INSTITUTE OF PHYSICS PUBLISHING JOURNAL OF PHYSICS A: MATHEMATICAL AND GENERAL

J. Phys. A: Math. Gen. **35** (2002) 10065–10076 PII: S0305-4470(02)25747-9

Quantum key distribution using multilevel encoding: security analysis

Mohamed Bourennane[1,2], Anders Karlsson[3], Gunnar Björk[3], Nicolas Gisin[4] and Nicolas J Cerf[5,6]

[1] Sektion Physik, Ludwig-Maximilians-Universität, D-80797 München, Germany
[2] Max-Planck-Institut für Quantenoptik, D-85748 Garching, Germany
[3] Department of Microelectronics and Information Technology, Royal Institute of Technology (KTH), Electrum 229, SE-164 40 Kista, Sweden
[4] GAP-Optique, Université de Genève, 20 rue de l'Ecole de Médecine, Genève 4, Switzerland
[5] Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium
[6] JPL-Caltech, Pasadena, CA 91109, USA

Received 14 June 2001, in final form 5 July 2002
Published 12 November 2002
Online at stacks.iop.org/JPhysA/35/10065

Abstract

We propose an extension of quantum key distribution based on encoding the key into quNits, i.e. quantum states in an N-dimensional Hilbert space. We estimate both the mutual information between the legitimate parties and the eavesdropper, and the error rate, as a function of the dimension of the Hilbert space. We derive the information gained by an eavesdropper using optimal incoherent attacks and an upper bound on the legitimate party error rate that ensures unconditional security when the eavesdropper uses finite coherent eavesdropping attacks. We also consider realistic systems where we assume that the detector dark count probability is not negligible.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.−a, 03.65.Ta

1. Introduction

Quantum cryptography aims to provide an *unconditionally* secure key distribution between two parties, Alice and Bob. Bennett and Brassard (BB84) proposed a quantum key distribution protocol where Alice and Bob choose randomly between two complementary (conjugate) bases and in each basis the 'information' is encoded using two orthogonal quantum states (qubits) [1]. Since the basis is unknown to the eavesdropper (by convention called Eve), she cannot copy the sent states perfectly (the non-cloning theorem). The use of a random choice of complementary bases furthermore implies that if the sender Alice prepares a state in one basis, the outcome of a measurement by Bob or Eve in a complementary basis will yield a totally random outcome. These features guarantee that any eavesdropping attempt will invariably introduce errors, which can be detected by the legitimate communicating parties.

An extension to the BB84 protocol was made by Bruß [2] and by Bechmann-Pasquinucci and Gisin [3] into a six-state, three complementary bases protocol. The security analysis of the six-state protocol shows that Eve's information gain for a given impaired error rate is lower than in the BB84 protocol [2, 3]. Recently two other extensions were proposed where the authors have considered schemes using four states and two bases [4], and three states and four bases [5]. In an earlier work we generalized the BB84 protocol using an N-level system and $M \leqslant N+1$ complementary bases [6]. We have analysed some specific and rather simple, but realistic, eavesdropping attacks.

The goal of this work is to find an ultimate and practical condition for the security of N-level quantum key distribution protocols, sufficiently general to encompass most types of eavesdropping. We will also derive the upper permissible limit for Bob's error rate to ensure unconditional security when Eve uses incoherent and finite coherent eavesdropping attacks (defined in section 5).

The paper is organized as follows: in section 2, we give a brief introduction to our protocol. In section 3, we reiterate the secrecy capacity of a channel and derive the results for an intercept–resend eavesdropping attack. In sections 4 and 5, we analyse the optimal individual and finite coherent eavesdropping attacks, respectively. In section 6, we consider realistic systems where we assume that the detector dark count probability is not negligible. Finally, in section 7 we present our conclusions.

2. A multibases multistate quantum key distribution protocol

In the BB84 protocol [1], Alice first randomly chooses between one of the two complementary bases to prepare her qubit, and secondly she randomly decides which of the two orthogonal qubits in the chosen basis to send. Extending this protocol to an N-level system in N-dimensional Hilbert space $\mathcal{H}_N$, where the 'information' encoded by the chosen state will from hereon be denoted as quNits. Each symbol sent by Alice in one of the M bases is chosen randomly among N possible symbols with equal probability, i.e. each of the possible NM states appears with probability $1/(MN)$. We first define the bases $\{\psi_A\}$ and $\{\psi_B\}$ over an N-dimensional space to be *mutually complementary* if the inner products between all possible pairs of vectors, with one state from each basis, have the same magnitude:

$$|_A\langle\psi_i|\psi_j\rangle_B| = 1/\sqrt{N} \qquad \forall i, j. \tag{1}$$

If a quantum state is prepared in the $\{\psi_A\}$ basis, and measured in the complementary $\{\psi_B\}$ basis, the outcome is completely random. Wootters and Fields have shown [7] that when $N = p^k$, where p is a prime and k is a positive integer, to which we restrict ourselves here, then there exists a set of $M = N + 1$ mutually complementary bases [7].

To estimate the amount of mutual information between Alice and Bob or Alice and Eve, the relevant information measure is the Shannon information of the *sifted* symbols, i.e. the symbols for which Alice and Bob have used the same bases. For simplicity, we choose to measure this information in bits. From the receiver's (Bob's or Eve's) point of view, there will be an *a priori* $p(x)$ and an *a posteriori* $p(x|y)$ probability, the latter being the conditional probability of the sending party (Alice) having sent the symbol x, given that the receiver (Eve or Bob) measured the result y. The receiver's mean information gain from Alice's symbol, I^N_{AY}, where $Y = B, E$ denotes either Bob or Eve, equals his or her entropy decrease:

$$I^N_{AY} = H^N_{apri} - H^N_{apost}. \tag{2}$$

The *a priori* probability for Alice's symbol is uniform (since the protocol dictates that Alice must chooses randomly the symbols she sends), leading to $H^N_{apri} = \log(N)$. The *a posteriori* entropy is defined as

$$H^N_{apost} = \sum_y p(y) \sum_x p(x|y) \log(p(x|y)) \tag{3}$$

where the *a posteriori* probability of symbol y, given the observer's result x, is expressed by Bayes' theorem:

$$p(x|y) = \frac{p(y|x)p(x)}{p(y)} \tag{4}$$

with $p(y) = \sum_x p(y|x)p(x)$. The mutual information between Bob and Alice as a function of Bob's error rate is derived by using equation (2) and the symmetry properties of the protocol, i.e. Alice and Bob choose independently to prepare and measure in one of the $N + 1$ bases, respectively. We also suppose that Bob's measurement errors are uniform for all quNits sent by Alice and for Eve's eavesdropping attacks:

$$I^N_{AB}\left(e^N_B\right) = \log(N) + \left(1 - e^N_B\right)\log\left(1 - e^N_B\right) + e^N_B \log\left(\frac{e^N_B}{N-1}\right) \tag{5}$$

where e^N_B is Bob's error rate, i.e. the probability that he measures a symbol erroneously. Note that expressions (2) and (5) refer to both the information and the errors contained in the sifted symbols. These errors are due to a possible eavesdropping disturbance and system noise and not due to Bob's random choice of measurement basis.

3. Eavesdropping

In an ideal system, after the quNit string has been transmitted, measured and sifted, Alice and Bob will share a common key. However, in real systems there are always some errors, and some of these errors may be due to an eavesdropper. Alice and Bob need to use error correction through a classical channel in order to establish an error-free and identical key, and privacy amplification in order to obtain a secret common key [8, 9]. The eavesdropping attacks by Eve will introduce errors. In the case of simple intercept–resend attacks, Eve obtains one of the NM possible results. After Alice and Bob have announced their choice of bases, the probabilities are $p(x = y|\{\psi_A\} = \{\psi_E\}) = 1$, $p(x \neq y|\{\psi_A\} = \{\psi_E\}) = 0$ and $p(y|\{\psi_A\} \neq \{\psi_E\}) = 1/N$, $\forall x, y$. Therefore, according to (2) and (5), Eve's information gain is $I_{AE} = \log(N)/M$ and Bob's error rate becomes $e^N_B = (1 - 1/M)(1 - 1/N)$.

Csiszár and Körner [10] have given a lower bound for the *secrecy capacity*, that is, the maximum rate at which Alice can reliably send random symbols to Bob so that the rate at which Eve obtains information about the symbols is arbitrarily small. Below we give their result as a theorem and the proof of this theorem is given in [10].

Theorem 1. *Alice and Bob can establish a secret key (using one-way classical communication) if, $I^N_{AB} \geqslant I^N_{AE}$ or $I^N_{AB} \geqslant I^N_{BE}$, where I^N_{AB}, I^N_{AE} and I^N_{BE} are the mutual information between Alice and Bob, Alice and Eve, and Bob and Eve, respectively.*

Taking into account the sifting, error correction and privacy amplification, we can define an effective transmission rate as

$$R^N_{AB}\left(e^N_B\right) = \frac{1}{M}\left(I^N_{AB}\left(e^N_B\right) - I^N_{AE}\left(e^N_B\right)\right). \tag{6}$$

In the following sections, we will discuss the different eavesdropping strategies and present a security analysis. First, we consider individual attacks where Eve attaches independent

probes to each quNit and measures her probes separately. Second, we consider coherent attacks in which Eve processes several quNits jointly.

4. Individual eavesdropping attacks: universal quantum cloning machine

Below we discuss an individual eavesdropping strategy based on the use of an asymmetric version of the N-dimensional symmetric universal quantum cloning machine (UQCM), introduced by Bužek and Hillery [11]. This asymmetric cloner [12, 13] can be used to obtain two copies of Alice's quantum state that are not of the same fidelity. Eve then keeps one of the copies (typically, the bad one) for herself, and passes the other copy (typically, the good one) to Bob. Then, after Bob and Alice have announced their chosen bases among $M = N + 1$ mutually complimentary bases, Eve does the same measurement as Bob did; i.e., she measures her copy in the same basis as Alice and Bob. The asymmetry parameter of the cloner allows her to adjust the amount of information she gained, and thereby the amount of information Bob lost. The asymmetric cloner is universal, just as the UQCM [11], so that all input states are copied equally well (Bob's fidelity and Eve's fidelity depend on neither Alice's chosen state nor chosen basis). Note that the quantum circuit that implements this asymmetric cloner is shown in [14].

In order to extract maximum information on Alice's quantum state, Eve can exploit the state of her copy and also that of the cloning machine (or ancilla). In particular, she can make a coherent measurement on the state of the cloning machine and her copy in order to infer whether she introduced an error at Bob's station (and precisely what error) [3]. For increasing disturbance, the fidelity F_{AB}^{N} between the sent state and the state inferred by Bob (defined on the sifted symbols) that governs the probability that he and Alice will accept the transmitted state decreases, while Eve's probability of correctly guessing the symbol increases.

Let us analyse the situation when Eve uses an N-dimensional copying machine such as described in [12, 13]. If Alice sends the state $|\psi_k\rangle$, the output state is given by

$$|\psi_k\rangle_A \rightarrow \sum_{m,n=0}^{N-1} a_{m,n} U_{m,n} |\psi_k\rangle_B |\Psi_{m,N-n}\rangle_{EM} \tag{7}$$

where the amplitudes $a_{m,n}$ (with $m, n = 0, \ldots, N-1$) characterize the cloner and A, B, E and M stand for Alice, Bob, Eve and the cloning machine, respectively. Here, the states $|\Psi_{m,n}\rangle_{EM}$ are the generalization of the Bell states, that is, a set of N^2 orthonormal maximally-entangled states of two N-dimensional systems:

$$|\Psi_{m,n}\rangle_{EM} = \frac{1}{\sqrt{N}} \sum_{l=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i}(ln/N)} |\psi_l\rangle_E |\psi_{l+m}\rangle_M \tag{8}$$

where the indices m and n ($m, n = 0, \ldots, N-1$) label the N^2 states. Note, here and below, that in the ket labels the additions are taken modulo N. The operators $U_{m,n}$, defined as

$$U_{m,n} = \sum_{k=0}^{N-1} \mathrm{e}^{2\pi \mathrm{i}(kn/N)} |\psi_{k+m}\rangle\langle\psi_k| \tag{9}$$

form a group of error operators on N-dimensional states, generalizing the Pauli matrices for qubits: m labels the 'shift' errors (generalizing the bit flip σ_x) while n labels the phase errors (generalizing the phase flip σ_z). Using the definition of the states $|\Psi_{m,n}\rangle$ and operators $U_{m,n}$, equation (7) can be reexpressed as

$$|\psi_k\rangle_A \rightarrow \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} |\psi_{k+m}\rangle_B \sum_{l=0}^{N-1} c_{m,k-l} |\psi_l\rangle_E |\psi_{l+m}\rangle_M \tag{10}$$

where

$$c_{m,j} = \sum_{n=0}^{N-1} a_{m,n}\, \mathrm{e}^{2\pi \mathrm{i}(jn/N)}. \tag{11}$$

Tracing the output joint state as given by equation (7) over E and M, it is easy to check that Alice's state $|\psi_k\rangle_A$ gets transformed, at Bob's station, into the mixture

$$\rho_B = \sum_{m,n=0}^{N-1} |a_{m,n}|^2 |\psi_{k+m}\rangle\langle\psi_{k+m}|. \tag{12}$$

Thus, the state undergoes a $U_{m,n}$ error with probability $p_{m,n} = |a_{m,n}|^2$ (with $\sum_{m,n} p_{m,n} = 1$). Note that $U_{0,0} = \mathbb{1}$, the identity operator, implying that the state is left unchanged with probability $p_{0,0}$. The phase errors ($n \neq 0$) clearly do not play any role in the above mixture, so the fidelity for Bob can be expressed as

$$F_B = \langle\psi_k|\rho_B|\psi_k\rangle = \sum_{n=0}^{N-1} |a_{0,n}|^2. \tag{13}$$

Now, we will impose that the cloner described above is universal, that is [12, 13]

$$a_{m,n} = \alpha\delta_{m,0}\delta_{n,0} + \frac{\beta}{N} \tag{14}$$

with the normalization relation

$$\alpha^2 + \frac{2}{N}\alpha\beta + \beta^2 = 1 \tag{15}$$

where the balance α versus β parametrizes the asymmetry of the cloner ($\alpha = 1$ and $\beta = 0$ correspond to the case where Bob gets all the information, whereas $\alpha = 0$ and $\beta = 1$ correspond to Eve getting all the information). This implies that

$$c_{m,j} = \alpha\delta_{m,0} + \beta\delta_{j,0} \tag{16}$$

so that we obtain for the cloning transformation

$$\begin{aligned} |\psi_k\rangle_A \to \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} |\psi_{k+m}\rangle_B \left(\alpha\delta_{m,0} \sum_{l=0}^{N-1} |\psi_l\rangle_E |\psi_l\rangle_M + \beta |\psi_k\rangle_E |\psi_{k+m}\rangle_M \right) \\ = |\psi_k\rangle_B \left(\frac{\alpha}{\sqrt{N}} \sum_{l=0}^{N-1} |\psi_l\rangle_E |\psi_l\rangle_M + \frac{\beta}{\sqrt{N}} |\psi_k\rangle_E |\psi_k\rangle_M \right) \\ + \sum_{m=1}^{N-1} |\psi_{k+m}\rangle_B \left(\frac{\beta}{\sqrt{N}} |\psi_k\rangle_E |\psi_{k+m}\rangle_M \right) \end{aligned} \tag{17}$$

where the first term on the rhs corresponds to Bob having no error, while the $(N-1)$ other terms correspond to all possible errors for Bob.

Eve's strategy is as follows. She first measures both her copy E and the 'cloning machine' M in the good basis (after the chosen basis is disclosed by Alice and Bob). If the two outcomes coincide, then she knows for sure that Bob has no error ($m = 0$), so that the state she has is the first term on the rhs of equation (17). Otherwise, she knows Bob had an error ($m > 0$), and she gets one of the other terms on the rhs of equation (17). Let us consider these two cases:

(i) $m = 0$. The joint probability that Eve obtains $m = 0$ with the right value of k is

$$p_{m=0}(k) = \frac{(\alpha+\beta)^2}{N} \tag{18}$$

while the probability that she obtains $m = 0$ with any other of the $(N-1)$ possibilities $l \neq k$ is

$$p_{m=0}(l) = \frac{\alpha^2}{N}. \tag{19}$$

(ii) $m \neq 0$. Then, a measurement of her copy gives Eve the right value of k with certainty. Thus, the joint probability that Eve obtains any of the $N-1$ values of $m \neq 0$ together with the good k is

$$p_{m\neq 0}(k) = \frac{\beta^2}{N}. \tag{20}$$

The fidelity of Bob is given by

$$\begin{aligned} F_B &= p_{m=0}(k) + \sum_{l\neq k} p_{m=0}(l) \\ &= \frac{(\alpha+\beta)^2}{N} + (N-1)\frac{\alpha^2}{N} \\ &= 1 - \frac{N-1}{N}\beta^2. \end{aligned} \tag{21}$$

The corresponding mutual information between Alice and Bob is given by

$$\begin{aligned} I(A{:}B) &= \log(N) - H\left[F_B, \frac{1-F_B}{N-1}, \ldots, \frac{1-F_B}{N-1}\right] \\ &= \log(N) + F_B \log[F_B] + (1-F_B)\log\left[\frac{1-F_B}{N-1}\right]. \end{aligned} \tag{22}$$

Consider now the mutual information between Alice and Eve. Conditionally on Eve's measured value of m (i.e. conditionally on Bob's error), this information can be expressed as

$$\begin{aligned} I(A{:}E|m=0) &= \log(N) - H\left[\frac{(\alpha+\beta)^2}{NF_B}, \frac{\alpha^2}{NF_B}, \ldots, \frac{\alpha^2}{NF_B}\right] \\ I(A{:}E|m\neq 0) &= \log(N). \end{aligned} \tag{23}$$

Thus, the average mutual information between Alice and Eve is

$$\begin{aligned} I(A{:}E) &= F_B I(A{:}E|m=0) + (1-F_B) I(A{:}E|m\neq 0) \\ &= \log(N) - F_B H\left[\frac{(\alpha+\beta)^2}{NF_B}, \frac{\alpha^2}{NF_B}, \ldots, \frac{\alpha^2}{NF_B}\right] \\ &= \log(N) + \frac{(\alpha+\beta)^2}{N}\log\left[\frac{(\alpha+\beta)^2}{NF_B}\right] + \frac{N-1}{N}\alpha^2 \log\left[\frac{\alpha^2}{NF_B}\right]. \end{aligned} \tag{24}$$

This information can also be reexpressed, using Eve's fidelity

$$F_E = 1 - \frac{N-1}{N}\alpha^2 \tag{25}$$

as

$$\begin{aligned} I(A{:}E) &= \log(N) - F_B H\left[\frac{F_B+F_E-1}{F_B}, \frac{1-F_E}{(N-1)F_B}, \ldots, \frac{1-F_E}{(N-1)F_B}\right] \\ &= \log(N) + (F_B+F_E-1)\log\left[\frac{F_B+F_E-1}{F_B}\right] \\ &\quad + (1-F_E)\log\left[\frac{1-F_E}{(N-1)F_B}\right]. \end{aligned} \tag{26}$$

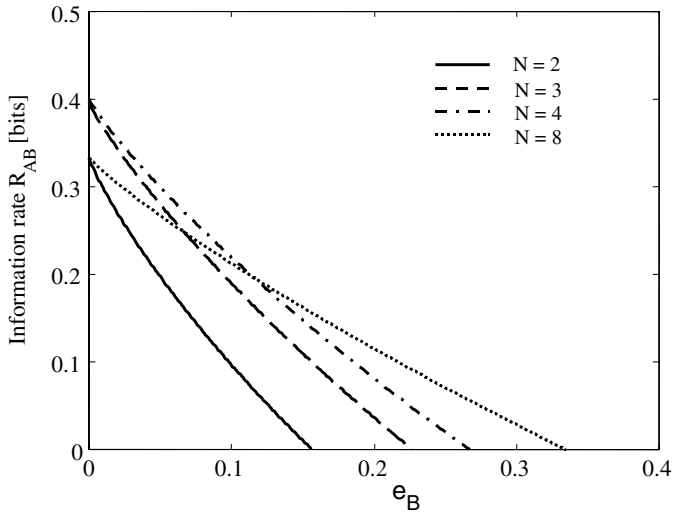

Figure 1. The information rate R_{AB}, defined by equation (6), as a function of Bob's error rate e_B^N for different Hilbert space dimensions N, assuming that $M = N + 1$, using the universal quantum cloning machine eavesdropping strategy.

As shown in [11] the maximal fidelity of copying a quNit is obtained using the UQCM. This maximal value of the fidelity corresponds precisely to the fidelity of the optimal incoherent eavesdropping strategy, as Bechmann-Pasquinucci and Gisin have shown explicitly for the ($N = 2$, $M = 3$) case [3]. From the symmetry of the problem it follows that for $M = N + 1$, the fidelity of the optimal incoherent eavesdropping is accomplished using a UQCM.

In figure 1, we plot the information rate R_{AB}^N, defined by equation (6), as a function of Bob's error rate for different values of N. For each N, the intersection between the graphs R_{AB}^N and the horizontal axis corresponds to the upper permissible bound for Bob's error rate to enable secure key distribution. In all cases, the UQCM gives the best performance (from the viewpoint of the eavesdropper), so Alice and Bob should use the UQCM model to estimate the 'leakage' of information to Eve when applying privacy amplification.

5. Finite coherent eavesdropping attacks

In the previous section we have assumed only individual attacks, i.e. Eve manipulates and performs measurements on each quNit separately. In this section we address the case where Eve manipulates coherently finitely many quNits, that is, Eve attacks coherently an arbitrary large but fixed and finite number of quNits. We call such strategies *finite coherent attacks*. We like to stress that the length of the key must be much longer than the number of coherently manipulated quNits and that Eve applies the same strategy independently to all the blocks of quNits. This is a very reasonable assumption even assuming a very powerful Eve. In this way Alice and Bob have a long series of independent realization of random variables to which theorem 1 applies. The question then is: what is the maximum rate of errors detected by Bob that allows Alice and Bob to still apply error correction and privacy amplification to extract a secure key? Already in 1996, Mayers presented ideas on how to prove such a bound [16], even when the block size tends to infinity. Now several proofs exist [16–24] for security against coherent attacks, but they are all specific to a particular protocol. In contrast, here we shall

present the proof in a form quite different from the previous ones, which is fairly general as it does not depend on the number M of bases used and is not limited in dimension.

Theorem 2. *In N-dimensional Hilbert space, two users Alice and Bob can establish a secret key (using one-way classical communication) when the adversary Eve is restricted to finite coherent attacks if Bob's error rate satisfies the inequality*

$$\left(1 - e_B^N\right) \log\left(1 - e_B^N\right) + e_B^N \log\left(\frac{e_B^N}{N-1}\right) > -\frac{1}{2}\log(N), \tag{27}$$

where e_B^N is Bob's error rate.

Thus this gives a sufficient (but not necessary) condition for the generation of a secure key regardless of the number of mutually complimentary bases ($M \geqslant 2$), the only restriction being that finite-length blocks of quNits are attacked. To prove this theorem we need another theorem due to Hall [15] that sets a limit on the sum of the mutual information between Alice and Bob and the mutual information between Alice and Eve:

Theorem 3. *Let $\hat{B}$ and $\hat{E}$ be symbol observables for Bob and Eve, respectively, in an N-dimensional Hilbert space so that the maximum possible overlap between any two eigenvectors $|\psi_i\rangle_B$ and $|\psi_j\rangle_E$ corresponding to these observables is $C = \mathrm{Max}_{i,j}\{|_B\langle\psi_i|\psi_j\rangle_E|\}$. Then the mutual information Alice–Bob and Alice–Eve satisfy the following inequality:*

$$I_{AB}^N + I_{AE}^N \leqslant 2\log_2(NC). \tag{28}$$

Now we are ready to prove theorem 2.

Proof of theorem 2. Suppose Alice sent a large number of quNit symbols, and that Bob performed this measurement on n quNits of them using the correct basis. The Hilbert space dimension of the total sifted symbol space is thus N^n. Let us now relabel the bases for each of the n quNits such that, by definition, Alice used all n times the $\{\psi_B\}$ basis. Hence, using this relabelling, Bob's observable is the n-time tensor product $\hat{B}_1 \otimes \cdots \otimes \hat{B}_n$. Since Eve had no way to know the correct bases, her optimal information on the correct ones is precisely the same as her optimal information on the incorrect ones. Hence, one can bound her information assuming she measures $\hat{E}_1 \otimes \cdots \otimes \hat{E}_n$, where $\hat{E}_i$ is a complementary observable to $\hat{B}_i$. It follows that $C = N^{-n/2}$. By applying theorem 3, we obtain the following inequality:

$$I_{AB}^N + I_{AE}^N \leqslant n\log_2(N). \tag{29}$$

By using the inequality $I_{AB}^N \geqslant I_{AE}^N$ of theorem 1 and equation (29), we obtain

$$I_{AB}^N \geqslant \frac{n}{2}\log_2(N). \tag{30}$$

For a string of n symbols, the mutual information between Alice and Bob becomes

$$I_{AB}^N\left(e_B^N\right) = n\left(\log(N) + \left(1 - e_B^N\right)\log\left(1 - e_B^N\right) + e_B^N \log\left(\frac{e_B^N}{N-1}\right)\right). \tag{31}$$

Using equations (30) and (31), we obtain theorem 2. □

In figure 2, we plot the upper bound for Bob's error rate as a function of N in the case of the optimal incoherent and finite coherent eavesdropping attacks. For $N = 2$ we recover the results for coherent attacks by Shor and Preskill, $e_B^2 = 11\%$ [19]. We would like to stress again that we have considered the case of coherent attacks on fixed and finite number of quNits and a key much longer than n. In contrast, in Mayers, Lo, and Shor and Preskill

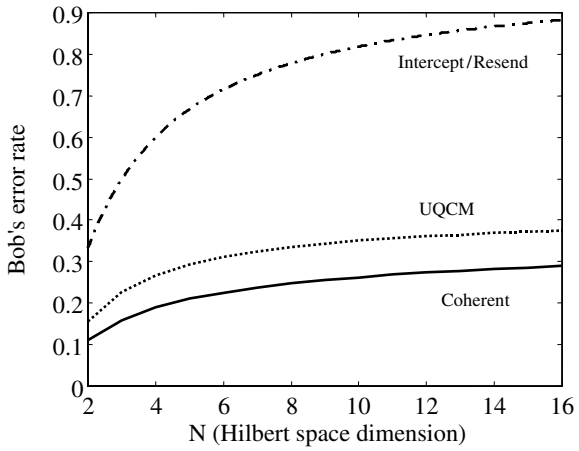

Figure 2. Bob's error rate e_B^N as a function of the dimension of the Hilbert space N for optimal incoherent and coherent eavesdropping strategies.

proofs, the coherent attacks are more general and unlimited. For the qubit, Shor and Preskill have used for their proof Calderbank–Shor–Steane (CSS) quantum error correction codes. The security of their protocol depends on the fact that for low error rate, a CSS code transmits the encoded information with very little information leaked to Eve. Therefore a secure key can be established if the error rate is low enough for the CSS codes to achieve a nonvanishing asymptotic rate [19]. One can generalize the Shor and Preskill security proof to quNits [25]. In a recent result due to Harrington and Preskill, an achievable rate for quNit CSS codes is estimated in [26] (equation (76)). It is given by

$$R_d = \frac{k}{N} \leqslant 1 - 2H_d(P_x) - 2p_x \log_d(d-1) \tag{32}$$

where d is the dimension of Hilbert space and p_x is the error probability. By using the definition of the entropy and $\log_d(x) = \frac{\log_2(x)}{\log_2(d)}$, we obtain

$$\begin{aligned} &1 - 2H_d(P_x) - 2p_x \log_d(d-1) \\ &\quad = 1 + 2(1-p_x)\log_d(1-px) + 2(p_x)\log_d(px) - 2p_x \log_d(d-1) \\ &\quad = \log_2(d)\left(1 + 2(1-p_x)\log_2(1-px) + 2(p_x)\log_2\left(\frac{p_x}{d-1}\right)\right) \end{aligned} \tag{33}$$

and changing p_x to e_B^N and N to d

$$R_N \leqslant \frac{1}{2\log_2(N)}\left(\frac{1}{2}\log_2\left(e_B^N\right) + \left(1-e_B^N\right)\log_2\left(1-e_B^N\right) + \left(e_B^N\right)\log_2\left(\frac{e_B^N}{N-1}\right)\right). \tag{34}$$

This bound again coincides with our bound (equation (27)). Note, however, that our bound is derived straightforwardly from an information-theoretic Heisenberg uncertainty principle, even though the argument is limited to finite-length coherent attacks. It would be interesting to have a transparent demonstration of the equivalence between these two apparently different approaches.

6. Realistic systems

The attacks presented in the previous sections assume perfect eavesdropping and measurement apparatus, ideal single quNit sources and a noise-free channel. In real secret key distribution

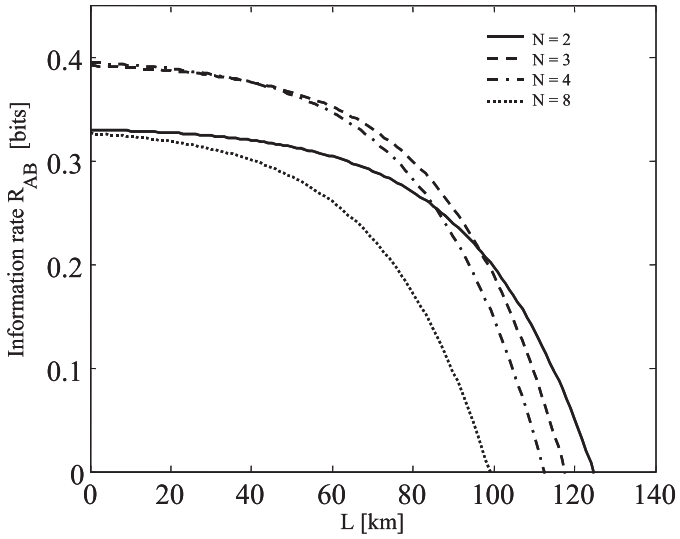

Figure 3. The information rate R_{AB}, defined by equation (6), as a function of the transmission distance L (the distance L is related to the quantum bit error rate by equation (38)). Curves are plotted for different dimensions of the Hilbert space N, assuming that $M = N + 1$ and that the universal cloning machine eavesdropping strategy is used.

systems there are several limitations: the sources can emit more than one photon, some photons never get to Bob's detector (channel loss), the detector quantum efficiency is limited and the dark count probability (counts not produced by photons) of the detectors is not negligible. For an N-dimensional Hilbert space where we assume that we have ideal single quNit sources, the optical noise remains negligible even for large N and the only source of noise is the dark count of the detectors. Under these assumptions the experimental QBER (quantum bit error rate) is given by

$$\mathrm{QBER} = \frac{P_{\mathrm{incorrect}}}{P_{\mathrm{incorrect}} + P_{\mathrm{correct}}} \approx \frac{P_{\mathrm{incorrect}}}{P_{\mathrm{correct}}} \tag{35}$$

where it was assumed that the QBER is small and where

$$P_{\mathrm{correct}} = \mu \eta_D \, \mathrm{e}^{-\alpha L} \frac{1}{M}. \tag{36}$$

In equation (36), μ is the average photon number per symbol, η is the detector quantum efficiency, α is the channel attenuation coefficient, L is the transmission length and $q_{\mathrm{basis}} = 1/M$ is a factor which depends inversely on the number of bases used in the protocol. The probability of incorrect counts, when we assume that all incorrect counts come from the detectors and they have the same dark count probability, is given by

$$P_{\mathrm{incorrect}} \approx P_{\mathrm{dark}}(N-1)\frac{1}{M} \tag{37}$$

where P_{dark} is the probability of dark counts by the detector. The QBER becomes

$$\mathrm{QBER} \approx \frac{P_{\mathrm{dark}}(N-1)}{\mu \eta \, \mathrm{e}^{-\alpha L}}. \tag{38}$$

In figure 3 we plot the information rate R_{AB} as a function of the transmission distance. The intersection of the two curves gives the maximal distance allowed between Alice and

Bob so that they can establish a secret key with typical parameter values $\eta_D = 20\%$, $\alpha = 0.2$ dB km^{-1}, $\mu = 0.1$ and $P_{\text{dark}} = 10^{-5}$.

Very recently, for the qubits, Inamori *et al* have given the unconditional security proof when the practical signal sources contain multiphoton contributions [27] and they have shown that the combination of multiphoton signals of the source together with a lossy quantum channel in the presence of errors leads to limitations of the rate [27]. The same practical problem was also analysed in a pragmatic way by Felix *et al* [28].

7. Discussion and conclusions

In this work we have considered an extension of Bennett and Brassard's seminal quantum key distribution protocol into an N-dimensional Hilbert space. We have obtained bounds on Bob's permissible error rate in the case of individual and finite coherent eavesdropping attacks, and we have given the limits for the transmission distances in non-ideal systems. Using similar arguments and methods one could also generalize Ekert's quantum cryptographic protocol [30], based on quantum entanglement and the test of Bell inequality to detect the eavesdropping, to an N-dimensional Hilbert space. Recently, Kaszlilowski *et al* have shown [31] that the violation of local realism by two entangled quNits is stronger than the violation for two entangled qubits. We conjecture that this would also imply a higher degree of security in entanglement-based multilevel quantum cryptography. One should also extend our security analysis for N-dimensional quantum key distribution by considering weak coherent sources which contain multiphoton states.

Very recently Gottesman and Lo have shown that when Alice and Bob use two-way classical communications, the protocol allows a higher key generation rate [29]. For the BB84 protocol, they have found that the allowed error rate is about 17%, which is higher than the 11% obtained by using one-way classical communication. Unfortunately, we cannot extend our proof to include two-way classical communication because to our knowledge there is no theorem for two-way classical communication equivalent to theorem 1 in classical information theory. We can only conjecture that for higher dimensional Hilbert space, the bound on the error rate will be higher when Alice and Bob use two-way classical communication.

Acknowledgments

We would like to thank John Preskill, Harald Weinfurter and Hugo Zbinden for useful discussions. This work was supported by the Swedish Research Council for Engineering Sciences (TFR), Bundesministerium für Bildung und Forschung (BMBF/VDI), the European Commission through the IST FET QIPC QuComm and EQUIP projects. One of us, MB, thanks GAP-optique for their kind hospitality during his stay there, and the European Science Foundation for financial support.

Note added in proof. It has been shown recently (in the 5th revised version of [24], which appeared on the quant-ph preprint server after completion of this work) that a slightly higher threshold can be put on the error rate at 12.7% for the 6-state protocol with one-way classical communication. This does not contradict our bound at 11% (nor the bound of Shor and Preskill [19]) since it is general and therefore applies to BB84 as well as to the 6-state protocol. As far as we know, no better bound is known today for BB84.

References

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

[2] Bruss D 1998 *Phys. Rev. Lett.* **81** 3018
[3] Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev.* A **59** 4238
[4] Bechmann-Pasquinucci H and Tittel W 2000 *Phys. Rev.* A **61** 062308
[5] Bechmann-Pasquinucci H and Peres A 2000 *Phys. Rev. Lett.* **85** 3313
[6] Bourennane M, Karlsson A and Björk G 2001 *Phys. Rev.* A **64** 052313
[7] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363
[8] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptology* **5** 3
[9] Bennett C H, Brassard G, Crepeau C and Maurer U 1995 *IEEE Trans. Inf. Theory* **41** 1915
[10] Csiszár I and Körner J 1978 *IEEE Trans. Inf. Theory* **24** 339
[11] Bužek V and Hillery M 1998 *Phys. Rev. Lett.* **81** 5003
[12] Cerf N J 1998 *Acta Phys. Slov.* **48** 115 (special issue on quantum information)
[13] Cerf N J 2000 *J. Mod. Opt.* **47** 187
[14] Braunstein S L, Bužek V and Hillery M 2001 *Phys. Rev.* A **63** 052313
[15] Hall M J W 1998 *Phys. Rev. Lett.* **74** 3307
[16] Mayers D 2001 *J. Assoc. Comput. Math.* **48** 351 (*Preprint* quant-ph/9802025)
(Preliminary version in 1996 *Advances in Cryptography: Proc. of Crypto '96* (New York: Springer) p 343)
[17] Lo H-K and Chau H F 1999 *Science* **283** 2050
[18] Biham E, Boyer M, Boykin P O, Mor T and Roychowdhury V 2000 *Proc. 32nd Annual ACM Symposium on Theory of Computing* (New York: ACM) pp 715–24
[19] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[20] Gottesman D and Preskill J 2000 *Preprint* quant-ph/0008046
[21] Inamori H 2000 *Preprint* quant-ph/0008064
[22] Inamori H 2000 *Preprint* quant-ph/0008076
[23] Lo H-K, Chau H H and Ardehali M 2000 *Preprint* quant-ph/0011056
[24] Lo H-K 2001 *Preprint* quant-ph/0102138
[25] Preskill J 2001 Private communication
[26] Harrington J and Preskill J 2001 *Preprint* quant-ph/0105058
[27] Inamori H, Lutkenhaus N and Mayers D 2001 *Preprint* quant-ph/0107017
[28] Felix S *et al* 2001 *J. Mod. Opt.* **48** 2009
[29] Gottesman D and Lo H-K 2001 *Preprint* quant-ph/0105121
[30] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[31] Kaszlikowski D, Gnascinski P, Zukowski M, Miklaszewski W and Zeilinger A 2000 *Phys. Rev. Lett.* **85** 4418