Quantum key distribution using multilevel encoding

Mohamed Bourennane,* Anders Karlsson, and Gunnar Björk
Department of Electronics, Laboratory of Quantum Optics and Quantum Electronics, Royal Institute of Technology (KTH), Electrum 229, 164 40 Kista, Sweden

(Received 15 August 2000; published 6 June 2001)

In this article, protocols for quantum key distribution based on encoding in higher dimensional systems in *N*-dimensional Hilbert space are proposed. We extend the original Bennett-Brassard protocol using two complementary bases and two-dimensional states to *M* mutually complementary bases and *N* orthogonal vectors in each base. We study the mutual information between the legitimate parties and the eavesdropper and the error rate by considering various incoherent eavesdropping attacks as a function of the dimension of the Hilbert space.

DOI: 10.1103/PhysRevA.64.012306 PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Ta

I. INTRODUCTION

Quantum cryptography ideally provides *unconditionally* secure key distribution between two parties, Alice and Bob, followed by secret key cryptography over a public channel to convey the message to be kept secret. In the original protocol proposed by Bennett and Brassard (BB84) [1], Alice and Bob randomly choose between two complementary (conjugate) bases and the information for each basis is encoded using two orthogonal quantum states (qubits). Complementary bases are defined such that if Alice prepares her state in one basis, the outcome of a measurement in a complementary basis will be totally random. This is the feature used to guarantee that any eavesdropping will invariably introduce errors in the transmission that can be detected by the communicating parties. An extension made by Bruß [2] and Bechmann-Pasquinucci and Gisin [3] to a six-state (three complementary bases) protocol shows that an eavesdropper's (by convention denoted by Eve) information gain for a given impaired error rate is lower than in the BB84 protocol [2,3]. Very recently Bechmann-Pasquinucci and Tittel [4] and Bechmann-Pasquinucci and Peres [5] have considered schemes using four states and two bases, and three states and four bases, respectively. In the present article, we generalize these results to encoding in *N*-dimensional Hilbert space using *M* bases and show, for each *N*, what is the optimal choice of *M*.

II. QUANTUM KEY DISTRIBUTION PROTOCOL

In the BB84 protocol, Alice first randomly chooses in which of two bases she wants to prepare her state, and second, she decides which state to send. In an *N*-dimensional Hilbert space $\mathcal{H}_N$, Alice first chooses in which of *M* complementary bases she wants to prepare her state, and second, decides which of the *N* states to send. The information conveyed in the state will from hereon be denoted by quNits. Each symbol sent in the *M* bases and *N* quNits is chosen randomly 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:

$$|\langle \psi_i^a | \psi_j^b \rangle| = 1/\sqrt{N} \quad \forall i,j. \tag{1}$$

If a quantum state is prepared in the $\{\psi^a\}$ basis, but measured in the complementary $\{\psi^b\}$ basis, the outcome is completely random. Wootters and Fields have shown [6] that when $N=p^k$, where *p* is a prime and *k* an integer, which we restrict ourselves to here, then there exists a set of $M=N+1$ mutually complementary bases [6]. In general, we arbitrarily choose the first basis as

$$|\psi_0^a\rangle, |\psi_1^a\rangle, \ldots, |\psi_{N-1}^a\rangle, \tag{2}$$

where the states satisfy $|\langle \psi_k^a | \psi_l^a \rangle| = \delta_{kl}$. For the case of only two complementary bases, $M=2$, the components of the second basis can be chosen as

$$|\psi_k^b\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \exp\left(\frac{2\pi i k n}{N}\right) |\psi_n^a\rangle. \tag{3}$$

For other cases one can use the explicit construction given in Ref. [6]. Every time Bob receives a quNit, he chooses randomly to measure it in one of the *M* bases. At the end of the transmission Alice and Bob will, as in the qubit case, have a public discussion where they only retain the symbols where they used the same basis. This procedure is referred to as sifting. Since they both make random choices, on average $(1-1/M)$ of the transmitted symbols have to be discarded.

To estimate the mutual information between Alice and Bob, and the information gain of the eavesdropper, the relevant information measure is the Shannon information I_S^N of the sifted symbols given by

$$I_S^N = \log_2(N) - H_N(p_0,..,p_{N-1}) \quad \text{in bits}, \tag{4}$$

where $H_N(p_0,..,p_{N-1}) = -\sum_{k=0}^{N-1} p_k \log_2 p_k$ is the entropy function and p_k (for $k=0,\ldots,N-1$) are the probability distributions of the possible outcomes (from hereon all information measures are in units of bits). Another important

*Electronic address: boure@ele.kth.se

quantity is the error probability, i.e. that a symbol is wrongly received at the receiver side, $e_{Bob}^{N,M}$, which for an ideal system is a function only of Eve's information gain. Alice and Bob will use $e_{Bob}^{N,M}$ to estimate the amount of eavesdropping. The better the scheme, the larger is the impaired $e_{Bob}^{N,M}$ for a given amount of information for Eve. In what follows, we will discuss various eavesdropping strategies and compare their performance.

III. EAVESDROPPING ATTACKS

A. Intercept-resend strategy

The simplest possible eavesdropping strategy is the intercept-resend strategy, in which Eve intercepts the transmitted data from Alice, performs a measurement, and according to the outcome of her measurement, prepares a new state and sends it on to Bob. Suppose Alice prepares and sends the quantum state $|\psi_k^a\rangle$ that belongs to the basis $\{\psi^a\}$. If Eve performs her measurement in the $\{\psi^a\}$ basis, she will detect the correct state $|\psi_k^a\rangle$ and she will subsequently prepare and send the correct state to Bob. Hence, Eve introduces no error and Bob detects the quantum state sent by Alice, provided that he chooses the correct measurement basis. If, instead, Eve measures in the $\{\psi^b\}$ basis with $b \neq a$, her result will be completely random, she will gain no information, and will cause maximal disturbance. The average information of Eve, in the case when Eve eavesdrops only a fraction η of the string sent by Alice, is given by

$$I_{Eve}^{N,M}(\eta) = \eta \frac{\log_2(N)}{M}. \tag{5}$$

We note that the measurement result is deterministic each time she uses the correct basis. The crucial reason to go to higher dimensional encoding is that in the quNit case, the eavesdropper introduces a higher error rate for Bob,

$$e_{Bob}^{N,M}(\eta) = \eta\left(1 - \frac{1}{M}\right)\left(1 - \frac{1}{N}\right). \tag{6}$$

The mutual information between Bob and Alice as function of $e_{Bob}^{N,M}$ is given by

$$I_{AB}^{N,M}(\eta) = \log_2(N) + [1 - e_{Bob}^{N,M}(\eta)]\log_2[1 - e_{Bob}^{N,M}(\eta)] + e_{Bob}^{N,M}(\eta)\log_2\left(\frac{e_{Bob}^{N,M}(\eta)}{N-1}\right). \tag{7}$$

As discussed by Bechmann-Pasquinucci and Peres [5], if Alice and Bob only want to know if Eve is active or not, a good benchmark is the ratio $e_{Bob}^{N,M}(\eta)/I_{Eve}^{N,M}(\eta)$.

B. The intermediate basis

As in the qubit ($N=2$) protocol case, Eve may also choose to perform her measurement in what is known as the intermediate, or Breidbart, basis [7], instead of using the same bases Alice and Bob are using. Eavesdropping in the intermediate basis is the simplest example of a strategy giving the eavesdropper probabilistic information. The intermediate $\{\psi^c\}$ basis for $M=2$ is defined with the following requirements:

$$|\langle\psi_k^c|\psi_k^a\rangle| = |\langle\psi_k^c|\psi_k^b\rangle| = \text{maximum}, \quad \forall k \tag{8}$$

and

$$|\langle\psi_k^c|\psi_l^a\rangle| = |\langle\psi_k^c|\psi_l^b\rangle| = \text{minimum}, \quad \forall k \neq l. \tag{9}$$

The vector that gives the same (maximal) overlap with $|\psi_k^a\rangle$ and $|\psi_k^b\rangle$ is the one with the same minimum distance to both of states, which is

$$|\psi_k^c\rangle = \frac{1}{\sqrt{C}}(|\psi_k^a\rangle + |\psi_k^b\rangle), \tag{10}$$

where $C = 2(1 + 1/\sqrt{N})$ is the normalization constant. The intermediate states defined by Eqs. (8) and (9) satisfy

$$|\langle\psi_k^c|\psi_k^a\rangle| = |\langle\psi_k^c|\psi_k^b\rangle| = \frac{\sqrt{1 + \frac{1}{N} + \frac{2}{\sqrt{N}}}}{\sqrt{C}},$$

$$|\langle\psi_k^c|\psi_l^a\rangle| = |\langle\psi_k^c|\psi_l^b\rangle| = \frac{1}{\sqrt{CN}}. \tag{11}$$

Assume that Alice sends the state $|\psi_0^a\rangle$ and Eve measures in the intermediate basis, i.e., in the $\{\psi^c\}$ basis. Then she will find the following outcomes with the corresponding probabilities: $P(\psi_0^c) = (1 + 1/N + 2/\sqrt{N})/C$ and $P(\psi_1^c) = \cdots = P(\psi_{N-1}^c) = 1/NC$. These probabilities give Eve the following Shannon information:

$$I_{Eve}^{N,2} = \log_2(N) + P(\psi_0^c)\log_2[P(\psi_0^c)] + \sum_{k=1}^{N-1} P(\psi_k^c)\log_2[P(\psi_k^c)]. \tag{12}$$

Bob will consequently have the following probability of finding the correct state:

$$P_{Bob}^{correct} = P(\psi_0^c)^2 + \sum_{k=1}^{N-1} P(\psi_k^c)^2. \tag{13}$$

This means that even if Eve measures in the intermediate basis, she will introduce the following error rate: $e_{Bob}^{N,2} = 1 - P_{Bob}^{correct}$. For $M = N+1$, it can be shown [8] that an intermediate measurement basis cannot be constructed with the properties above for $N=3$ and $N=4$. From this we conjecture that intermediate bases do not exist for $M = N+1$ when $N > 2$.

In Fig. 1 we show the ratio $e_{Bob}^{N,M}(\eta)/I_{Eve}^{N,M}(\eta)$ as a function of N for both intercept-resend and intermediate bases eavesdropping, finding that the ratio is maximized if one chooses $M = N+1$. However, if we want to keep on using the channel by actively removing Eve's information using

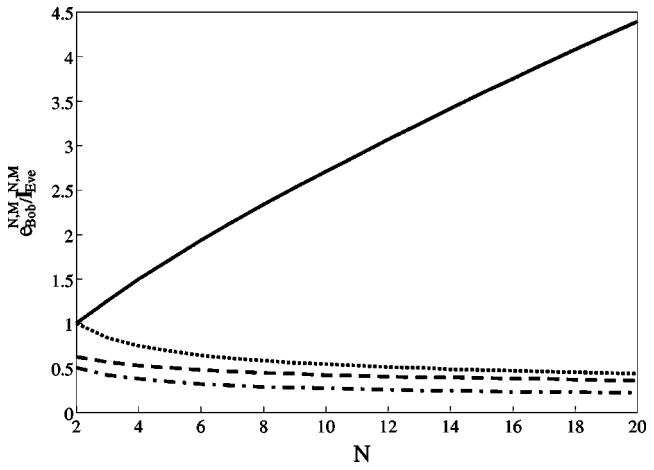

FIG. 1. The ratio $e^{N,M}_{AB}/I^{N,M}_{Eve}$ as a function of the dimension of Hilbert space *N*. Solid, dotted, and dash-dotted lines correspond to the case when Eve uses intercept-resend strategy for $M=N+1$, $M=3$, and $M=2$ complementary bases, respectively. The dashed line corresponds to the intermediate basis strategy and $M=2$.

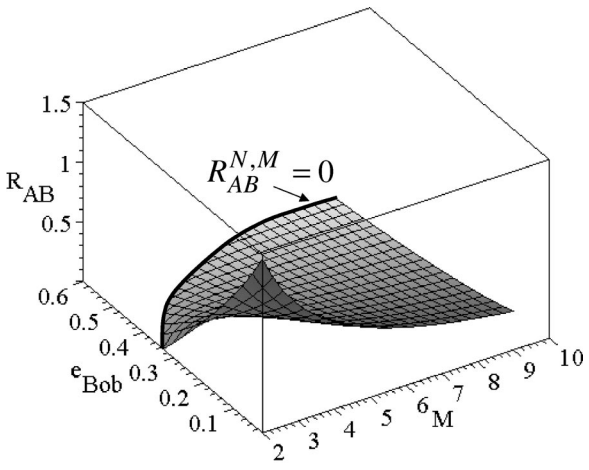

FIG. 2. The effective transmission rate $R^{N,M}_{AB}$ as a function of the number of complementary bases *M* and Bob's error rate $e^{N,M}_{Bob}$ for the case of Hilbert space dimension $N=2^3=8$.

privacy amplification [9], a better benchmark than $e^{N,M}_{Bob}(\eta)/I^{N,M}_{Eve}(\eta)$ could be the transmitted information per symbol. Taking the sifting, error correction, and privacy amplification into account, we can define an effective transmission rate as

$$R^{N,M}_{AB}(\eta)=\frac{1}{M}[I^{N,M}_{AB}(\eta)-I^{N,M}_{Eve}(\eta)]. \tag{14}$$

As discussed by Ekert, Huttner, Palma, and Peres [10], this is the lower bound for the *secrecy capacity* of Csiszár and Körner [11], giving the maximum rate at which Alice can reliably send information to Bob such that the rate at which Eve obtains this information is arbitrarily small. From the perspective of optimizing the impaired error rate for a given $R^{N,M}_{AB}(\eta)$, which tells how easy it is for Bob to detect Eve in the presence of technical noise, what is the optimum choice for *M*? First we note from the above that the maximum number of mutually complementary bases is $M=N+1$. We also note that for the case of no eavesdropping, that the effective transmission rate in bits per symbol after sifting cannot be more than $\log_2(N)/M$, so choosing *M* too large will lower the rate. In Fig. 2 we show the rate $R^{N,M}_{AB}$ as a function of number of complementary bases *M* and $e^{N,M}_{Bob}$ for $N=8$. Due to the loss of symbols in the sifting procedure, i.e., the $1/M$ dependence in the rate, it seems that the lower *M*'s are preferable. In the case when Alice and Bob use $N+1$ bases, we plot (see Fig. 3) $R^{N,M}_{AB}$ as a function of *N* and $e^{N,N+1}_{Bob}$. For a lower error rate, we observe that the transmission rate has a maximum value for $N\approx 4$ and starts to decrease when *N* increases. The zero transmission rate increases when *N* increases, and for $N=4$ corresponds to $e^{4,5}_{Bob}\approx 0.4$.

C. Optimal eavesdropping: The case of the universal quantum cloning machine

Let us finally discuss eavesdropping from the perspective of quantum cloning. The basic idea is that Eve uses a universal quantum cloning machine (UQCM), introduced by Bužek and Hillery [12], to obtain two copies of Alice's quantum state, keep one of the copied states for herself, and pass the other copy on to Bob. Then, after Bob and Alice have made their measurements and announced their basis, Eve does the same measurement as Bob, i.e., she measures in the same basis as Alice and Bob, and therefore on the average, she will obtain the same information as Bob. She can also make a coherent measurement on her state of the cloning machine and her copy, and then also know if and when she introduced an error for Bob [3]. For increasing disturbance, Bob's fidelity *F*, i.e., the probability that he and Alice will accept the transmitted state, decreases, while Eve's probability of guessing the symbol correctly increases. As shown in Ref. [12], the maximal fidelity of copying a quNit is obtained using the UQCM. In the *N*-dimensional case, from the symmetry of the problem, we conjecture (without proof) that for $M=N+1$, the optimal incoherent eavesdropping is again done using the UQCM.

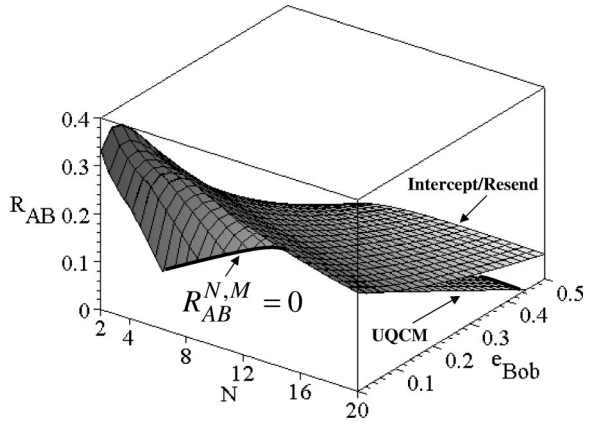

FIG. 3. The effective transmission rate $R^{N,M}_{AB}$ as function of the dimension of Hilbert space *N* for $M=N+1$ complementary bases using either the intercept-resend or the universal cloning machine eavesdropping strategies.

If Alice sends the state $|\psi_k\rangle_{Alice}$, then the operation of the UQCM corresponds to the following unitary transformation:

$$|\psi_k\rangle_{Alice}|0\rangle_{Eve}|X\rangle_x \overset{U_{QCM}}{\rightarrow} c|\psi_k\rangle_{Alice}|\psi_k\rangle_{Eve}|X_k\rangle_x + d\sum_{l\neq k}^{N}(|\psi_k\rangle_{Alice}|\psi_l\rangle_{Eve}+|\psi_l\rangle_{Alice}|\psi_k\rangle_{Eve})|X_l\rangle_x, \tag{15}$$

where $|\psi_k\rangle_{Alice}=|\psi_k\rangle_{Eve}$ are the two identical output quantum state copies and $|X_k\rangle_x$ is the orthonormal basis of Eve's cloning machine Hilbert space. The cloner is initially prepared in particular state $|X\rangle_x$ and $|0\rangle_l$ is an N-dimensional ancilla state. From the unitarity of the transformation it follows that c and d satisfy $c^2+2(N-1)d^2=1$. The maximal value of the fidelity F^N_{UCM} for the optimal cloning of a quNit to two copies is given from Ref. [12] as $F^N_{UCM}=(N+3)/[2(N+1)]$ and the corresponding disturbance is $D^N_{UCM}\equiv 1-F^N_{UCM}=(N-1)/2(N+1)$.

Assuming that Eve listens in on a fraction η of the symbols sent to Bob, then we may define an equivalent error rate $e^{N,M}_{Bob}\equiv \eta D^N_{UCM}$, and the relevant mutual informations becomes

$$I^N_{AB}=\log_2(N)+(1-e^{N,M}_{Bob})\log_2(1-e^{N,M}_{Bob}) + e^{N,M}_{Bob}\log_2\left(\frac{e^{N,M}_{Bob}}{N-1}\right), \tag{16}$$

$$I^N_{AE}=\eta\log_2(N)+(1-e^{N,M}_{Bob})\log_2(1-e^{N,M}_{Bob}) + e^{N,M}_{Bob}\log_2\left(\frac{e^{N,M}_{Bob}}{N-1}\right), \tag{17}$$

and the effective transmission rate is

$$R^{N,M}_{AB}(\eta)=\frac{1-\eta}{N+1}\log_2(N). \tag{18}$$

In Fig. 3 we have plotted the effective transmission rate $R^{N,M}_{AB}$ as a function of the dimension of Hilbert space N and Bob's error rate in the case when Eve is allowed to use the UQCM strategy. As can be seen, the maximum transmission rate is for $N\approx 4$. For low error rates, as Eve gets little information, the rate is the upper bound of $\log_2(N)/(N+1)$. In all cases, the UQCM gives the best performance (from the viewpoint of the eavesdropper), and for $N=4$ we obtain a zero transmission rate at $e^{4,5}_{Bob}\approx 0.3$. We conclude that in the case of individual eavesdropping attacks, Alice and Bob should use the UQCM estimate of information for Eve when applying privacy amplification.

IV. DISCUSSIONS AND CONCLUSION

So far, we have discussed the protocol without considering the role of the error correction and privacy amplification stages [9]. A simple protocol for the multilevel coding goes as follows: After Alice and Bob have recorded the sifted key, they randomly choose pairs of symbols and compute their XOR sum modulo N. For error correction, they announce the XOR value and keep the first symbol if and only if they agree on the XOR value (the second symbol is always discarded). For privacy amplification, Alice and Bob do not announce the XOR value, but discard the two randomly chosen symbols, while keeping the XOR sum for a new key with improved privacy [9]. Note, however, that the estimate based on $R^{N,M}_{AB}(\eta)$ of Eqs. (14) and (18) includes the privacy amplification by giving an upper limit assuming that for each N and M we can find algorithms that do not remove more bits than the difference between the mutual information Alice-Bob and Alice-Eve.

We can also generalize Ekert's quantum cryptographic protocol [13] based on quantum entanglement and the test of the Bell inequality to detect the eavesdropping to N-dimensional Hilbert space. Recently Kaszlilowski *et al.* have shown [14] that the violations of local realism by two entangled quNits are stronger than for two entangled qubits. We conjecture that this would also imply a higher degree of security in entanglement based on multilevel quantum cryptography.

As for an experimental realization of multilevel quantum key distribution, this can be done as proposed in Ref. [4] for the ($N=4$ and $M=2$) case by time multiplexing and phase encoding in an interferometric system. For N quantum states and $M=2$ bases, the time basis and energy basis, we can use the same experimental system, but with N different delay times and N different phase encoding. In realistic quantum key distribution systems, one limitation factor is the detector noise and more precisely the dark count probability P_{dark}. One can show that the quantum bit error rate scales linearly with $(N-1)P_{dark}$.

ACKNOWLEDGMENTS

This work was supported by the Swedish Technical Science Research Council (TFR), the Swedish Natural Science Research Council (NFR), and the European Commission through the IST FET QIPC QuComm project.

[1] C.H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984), p. 175.
[2] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[3] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[4] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[5] H. Bechmann-Pasquinucci and A. Peres, Los Alamos e-print archive, quant-ph/0001083.
[6] W.K. Wootters and B.D. Fields, Ann. Phys. (Leipzig) **191**, 363 (1989).

[7] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[8] R. Asplund, G. Björk, and M. Bourennane, Los Alamos e-print archive quant-ph/0011037.
[9] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[10] A.K. Ekert, B. Huttner, G.M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1992).
[11] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[12] V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
[13] A.K. Ekert, Phys. Rev. A, **67**, 661 (1991).
[14] D. Kaszlikowski, P. Gnascinski, M. Zukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).