Security of Quantum Key Distribution Using *d*-Level Systems

Cerf, Nicolas J.; Bourennane, Mohamed; Karlsson, Anders; Gisin, Nicolas

How to cite

CERF, Nicolas J. et al. Security of Quantum Key Distribution Using *d*-Level Systems. In: Physical review letters, 2002, vol. 88, n° 12. doi: 10.1103/PhysRevLett.88.127902

This publication URL: https://archive-ouverte.unige.ch/unige:36785
Publication DOI: 10.1103/PhysRevLett.88.127902

Security of Quantum Key Distribution Using d-Level Systems

Nicolas J. Cerf,[1,2] Mohamed Bourennane,[3] Anders Karlsson,[3] and Nicolas Gisin[4]

[1]*Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*
[2]*Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California 91109*
[3]*Department of Microelectronics and Information Technology, Royal Institute of Technology (KTH), Electrum 229, SE-164 Kista, Sweden*
[4]*GAP-Optique, Université de Genève, 20 rue de l'Ecole de Médecine, Genève 4, Switzerland*

(Received 26 July 2001; published 8 March 2002)

We consider two quantum cryptographic schemes relying on encoding the key into *qudits,* i.e., quantum states in a d-dimensional Hilbert space. The first cryptosystem uses two mutually unbiased bases (thereby extending the BB84 scheme), while the second exploits all $d + 1$ available such bases (extending the six-state protocol for qubits). We derive the information gained by a potential eavesdropper applying a cloning-based individual attack, along with an upper bound on the error rate that ensures unconditional security against coherent attacks.

DOI: 10.1103/PhysRevLett.88.127902 PACS numbers: 03.67.Dd, 03.67.Hk, 89.70.+c

Quantum key distribution is probably one of the most promising concepts in quantum information theory, and has been extensively studied both theoretically and experimentally since its discovery by Bennett and Brassard in 1984 [1]. This cryptographic method allows two remote parties to share a secret key by use of a quantum channel supplemented with a public authenticated classical channel (see, e.g., [2] for a review). The impossibility for an eavesdropper to tap the quantum channel without disturbing the communicated data—in a way that can, in principle, be detected using the classical channel—ensures the security of the key distribution. Most of the research effort to date has focused on quantum cryptosystems based on two-dimensional quantum variables (qubits) carried, e.g., by the polarization state of individual photons. In particular, the optimal individual attack is now known both for the BB84 protocol (using two mutually unbiased bases [3]) and for the six-state protocol (using all three mutually unbiased bases [4,5]). Strong bounds have also been derived in the more general case of coherent attacks, which are useful to assess the security of quantum cryptography (see, e.g., [6–8]). For higher-dimensional systems, however, very few results have been obtained on the resistance to eavesdropping of *qudit*-based schemes (i.e., schemes based on encoding the key on d-level systems). The only schemes that have been considered use either two bases for a four-level system [9] or four bases for a qutrit [10], but their security was investigated against simple nonoptimal attacks only.

In this Letter, we investigate more general quantum cryptosystems where the encoding is made into qudits with arbitrary d, extending on an earlier study by some of us that considered only simple individual attacks [11]. A first protocol we study consists in using two mutually unbiased bases, just as in the original BB84 scheme. The sender Alice sends a basis state in one of these two bases chosen at random, while the receiver Bob makes a measurement in one of these two bases, again at random. The basis used by each party is subsequently disclosed on the public channel, so that Alice and Bob obtain correlated d-ary random variables if they used the same bases (and if there was no disturbance on the channel), which happens with probability $1/2$. The use of mutually unbiased (or complementary) bases implies that if Alice and Bob use different bases, Bob's measurement yields a random number that is uncorrelated with Alice's state. The raw secret key is then made out of the correlated data (discarding the uncorrelated data is known as the sifting procedure). This procedure ensures that any attempt by an eavesdropper Eve (oblivious of the chosen basis) to gain information on Alice's state induces errors in the transmission, which can then be detected by the legitimate parties. In the second qudit-based protocol that we study, Alice and Bob choose their basis at random among all $d + 1$ mutually unbiased bases that are available in a d-dimensional Hilbert space, much in the same way as in the six-state protocol for qubits. Note that these bases are only known for d being a power of a prime number [12], so the protocol is only defined then. This second protocol clearly has a lower yield than the first one since the sifting procedure only keeps one transmission out of $d + 1$ (instead of $1/2$). However, as we shall see, it is more secure against individual attacks in the sense that a slightly higher error rate is acceptable.

In what follows, we will analyze the security of these two cryptographic protocols against individual attacks (where Eve monitors the qudits separately) as well as coherent attacks (where Eve monitors several qudits jointly). For the individual case, we consider a fairly general class of eavesdropping attacks that are based on (not necessarily universal) quantum cloning machines. It is known for qubits that such a cloning-based attack is the optimal eavesdropping strategy, that is, the best Eve can do is to clone (imperfectly) Alice's qubit and keep a copy while sending the original to Bob. An appropriate measurement of the clone (and the ancilla system) after disclosure of the basis enables Eve to gain the maximum

possible information on Alice's key bit. Extending this cloning-based attack to higher dimensions results in a lower bound on the information accessible to Eve for a given error rate. Hence, this yields an upper bound on the error rate, which is a *necessary* condition for security against individual attacks (higher error rates cannot permit one to establish a secret key using one-way communication). We argue that applying the optimal cloner is actually the best strategy for Eve in any dimension, so that this bound is tight. For coherent attacks, we consider a situation where Eve interacts with a qudit sequence of arbitrary (but finite) length and then uses the basis information to extract key information. In particular, we make use of an information uncertainty principle to derive a lower bound on Bob's information, or, equivalently, an upper bound on the error rate. It is a *sufficient* condition for the protocol to be guaranteed to generate a nonzero net key rate for all finite-length attacks.

Let us consider first an individual eavesdropping based on the use of a quantum cloning machine for qudits. The particular cloning machine that is best to use depends on whether the protocol uses two bases or $d + 1$ bases. We focus on the case of two bases first, for which we need to use a cloner that copies equally well two mutually unbiased bases, e.g., the computational basis $\{|k\rangle\}$, with $k = 0, \ldots, d - 1$, and its dual under a Fourier transform

$$|\bar{l}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{2\pi i(kl/d)} |k\rangle, \tag{1}$$

with $l = 0, \ldots, d - 1$. We use a general class of cloning transformations as defined in [13]. If Alice sends the state $|\psi\rangle$, the transformation reads

$$|\psi\rangle_A \rightarrow \sum_{m,n=0}^{d-1} a_{m,n} U_{m,n} |\psi\rangle_B |B_{m,-n}\rangle_{E,E'}, \tag{2}$$

where A, B, E, and E' stand for Alice's qudit, Bob's clone, Eve's clone, and the cloning machine, respectively. Here, the amplitudes $a_{m,n}$ (with $\sum_{m,n=0}^{d-1} |a_{m,n}|^2 = 1$) characterize the cloner, while the states $|B_{m,n}\rangle_{EE'}$ are d-dimensional Bell states, that is, a set of d^2 orthonormal maximally entangled states of two qudits,

$$|B_{m,n}\rangle_{EE'} = \frac{1}{\sqrt{d}} \sum_{k=0}^{N-1} e^{2\pi i(kn/d)} |k\rangle_E |k + m\rangle_{E'} \tag{3}$$

with $m, n = 0, \ldots, d - 1$. Note that the kets must be taken modulo d here. The operators $U_{m,n}$ defined as

$$U_{m,n} = \sum_{k=0}^{d-1} e^{2\pi i(kn/d)} |k + m\rangle\langle k| \tag{4}$$

form a group of qudit error operators, generalizing the Pauli matrices for qubits: m labels the shift errors (extending the bit flip σ_x), while n labels the phase errors (extending the phase flip σ_z). Tracing the output joint state of Eq. (2) over EE' implies that Alice's state $|\psi\rangle_A$ is transformed, at Bob's station, into the mixture

$$\rho_B = \sum_{m,n=0}^{d-1} |a_{m,n}|^2 U_{m,n} |\psi\rangle\langle\psi| U_{m,n}^{\dagger}. \tag{5}$$

Thus, the state undergoes a $U_{m,n}$ error with probability $|a_{m,n}|^2$. If Alice sends any state $|k\rangle$ in the computational basis, the phase errors ($n \neq 0$) clearly do not play any role in the above mixture since $U_{m,n}|k\rangle = e^{2\pi i(kn/d)}|k + m\rangle$, so Bob's fidelity can be expressed as

$$F = \langle k|\rho_B|k\rangle = \sum_{n=0}^{d-1} |a_{0,n}|^2. \tag{6}$$

In the complementary basis, we have $U_{m,n}|\bar{l}\rangle = e^{-2\pi i(l+n)m/d}|\overline{l + n}\rangle$, so the shift errors ($m \neq 0$) do not play any role and Bob's fidelity becomes

$$\overline{F} = \langle\bar{l}|\rho_B|\bar{l}\rangle = \sum_{m=0}^{d-1} |a_{m,0}|^2. \tag{7}$$

For the cloner to copy equally well the states of both bases, we choose a $d \times d$ amplitude matrix of the form

$$a = \begin{pmatrix} v & x & \cdots & x \\ x & y & \cdots & y \\ \vdots & \vdots & \ddots & \vdots \\ x & y & \cdots & y \end{pmatrix}, \tag{8}$$

with x, y, and v being real variables satisfying the normalization condition $v^2 + 2(d - 1)x^2 + (d - 1)^2 y^2 = 1$. Thus, Bob's fidelity is $F = v^2 + (d - 1)x^2$ in both bases, and the corresponding mutual information between Alice and Bob (if the latter measures his clone in the good basis) is given by

$$I_{AB} = \log_2 d + F \log_2 F + (1 - F) \log_2 \left(\frac{1 - F}{d - 1} \right) \tag{9}$$

since the $d - 1$ possible errors are equiprobable.

The clone kept by Eve can be shown to be in a state given by an expression similar to Eq. (5) but with the amplitudes $a_{m,n}$ replaced by their Fourier transform [13]

$$b_{m,n} = \frac{1}{d} \sum_{m',n'=0}^{d-1} e^{2\pi i(nm' - mn')/d} a_{m',n'}. \tag{10}$$

This corresponds to a matrix similar to Eq. (8) but with

$$\begin{aligned} x \rightarrow x' &= [v + (d - 2)x + (1 - d)y]/d, \\ y \rightarrow y' &= (v - 2x + y)/d, \\ v \rightarrow v' &= [v + 2(d - 1)x + (d - 1)^2 y]/d, \end{aligned} \tag{11}$$

resulting in a cloning fidelity for Eve given by $F_E = v'^2 + (d - 1)x'^2$. Maximizing Eve's fidelity F_E for a given value of Bob's fidelity F (using the normalization relation) yields the optimal cloner:

$$x = \sqrt{\frac{F(1 - F)}{d - 1}}, \qquad y = \frac{1 - F}{d - 1}, \qquad v = F. \tag{12}$$

The corresponding optimal fidelity for Eve is

$$F_E = \frac{F}{d} + \frac{(d-1)(1-F)}{d} + \frac{2}{d}\sqrt{(d-1)F(1-F)}. \quad (13)$$

Let us see how Eve can maximize her information on Alice's state. If Alice sends the state $|k\rangle$, then it is clear from Eq. (2) that Eve can obtain Bob's error m simply by performing a partial Bell measurement (measuring only the m index) on EE'. Then, it appears from Eqs. (8) and (12) that, in order to infer Alice's state, Eve must distinguish between d nonorthogonal states (corresponding to all possible values of k) with a same scalar product $(dF-1)/(d-1)$ for all pairs of states, regardless of the measured value of m. Consequently, Eve's information I_{AE} is simply given by the same expression as Eq. (9) but replacing F by F_E. As a result, Bob's and Eve's information curves intersect exactly where the fidelities coincide, that is, at

$$F = F_E = \frac{1}{2}\left(1 + \frac{1}{\sqrt{d}}\right). \quad (14)$$

We now use a theorem due to Csiszár and Körner [14], which provides a lower bound on the secret key rate, that is, the rate R at which Alice and Bob can generate secret key bits via privacy amplification: if Alice, Bob, and Eve share many independent realizations of a probability distribution $p(a,b,e)$, then there exists a protocol that generates a number of key bits per realization satisfying

$$R \geq \max(I_{AB} - I_{AE}, I_{AB} - I_{BE}). \quad (15)$$

It is therefore sufficient that $I_{AB} > I_{AE}$ in order to establish a secret key with a nonzero rate. If we restrict ourselves to one-way communication on the classical channel, this actually is also a necessary condition. Consequently, the quantum cryptographic protocol above ceases to generate secret key bits precisely at the point where Eve's information attains Bob's information. In Table I, we have computed the disturbance $D = 1 - F$ (or error rate) at which $I_{AB} = I_{AE}$ (or $F = F_E$), that is, above which Alice and Bob cannot distill a secret key any more by use of one-way privacy amplification protocols. Strictly speaking, since we only conjectured here that the cloning-based attack is optimal for all d, D_2^{ind} is actually only an upper bound on D that cannot be exceeded to generate secret key bits with one-way protocols. Interestingly, we note that D_2^{ind} increases with the dimension d, suggesting that a cryptosystem based on qudits is more secure for large d.

Now, we consider the second protocol where all $d+1$ bases are used for d being a power of any prime number. The cloner that must be used then is an asymmetric universal cloner [13], characterized by an amplitude matrix of the same form as (8) but with $x = y$, the normalization relation becoming $v^2 + (d^2-1)x^2 = 1$. Here, Bob's fidelity is given by $F = v^2 + (d-1)x^2 = 1 - d(d-1)x^2$, so that the cloner is characterized by

TABLE I. Disturbance $D = 1 - F$ (or error rate) as a function of the dimension d. The columns D_2^{ind} and D_{d+1}^{ind} display the values of D at which $I_{AB} = I_{AE}$ for a cloning-based individual attack with the two-bases or $(d+1)$-bases protocol, respectively. The column D^{coh} corresponds to an upper bound on D that guarantees security against coherent attacks.

d	D_2^{ind} (%)	D_{d+1}^{ind} (%)	D^{coh} (%)
2	14.64	15.64	11.00
3	21.13	22.67	15.95
4	25	26.66	18.93
5	27.64	29.23	20.99
8	32.32	33.44	24.70

$$x^2 = \frac{1-F}{d(d-1)}, \qquad v^2 = \frac{(d+1)F-1}{d}. \quad (16)$$

As before, Bob's information is given by Eq. (9). Eve's clone is characterized by a matrix of the same form, with

$$x \to x' = (v - x)/d$$
$$v \to v' = [v + (d^2-1)x]/d, \quad (17)$$

so the corresponding fidelity is $F_E = v'^2 + (d-1)x'^2 = 1 - d(d-1)x'^2$. For deriving Eve's information, we need first to rewrite the cloning transformation as

$$|k\rangle_A \to \frac{v-x}{\sqrt{d}}|k\rangle_B \sum_{l=0}^{d-1}|l\rangle_E|l\rangle_{E'} + x\sqrt{d}\sum_{m=0}^{d-1}|k+m\rangle_B|k\rangle_E|k+m\rangle_{E'}. \quad (18)$$

After the basis is disclosed, Eve's strategy is first to measure both E and E', the difference (modulo d) of the outcomes simply giving Bob's error m. Making use of $v - x = x'd$ and expressing x and x' as functions of F and F_E, it is easy to check that the best Eve can do then is to use the state of her clone E as an estimate of Alice's state $|k\rangle$. If Bob makes no error ($m = 0$), which happens with probability F, then this yields the correct value of k with probability $(F + F_E - 1)/F$, while it yields any other of the $d-1$ possibilities $l \neq k$ with probability $(1 - F_E)/[(d-1)F]$. In contrast, if Bob makes an error ($m \neq 0$), then Eve obtains the right k with probability one. Consequently, the average mutual information between Alice and Eve conditionally on Bob's error m can be written as

$$I_{AE} = \log_2 d + (F + F_E - 1)\log_2\left(\frac{F + F_E - 1}{F}\right) + (1 - F_E)\log_2\left(\frac{1 - F_E}{(d-1)F}\right). \quad (19)$$

One can check that, for a given F, I_{AE} is slightly lower here than for the two-bases protocol, which is consistent with the stronger requirement that we put on the cloner. Therefore, the fidelity F at which $I_{AB} = I_{AE}$ is slightly

lower, and the corresponding disturbance $D = 1 - F$ is slightly higher. In Table I, we have shown the corresponding upper bound D_{d+1}^{ind} for several values of d, illustrating that there is a slight advantage in using all $d + 1$ bases, as for the six-state protocol for qubits [4,5].

Our last result concerns an eavesdropping strategy that consists in applying a coherent attack on a qudit sequence of arbitrary but finite length n. Actually, our reasoning is simpler to state with a single qudit ($n = 1$), but it remains valid for $n > 1$ [15]. We use here an uncertainty principle due to Hall [16] that puts a limit on the sum of Bob's and Eve's information when both parties measure a same quantum system: if $\hat{B}$ and $\hat{E}$ are Bob's and Eve's observables applied on the qudit sent by Alice, then

$$I_{AB} + I_{AE} \leq 2 \log_2 (d \max_{i,j} |\langle b_i | e_j \rangle|), \qquad (20)$$

where $|b_i\rangle$ and $|e_j\rangle$ are the eigenstates of $\hat{B}$ and $\hat{E}$, respectively. This inequality holds with I_{AB} and I_{AE} being information on the qudit without knowledge of the basis chosen by Alice. However, by symmetry, it can be shown that Bob and Eve get the same average information when measuring the good or wrong basis, so that Eq. (20) also holds with information conditional on the chosen basis, as needed in a quantum cryptographic context [6]. Thus, one gets the tighter possible upper bound on I_{AE} for a given I_{AB} by assuming that Eve measures an observable $\hat{E}$ complementary to $\hat{B}$ (i.e. $|\langle b_i | e_j \rangle| = d^{-1/2}, \forall i, j$):

$$I_{AB} + I_{AE} \leq \log_2 (d). \qquad (21)$$

According to the discussion following Eq. (15), we conclude that $I_{AB} > \log_2(d)/2$ is a sufficient condition to warrant security against coherent attacks if the key is made out of a large number of independent realizations of n-qudit sequences (i.e., if the key is much longer than n). Using Eq. (9), this translates into a lower bound on F, or, equivalently, an upper bound on D

$$F \log_2 \left(\frac{1}{F} \right) + (1 - F) \log_2 \left(\frac{d - 1}{1 - F} \right) < \frac{\log_2 d}{2}, \qquad (22)$$

which guarantees that one can distill secret key bits. This bound, shown in Table I, exactly coincides with the well-known 11% security threshold for unlimited-length coherent attacks on qubits ($d = 2$) [8].

In summary, we have extended standard quantum cryptography to protocols where the key is carried by quantum states in a space of arbitrary dimension d. We have used a general model of quantum cloning in order to calculate the information accessible to an eavesdropper monitoring the qudits individually. This provides an upper bound on the error rate above which the legitimate parties cannot distill a secret key by use of one-way privacy amplification protocols (since $I_{AB} < I_{AE}$). Our analysis also suggested that the two-bases protocol should be preferred to a $(d + 1)$-bases one since its maximum acceptable error rate is only slightly lower, while the corresponding secret key rate is much larger. Finally, we have derived a very simple security proof of quantum cryptography with qudits that exploits an intuitive information inequality constraining the simultaneous measurement of conjugate observables. This results in an upper bound on the acceptable error rate that is more restrictive than the previous one, but guarantees that a nonzero secret key rate can be produced even with coherent attacks on qudit sequences of finite length. In the region between these two bounds, it is unknown whether the security is guaranteed or not. It should be stressed that all the bounds on D discussed above tend to $1/2$ for $d \to \infty$, reflecting the advantage of using higher-dimensional spaces. Another context where using high d might be advantageous is *key growing,* where an initially shared key is used to choose between two bases, the outcomes generating a longer key. However, practical limitations might be more severe in realistic high-d cryptosystems, in particular the influence of the detector's quantum efficiency and dark count rate. This is discussed in a related paper [15].

Work supported in part by Projects QuComm and EQUIP (EU-IST-FET Programme) and the ESF.

Note added.— After completion of this work, it was proven in an independent paper [17] that the optimal individual attack for qutrits ($d = 3$) when using all four mutually unbiased bases exactly coincides with our results.

[1] 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), pp. 175–179.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. (to be published); also in quant-ph/0101098.
[3] C. A. Fuchs *et al.,* Phys. Rev. A **56**, 1163 (1997).
[4] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).
[5] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[6] D. Mayers, J. Assoc. Comput. Machin. **48**, 351 (2001).
[7] H.-K Lo and H. F. Chau, Science **283**, 2050 (1999).
[8] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[9] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[10] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[11] M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 052313 (2001).
[12] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[13] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000); J. Mod. Opt. **47**, 187 (2000); Acta Phys. Slovaca **48**, 115 (1998).
[14] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[15] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, quant-ph/0106049.
[16] M. J. W. Hall, Phys. Rev. A **55**, 100 (1997).
[17] D. Bruss and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).