JOURNAL OF MODERN OPTICS, 2003, VOL. 50, NO. 6–7, 1025–1033

Security aspects of quantum cryptography with d-dimensional systems

C. MACCHIAVELLO† and D. BRUSS‡

†Dipartimento di Fisica 'A. Volta' and INFM-Unità di Pavia, Via Bassi 6, 27100 Pavia, Italy; e-mail: chiara@enterprise.unipv.it

‡Institut für Theoretische Physik, Universität Hannover, 30167 Hannover, Germany

(*Received 8 September 2002*)

Abstract. We analyse the security of quantum key distribution with three-dimensional systems, and show that this scheme is more advantageous against symmetric attacks than protocols using two-dimensional states. We generalize the resulting optimal eavesdropping transformation to cryptographic systems with arbitrary dimensions.

1. Introduction

At present quantum cryptography is the experimentally most advanced application of quantum information processing. Recently, the use of three-level systems rather than two-level systems for establishing a secure quantum key has been suggested [1]. This was a very timely proposal; actually the use of states with a dimension higher than two for quantum key distribution is not just of purely theoretical interest because higher-dimensional photonic quantum states can be realized experimentally with present technology [2]. It is therefore of great importance to study how the security of a quantum key distribution changes for increasing dimension.

The aim of this work is to study the security aspects of quantum cryptographic protocols based on the use of quantum systems with arbitrary dimension, and to derive in particular, following the approach of [3], the optimal eavesdropping transformation for the most secure protocol which employs three-dimensional systems (qutrits).

The paper is organized as follows. In section 2 we review some known results about the security of quantum cryptography with two-dimensional systems (qubits). In section 3 we introduce the qutrit protocol that we want to analyse, based on the proposal of [1]. In section 4 we derive the optimal eavesdropping strategy for the qutrit protocol and prove that this scheme is more secure than protocols based on qubits. In section 5 we generalize the above mentioned optimal eavesdropping strategy to quantum cryptographic schemes which employ quantum systems with dimensions higher than three. Finally we summarize and comment on our results in section 6.

Journal of Modern Optics ISSN 0950–0340 print/ISSN 1362–3044 online
http://www.tandf.co.uk/journals
DOI: 10.1080/0950340210000579 96

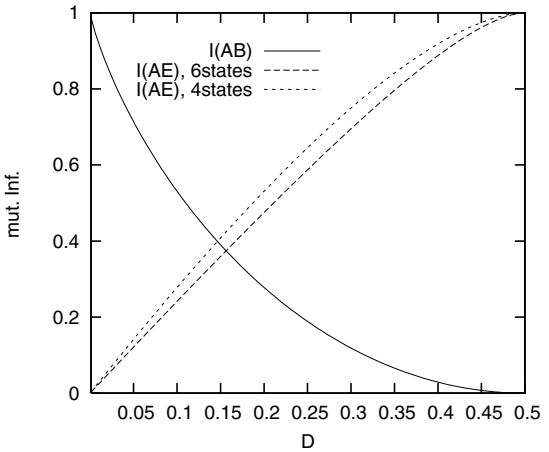

Figure 1. Maximal mutual information I_{AE} between Alice and Eve as a function of the disturbance D. The upper curve holds for BB84 and the lower curves refer to the six-state protocol. The mutual information between Alice and Bob is in both scenarios given by the curve I_{AB}.

2. The qubit case

The first protocol for quantum cryptography was introduced by Bennett and Brassard in 1984 (BB84) [4]. It is based on the use of two mutually unbiased bases†, e.g. the bases $\{|0\rangle, |1\rangle\}$ and $\{(|0\rangle + |1\rangle)/2^{1/2}, (|0\rangle - |1\rangle)/2^{1/2}\}$. Each of the four states is transmitted with the same probability. The optimal eavesdropping strategy based on incoherent attacks was derived in [5] (by incoherent attack we mean that the eavesdropper interacts with a single qubit at a time).

More recently, the so-called six state protocol was proposed [6, 7]. The main idea was to introduce a third basis, e.g. $\{(|0\rangle + \mathrm{i}|1\rangle)/2^{1/2}, (|0\rangle - \mathrm{i}|1\rangle)/2^{1/2}\}$, so that the maximum number of mutually unbiased bases, which is actually three for qubits, is employed. The analysis of the optimal eavesdropping strategy for this case [6, 7] showed that this scheme is more secure than BB84. This result can be intuitively understood by observing that from the BB84 scheme to the six state protocol the number of possible transmitted states is increased. In particular, while the four states of the BB84 protocol lie on an equator of the Bloch sphere, the states of the six-state protocol cover all three directions and thus span the whole Bloch sphere. Therefore, for the same amount of disturbance, an eavesdropper will be able to gain less information on the transmitted states in the six-state scheme. The curves corresponding to the optimal eavesdropping strategies for the two cases are reported in figure 1 for comparison (the meaning of this figure will be more clear after reading the discussion of section 4, where the qubit and the qutrit cases are compared). The main point is that in the six-state case the maximal information that Eve can acquire is lower than in the BB84 case, as seen by comparing the two dashed lines.

†Mutually unbiased bases are defined by the relation $|\langle\phi_i|\psi_j\rangle|^2 = 1/d$, where $|\phi_i\rangle$ and $|\psi_j\rangle$ are two state vectors belonging to different bases and d is the dimension of the state.

3. The qutrit protocol

We consider the cryptographic protocol suggested in [1], based on the use of four mutually unbiased bases. Such bases are given by $\{|0\rangle, |1\rangle, |2\rangle\}$ and

$$\left\{ |\alpha\rangle = \frac{1}{3^{1/2}}(|0\rangle + |1\rangle + |2\rangle), \right.$$

$$|\beta\rangle = \frac{1}{3^{1/2}}(|0\rangle + \omega|1\rangle + \omega^*|2\rangle),$$

$$\left. |\gamma\rangle = \frac{1}{3^{1/2}}(|0\rangle + \omega^*|1\rangle + \omega|2\rangle) \right\}; \tag{1}$$

$$\left\{ |\alpha'\rangle = \frac{1}{3^{1/2}}(\omega|0\rangle + |1\rangle + |2\rangle), \right.$$

$$|\beta'\rangle = \frac{1}{3^{1/2}}(|0\rangle + \omega|1\rangle + |2\rangle),$$

$$\left. |\gamma'\rangle = \frac{1}{3^{1/2}}(|0\rangle + |1\rangle + \omega|2\rangle) \right\}; \tag{2}$$

$$\left\{ |\alpha''\rangle = \frac{1}{3^{1/2}}(\omega^*|0\rangle + |1\rangle + |2\rangle), \right.$$

$$|\beta''\rangle = \frac{1}{3^{1/2}}(|0\rangle + \omega^*|1\rangle + |2\rangle),$$

$$\left. |\gamma''\rangle = \frac{1}{3^{1/2}}(|0\rangle + |1\rangle + \omega^*|2\rangle) \right\}, \tag{3}$$

where $\omega = \exp(2\pi i/3)$. The above states represent the maximum number of mutually unbiased bases for qutrits. In the present scheme each of the twelve states is transmitted with the same probability.

In [1] the authors study the most simple eavesdropping strategy, based on measuring the state and resending it. For this case they find that the present protocol leads to a higher security than a 2-dimensional one. In the following section we will generalize this result by deriving the most general eavesdropping strategy for single qutrits, and by showing that a security higher than for the qubit protocol is also achieved in this more general scenario.

4. Optimal eavesdropping

As mentioned above, we concentrate our attention on incoherent attacks, namely we assume that the eavesdropper interacts with a single 3-dimensional quantum system at a time. We study the case where the action of the eavesdropper disturbs all the possible quantum states by the same amount. The most general unitary eavesdropping strategy for a set of qutrits which disturbs the basis states $\{|0\rangle, |1\rangle, |2\rangle\}$ in the same way can be written as

$$\mathcal{U}|0\rangle|A\rangle = (1-D)^{1/2}|0\rangle|A_0\rangle + \left(\frac{D}{2}\right)^{1/2}|1\rangle|A_1\rangle + \left(\frac{D}{2}\right)^{1/2}|2\rangle|A_2\rangle,$$

$$\mathcal{U}|1\rangle|A\rangle = \left(\frac{D}{2}\right)^{1/2}|0\rangle|B_0\rangle + (1-D)^{1/2}|1\rangle|B_1\rangle + \left(\frac{D}{2}\right)^{1/2}|2\rangle|B_2\rangle, \tag{4}$$

$$\mathcal{U}|2\rangle|A\rangle = \left(\frac{D}{2}\right)^{1/2}|0\rangle|C_0\rangle + \left(\frac{D}{2}\right)^{1/2}|1\rangle|C_1\rangle + (1-D)^{1/2}|2\rangle|C_2\rangle.$$

Here $1-D$ is the fidelity of the state that arrives at Bob's site after Eve's interaction. The disturbance is given by D. We assume the disturbance of the two basis states that are orthogonal to the original to be equal: this symmetry is motivated by the fact that the three basis states should be treated in the same manner. The initial state of Eve's system is called $|A\rangle$, and her states after interaction are labelled $|A_0\rangle, |B_0\rangle, \ldots$ and are normalized. Their dimension is not fixed.

We have to satisfy the unitarity of $\mathcal{U}$. This leads to the constraints

$$\left(\frac{D(1-D)}{2}\right)^{1/2}(\langle B_0|A_0\rangle + \langle B_1|A_1\rangle) + \frac{D}{2}\langle B_2|A_2\rangle = 0,$$

$$\left(\frac{D(1-D)}{2}\right)^{1/2}(\langle C_2|A_2\rangle + \langle C_0|A_0\rangle) + \frac{D}{2}\langle C_1|A_1\rangle = 0, \tag{5}$$

$$\left(\frac{D(1-D)}{2}\right)^{1/2}(\langle C_1|B_1\rangle + \langle C_2|B_2\rangle) + \frac{D}{2}\langle C_0|B_0\rangle = 0.$$

We restrict ourselves to the case of symmetric attacks, i.e. Eve is supposed to introduce an equal disturbance to all possible input states written in the previous section†. We can then directly compare the security to schemes for qubits, mentioned in section 2, where only symmetric attacks have been studied. By imposing that the disturbance $D = 1 - \mathrm{Tr}\,(|\psi_i\rangle\langle\psi_i|\varrho_{\mathrm{B}}^{\mathrm{out}})$, where $\varrho_{\mathrm{B}}^{\mathrm{out}}$ is the reduced density operator of the state sent on to Bob, takes the same value for all 12 possible input states $|\psi_i\rangle$, introduced in the previous section, we derive the following relations that involve the scalar products of Eve's output states:

$$[2D(1-D)]^{1/2}(\langle A_1|A_0\rangle + \langle B_1|B_0\rangle + \langle C_2|B_0\rangle + \langle A_1|C_2\rangle) + D(\langle C_1|C_0\rangle + 3\langle B_0|A_1\rangle) = 0, \tag{6}$$

$$[2D(1-D)]^{1/2}(\langle B_1|C_0\rangle + \langle A_2|B_1\rangle + \langle A_2|A_0\rangle + \langle C_2|C_0\rangle) + D(\langle B_2|B_0\rangle + 3\langle C_0|A_2\rangle) = 0, \tag{7}$$

$$[2D(1-D)]^{1/2}(\langle B_2|B_1\rangle + \langle C_2|C_1\rangle + \langle B_2|A_0\rangle + \langle A_0|C_1\rangle) + D(\langle A_2|A_1\rangle + 3\langle C_1|B_2\rangle) = 0, \tag{8}$$

$$\langle A_1|C_0\rangle + \langle A_2|B_0\rangle + \langle B_0|C_1\rangle + \langle B_2|A_1\rangle + \langle C_1|A_2\rangle + \langle C_0|B_2\rangle = 0. \tag{9}$$

†If the noise of the physical device is known to be symmetric, then Alice and Bob could detect an asymmetric evesdropper by checking the error rate in a subset of states. Otherwise, the trade-off between Eve's information and the signal key is more complicated to handle.

Note that both the real and the imaginary part of these expressions have to vanish. Writing the disturbance introduced through the eavesdropping transformation (4) as a function of the scalar products of Eve's states, and taking into account unitarity (5) and the conditions (6)–(9), we find the following simple form:

$$D = 2\frac{1-S}{3-2S}, \tag{10}$$

where $S = \mathrm{Re}\,[\langle A_0|B_1\rangle + \langle B_1|C_2\rangle + \langle C_2|A_0\rangle]/3$. Notice that in the expression for the disturbance only the scalar products among the eavesdropper's states $|A_0\rangle$, $|B_1\rangle$ and $|C_2\rangle$ appear, while all the others do not contribute.

We will now derive the optimal eavesdropping transformation for a fixed value D of the disturbance, namely we maximize the mutual information I_{AE} between Alice and Eve. (This is a standard figure of merit for the description of the efficiency of an eavesdropping attack [5].) As mentioned above, the disturbance introduced by Eve is independent of the scalar products of her states, apart from the ones involving $|A_0\rangle$, $|B_1\rangle$ and $|C_2\rangle$. Therefore, for any value of D, Eve is free to choose those states on which D does not depend in such a way that she retrieves the maximal information. The optimal choice is to take all of these states orthogonal to each other, because in this case Eve can infer the original state sent by Alice in an unambiguous way from her measured state.

For symmetry reasons we assume that the three scalar products that appear in S have the same value, and choose them such that the mutual information is maximized for fixed S, i.e. for a given disturbance D. Without loss of generality we can take the scalar products to be real.

With this strategy we find the optimal mutual information between Alice and Eve to be

$$I_{\mathrm{AE}} = 1 + (1-D)\left[f(D)\,\log_3 f(D) + (1-f(D))\,\log_3\frac{1-f(D)}{2}\right], \tag{11}$$

where $f(D)$ is given by

$$f(D) = \frac{3-2D+2(2^{1/2})[D(3-4D)]^{1/2}}{9(1-D)}. \tag{12}$$

As we can see, Eve needs to employ two three-level systems for the optimal attack. The information for Bob decreases with increasing disturbance and takes the form

$$I_{\mathrm{AB}} = 1 + (1-D)\,\log_3(1-D) + D\,\log_3\frac{D}{2}. \tag{13}$$

Note that we renormalized the functions given in (11) and (13), as in [1], in order to be able to directly relate the values to the 2-dimensional case. We will now compare the security of the 3-dimensional scenario as described above with the

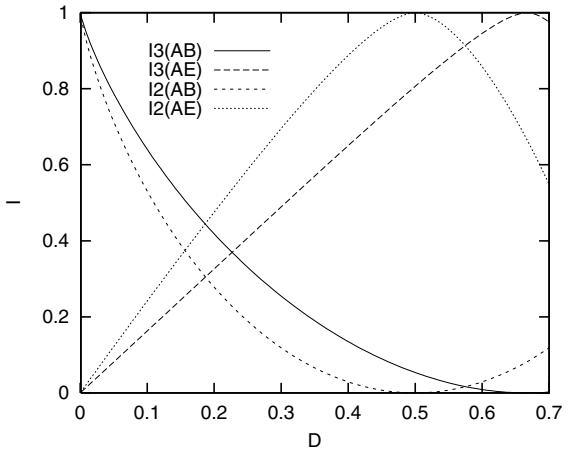

Figure 2. Mutual information for Alice/Bob and Alice/Eve as a function of the disturbance, for 2-dimensional and 3-dimensional quantum states.

most secure 2-dimensional scheme, the six-states protocol. The according information curves of both protocols are shown in figure 2.

We find that the 3-dimensional protocol is more secure in two respects: first, the information curves for Bob and Eve intersect at a higher disturbance D_c than for the 2-dimensional case, namely $D_{c,3} = 0.227$, while $D_{c,2} = 0.156$. In other words, Eve has to introduce *more* noise in order to gain the same information as Bob. In general, for disturbances $D < D_c$, a key distribution protocol can be considered secure, because $I_{AB} > I_{AE}$ [5]. Therefore, the 3-dimensional protocol is secure up to higher disturbances. Second, for a fixed disturbance $D < D_c$, Bob gets more and Eve less information than in the 2-dimensional case. The price that has to be payed for higher security is a lower efficiency: the basis for Bob matches the one of Alice in fewer cases than for two dimensions, as the number of bases is increased.

Notice that our derivation of the optimal eavesdropping transformation relies on equations (6)–(9) which guarantee that all the possible input states are disturbed in the same way. The resulting optimal transformation turns out to be a universal transformation for a qutrit state, in the sense that any input qutrit state, not only the twelve ones employed in the cryptographic scheme, is disturbed by the same amount D. Therefore, the present scheme based on the use of the maximum number of mutually unbiased bases is optimal for qutrits because if we increase the number of bases we do not achieve a higher security. Notice also that if we reduce the number of bases, not all of the conditions (6)–(9) will be necessary, thus leading to a less simple structure of D than the one given in (10). This would allow a different general form of the optimal eavesdropping transformation, and a higher curve for I_{AE} (for example, a lower bound on the I_{AE} curve for the case of two mutually unbiased bases was presented in [8]).

5. Generalization to higher-dimensional systems

Generalizing the ansatz given in (4) to higher dimensions, we find a lower bound on the eavesdropper's information for quantum cryptography with d-dimensional systems. The general ansatz is then

$$\mathcal{U}|0\rangle|A\rangle = (1-D)^{1/2}|0\rangle|A_0\rangle + \left(\frac{D}{d-1}\right)^{1/2}|1\rangle|A_1\rangle + \cdots,$$
$$\mathcal{U}|1\rangle|A\rangle = \left(\frac{D}{d-1}\right)^{1/2}|0\rangle|B_0\rangle + (1-D)^{1/2}|1\rangle|B_1\rangle + \cdots,$$
$$\vdots$$
$$\mathcal{U}|d-1\rangle|A\rangle = \left(\frac{D}{d-1}\right)^{1/2}|0\rangle|Z_0\rangle + \left(\frac{D}{d-1}\right)^{1/2}|1\rangle|Z_1\rangle + \cdots. \tag{14}$$

(The alphabet denoting Eve's states is supposed to contain d letters.) The accordingly generalized formula for the disturbance as a function of the scalar products is

$$D = \frac{(d-1)(1-S)}{d-S(d-1)}, \tag{15}$$

where S is now the real part of the average of all possible scalar products between $|A_0\rangle, |B_1\rangle, \ldots$. The function f is then given by

$$f_d(D) = \frac{d-2D+[(d-2D)^2 - d^2(1-2D)^2]^{1/2}}{d^2(1-D)}. \tag{16}$$

In figure 3 we plot Eve's corresponding information

$$I_{AE,d} = 1 + (1-D)\left[f_d(D)\,\log_d f_d(D) + (1-f_d(D))\,\log_d \frac{1-f_d(D)}{d-1}\right], \tag{17}$$

as a function of the dimension d for a fixed value of the disturbance D. We conjecture that this mutual information is optimal when employing the maximal number of mutually unbiased bases for a given dimension. The maximum number of mutually unbiased bases is known to be $d+1$ only for specific cases, namely when the dimension is a power of a prime number [9]. In these cases the cryptographic scheme based on the use of the maximum number of mutually

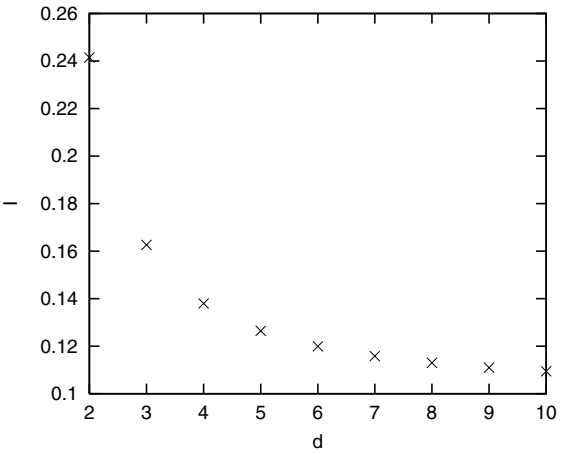

Figure 3. Mutual information between Eve and Alice as a function of the dimension, for $D = 0.1$.

unbiased bases would employ $d(d+1)$ equiprobable states. In the other cases the problem of finding the maximum number of mutually unbiased bases is still open.

We want to point out that in general the optimal eavesdropping strategy on the maximum number of mutually unbiased bases does not need to be a universal transformation. As mentioned in the previous sections, this is however the case for qubits and qutrits, but was not proven for higher dimensions. For a universal transformation we expect that the high symmetry of the ansatz would make the optimality problem easier to solve. At the moment, optimality of the curve given in equation (17) remains a conjecture.

6. Conclusions

We now summarize the main results shown in this paper. We have found a remarkable feature of higher-dimensional quantum systems: following the approach of [3], we have proven analytically for dimension $d = 3$ that the most general incoherent symmetric attack of an eavesdropper gives her less information than in the case of qubits. Therefore a three-dimensional scheme offers higher security than two-dimensional systems. We generalized the upper limit for Eve's information I_{AE} from $d = 3$ to higher dimensions: this limit decreases with the dimension, and numerically we find that it reaches $I_{\mathrm{AE}} = D$ in the limit $d \to \infty$. The optimality of Eve's information curve given in equation (17) is at present still a conjecture for dimensions higher than three.

We finally want to point out that these results are in agreement with the analysis performed in [8], where an eavesdropping strategy originating from an asymmetric cloning transformation was presented. It is interesting to note that the optimal eavesdropping transformations derived so far are related to optimal cloning transformations (in the case of qubits the optimal strategy for the BB84 scheme corresponds to the optimal phase covariant cloning [10], and for the six-state protocol it is related to the optimal asymmetric cloning [11]). However, in general there is not necessarily a connection between optimal eavesdropping strategies and optimal cloning transformations, since cloning transformations are only a subset of our general family of transformations $\mathcal{U}$ given in equation (4). The problem whether there is a fundamental relation between optimal eavesdropping and optimal cloning is of great interest and still open at the moment.

Acknowledgments

We wish to thank Maciej Lewenstein for discussions. This work has been supported by DFG (Schwerpunkt 'Quanteninformationsverarbeitung'), the ESF-Programme PESC, and the EU IST-Programmes EQUIP and ATESIT.

References

[1] BechmannPasquinucci, H., and Peres, A., 2000, *Phys. Rev. Lett.*, **85,** 3313.
[2] Gisin, N., Ribordy, G. G., Tittel, W., and Zbinden, H., 2002, *Rev. mod. Phys.*, **74,** 145.
[3] Bruß, D., and Macchiavello, C., 2002, *Phys. Rev. Lett.*, **88,** 127901.
[4] Bennett, C. H., and Brassard, G., 1984, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (New York: IEEE), pp. 175–179.

[5] Fuchs, C., Gisin, N., Griths, R., Niu, C.S., and Peres, A., 1997, *Phys. Rev.* A, **56,** 1163.
[6] Bruß, D., 1998, *Phys. Rev. Lett.*, **81,** 3018.
[7] BechmannPasquinucci, H., and Gisin, N., 1999, *Phys. Rev.* A, **59,** 4238.
[8] Cerf, N., Bourennane, M., Karlsson A., and Gisin, N., 2002, *Phys. Rev. Lett.*, **88,** 127902.
[9] Wootters, W. K., and Fields, B. D., 1989, *Ann. Phys.* (New York), **191,** 363.
[10] Bruß, D., Cinchetti, M., Dariano, G. M., and Macchiavello, C., 2000, *Phys. Rev.* A, **62,** 12302.
[11] Cerf, N., 2000, *Phys. Rev. Lett.*, **84,** 4497.