with the states $|\psi_\alpha\rangle, \ldots, |\psi_\delta\rangle$. To distinguish the four states of the ψ or time basis, it suffices to measure the arrival time of the photons with respect to t_0. Bob's analyzer thus simply consists of a photon detector and a fast clock.

In order to create one of the four states belonging to the ϕ or energy basis, Alice has to prepare a coherent superposition of the four emission times with appropriate phase differences. Hence, the first switch in the preparation device has to be replaced by a symmetric 1×4 optical coupler. Using the coupler depicted in Fig. 2 [11] and phases $\alpha_A, \ldots, \delta_A$, it is not difficult to show that it is possible to create the desired states $|\phi_\alpha\rangle, \ldots, |\phi_\delta\rangle$. For instance, choosing $\alpha_A=0$, β_A

---

[1] The same cannot be illustrated considering the eavesdropping strategy where Eve uses the same basis as Alice and Bob, since in that case she has either full information about the quart sent by Alice or no information at all.

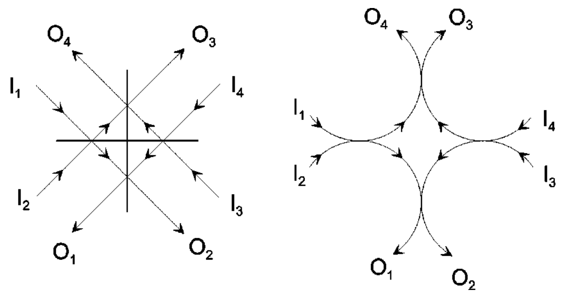

FIG. 2. Bulk- and fiber-optical realization of a symmetric 4×4 coupler.

$=\pi/2$, $\gamma_A=0$, and $\delta_A=-\pi/2$ leads (neglecting an unimportant overall phase) to the creation of $|\phi_\alpha\rangle$ [17]. In order to distinguish the four states of the energy basis, Bob has to have a device that coherently recombines the pulses arriving at times $t_\alpha, \ldots, t_\delta$ and then make them interfere in such a way that each state leads to completely constructive interference in specific output port, hence to a detection by a different detector. The device thus consists of an optical switch that routes the pulse arriving first to a long delay line, the pulse arriving second to a shorter one, etc. in a way that the delay difference introduced by Alice will be exactly compensated. Using the already mentioned 4×4 coupler and phase settings $\alpha_B=0$, $\beta_B=-\pi/2$, $\gamma_B=0$, and $\delta_B=\pi/2$, it is straightforward to show that each state indeed leads to detection in a different detector (i.e., $|\phi_\alpha\rangle$ leads to detection in D_α, etc.).

IV. DISCUSSION AND EXPERIMENTAL EXTENSIONS

As stated in the Introduction, one of the motivations for considering higher-dimensional systems for QKD is the increase of information per photon. This leads after error correction and privacy amplification of the high-dimensional (more-than-two-dimensional) key to a larger binary key. Beyond this, the important point of our proposal is that the mentioned speedup goes along with an increasing quantum transmission error rate introduced by eavesdropping. Unfortunately, this advantage of easier detection of an unlegitimized third person is somewhat hidden by a higher QTER introduced by Alice and Bob themselves. That is, the larger number of simultaneously active (and noisy) detectors engenders a higher probability that one detector sees a dark count while a photon is expected to arrive. However, we believe that as long as those errors are small, QKD using higher alphabets could still be advantageous compared to two-level systems.

Attention should be drawn to several interesting extensions of this proposal. First of all, similar to QKD schemes based on two-level systems, it is possible to find a ‘‘plug&play’’ system [18] using time multiplexed interferometry to realize systems of higher dimensions as well, the advantage being that there is no need to equalize the path differences of different interferometers. Second, our proposal can easily be extended to photon correlation experiments as well (for proposals in the domain of fundamental physics, see, i.e., [11,12]). To give an example, higher-dimensional secret sharing [19] could be realized in the following way. One could pump a nonlinear crystal with a laser pulse, having traveled via one out of n delay lines, or a coherent superposition of n delay lines, respectively. Similar to the case treated here, the created photon pair would then be described either in a time, or an energy basis. After having separated the two photons, each one is then analyzed in one of the two bases (in this context, see [20,21]).

V. CONCLUSION

We proposed to enlarge the dimensions of quantum systems for quantum key distribution and analyzed a protocol based on four orthogonal states in two different bases in terms of information transfer and introduced errors by an intercept/resend eavesdropping attack. Since every particle now carries more information, we find an increased flux of information which can be turned into an increased binary key creation rate. Beyond this, the quantum transmission error rate introduced by an eavesdropper for a given amount of acquired information is much higher than in the qubit case. Furthermore, we proposed an experimental realization using an interferometric setup. Even if the quantum transmission error rate introduced by the noise of the detectors is higher than in the qubit case, the new protocol will still be advantageous compared to two-level systems as long as these errors are small.

Besides these more practical considerations, the most important point of our proposal is that, in opposition to its classical counterpart, quantum information theory, at least quantum key distribution, changes when passing from two-dimensional to higher-dimensional systems. We thus believe that it might be interesting to consider other applications from this point of view as well.

ACKNOWLEDGMENTS

We would like to thank Nicolas Gisin for many stimulating discussions, and Nobert Lutkenhaus for helpful comments. H.B.-P. is supported by the Danish National Science Research Council (Grant No. 9601645). This work was also supported by the European IST project EQUIP.

[1] See, e.g., D. Welsh, *Codes and Cryptography* (Clarendon Press, Oxford, 1988).

[2] Phys. World **11** (3), (1998), special issue on quantum communication, including an article by W. Tittel, G. Ribordy, and N. Gisin on quantum cryptography.

[3] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).

[4] C.H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175;

A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C.H. Bennett, *ibid.* **68**, 3121 (1992); B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[5] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998); H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[6] C. Fuchs, N. Gisin, R.B. Griffiths, C.S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997); I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).

[7] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995); N. Lutkenhaus, Phys. Rev. A **54**, 97 (1996).

[8] E. Knill, e-print quant-ph/9608048; e-print quant-ph/9608049; D. Gottesman, e-print quant-ph/9802007.

[9] A.S. Parkins and H.J. Kimble, e-print quant-ph/9909021, and references therein.

[10] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, and G. Ribordy, Appl. Phys. B: Photophys. Laser Chem. **67**, 743 (1998).

[11] M. Zukowski, A. Zeilinger, and M.A. Horne, Phys. Rev. A **55**, 2564 (1997).

[12] M. Zukowski and D. Kaszlikowski, Phys. Rev. A **59**, 3200 (1999).

[13] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic, Dordrecht, 1995).

[14] T. Cover and J. Thomas, *Elements of Information Theory*, Wiley Series in Telecommunications (Wiley, New York, 1991).

[15] To generalize to infinitely high dimensions: Eve will correctly learn $\frac{1}{2}$ of the transmissions, but will introduce an error rate of $\frac{1}{2}$.

[16] H. Bechmann-Pasquinucci *et al.* (unpublished).

[17] Another experimental realization might be to keep the phases in the interferometer stable and to trigger different input ports in order to generate the different states.

[18] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997); G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, Electron. Lett. **34** (22), 2116 (1998).

[19] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999); M. Hillery, V. Buzek, and A. Berthiaume, e-print quant-ph/9806063.

[20] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden, Phys. Rev. Lett. **82**, 2594 (1999).

[21] W. Tittel *et al.* (unpublished).