Strathprints Institutional Repository

Quantum Cryptography Based On Bell Inequalities for Three-Dimensional System

Dagomir Kaszlikowski,[1] Kelken Chang,[1] D. K. L. Oi,[2] L.C. Kwek,[3] and C.H. Oh[1]

[1]*Department of Physics, Faculty of Science, National University of Singapore, Lower Kent Ridge, Singapore 119260, Republic of Singapore*
[2]*Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, UK*
[3]*National Institute of Education, Nanyang Technological University, 1 Nanyang Walk, Singapore 639798*

We present a crytographic protocol based upon entangled qutrit pairs. We analyse the scheme under a symmetric incoherent attack and plot the region for which the protocol is secure and compare this with the region of violations of certain Bell inequalities.

PACS numbers:

INTRODUCTION

The need to communicate secretly has always been an important issue for military strategists during war time. The one-time pad, first proposed by Vernam, has been shown to be one of the most secure means of encrypting a message provided the key is truly random and the key is as long as the message [1]. However, a major problem with the one-time pad is the establishment of a secure key between the two physically separated parties without the services of a courier. Recently, there has been a major proposal to apply the laws of quantum mechanics to establish this crucial key. This new proposal, called Quantum Key Distribution (QKD) protocols, therefore involves the use of quantum features such as uncertainty principle or quantum correlations to establish a the necessary key and hence provides unconditionally secure communication.

The first Quantum Key Distribution was proposed by Bennett and Brassard (BB84) in 1984 based on the fact that any measurement on an unknown state of a polarized photon by a third party will always disturb the state and hence detectable. An extension of the scheme to three-dimensional quantum states has recently been done [2] and it was shown to be more secure than two-dimensional case. Another well-known variation of QKD is based the idea of an entangled pair and detecting the presence of the eavesdropper using violations of the Bell-Clauser-Horne-Shimony-Holt (Bell-CHSH) inequality [3]. This protocol (Ekert protocol) is fundamentally interesting as it provides an example of how a fundamental problem in quantum mechanics, namely Bell-CHSH inequality and violation of local realism, can be applied to a physical problem. Naturally, one questions if it is possible to extend this latter protocol involving Bell-CHSH inequality to higher dimensional system.

The extension of Bell-CHSH inequality to higher dimensions is a non-trivial and interesting problem. As higher dimensional quantum systems require much less entanglement to be non-separable than two-dimensional systems (qubits), it was suspected that higher dimensional entangled systems may lead to stronger violations of local realism. These results have been shown numerically using linear optimization method by searching for an underlying local realistic joint probability distribution that could reproduce the quantum predictions [4] and confirmed analytically [5, 6].

CRYPTOGRAPHIC KEY

The quantum channel we consider consists of a source producing two qutrits [7], which we denote by A and B, in the maximally entangled state $|\psi\rangle = \frac{1}{\sqrt{3}} \sum_{k=0}^{2} |k\rangle_A \otimes |k\rangle_B$, where $|k\rangle_A$ and $|k\rangle_B$ are the k-th basis state of the qutrit A and B respectively (these basis states can represent, for instance, spatial degrees of freedom of photons). Qutrit A flies towards Alice whereas qutrit B flies towards Bob. Each observer has at his or her disposal a symmetric unbiased six-port beamsplitter.

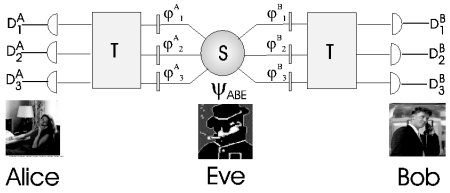

FIG. 1: Qutrit Protocol

An unbiased symmetric six-port beamsplitter performs a unitary transformation between "mutually unbiased" bases in the Hilbert space [8, 9, 10]. Such devices were tested in several quantum optical experiments [11, 12], and also various aspects of such devices were analyzed theoretically [13, 14].

This quantum optical device has three input and three output ports. In front of each input port there is a phase shifter. When all the phase shifters are set to zero an

incoming photon through one of the input ports has an equal chance to leave the device through any of the output ports. The elements of the unitary transformation, which describes its action, are given by

$$U^{k\ell} = \frac{1}{\sqrt{3}}\,\alpha^{k\ell}\,e^{i\varphi_\ell}\,, \tag{1}$$

where $\alpha = e^{2\pi i/3}$ and the indices k, ℓ ($k,\ell = 0,1,2$) denote the input and exit ports respectively; φ_ℓ are the phase shifters. These phase shifters can be changed by an observer. For convenience, we will denote the values of the three phase shifts in the form of a three dimensional vector $\vec{\varphi} = (\varphi_1, \varphi_2, \varphi_3)$. In our protocol both observers perform three distinct unitary transformations on their qutrits. The transformations at Alice's side are defined by the following vectors of phases $\vec{\varphi}_1^A = (0,0,0)$, $\vec{\varphi}_2^A = (0, \frac{\pi}{3}, -\frac{\pi}{3})$, $\vec{\varphi}_3^A = (\pi, 0, -\pi)$ whereas the transformations at Bob's side are defined by $\vec{\varphi}_1^B = (0, \frac{\pi}{6}, -\frac{\pi}{6})$, $\vec{\varphi}_2^B = (0, -\frac{\pi}{6}, \frac{\pi}{6})$, $\vec{\varphi}_3^B = (-\pi, 0, \pi)$. The observers choose their transformations randomly and independently for each pair of incoming qutrits. After performing the transformation defined by the vectors of phases $\vec{\varphi}_m^A, \vec{\varphi}_n^B$ the state $|\psi\rangle$ reads $|\widetilde{\psi}\rangle_{mn} = U_A(\vec{\varphi}_m^A) \otimes U_B(\vec{\varphi}_n^B)|\psi\rangle$. The observers perform the measurement of the state of the qutrit in the basis in which $|\psi\rangle$ is defined, that is, $|0\rangle_x, |1\rangle_x, |2\rangle_x$ ($x = A, B$). We have adopted an uncommon but useful complex value assignment to the results of the measurements, first used in [11]: namely, for the result of the measurement of the ket $|k\rangle_x$ we ascribe the value α^k. This value assignment naturally leads to the following definition of the correlation function $Q(\vec{\varphi}_k^A, \vec{\varphi}_\ell^B)$ ($Q_{k\ell}$ for short) between the values of Alice's and Bob's results of measurements [11]

$$Q_{k\ell} = \sum_{a,b=0}^{2} \alpha^{a+b}\, P(a,b;\vec{\varphi}_k^A, \vec{\varphi}_\ell^B)\,, \tag{2}$$

where $P(a,b;\vec{\varphi}_k^A, \vec{\varphi}_\ell^B)$ denotes the probability of obtaining the result a by Alice and the result b by Bob for the respective values of the phase shifts they have used. It can be shown that the above correlation function reads

$$Q_{k\ell} = \frac{1}{3}\Big[e^{i(\varphi_0^A(k) - \varphi_1^A(k) + \varphi_0^B(\ell) - \varphi_1^B(\ell))} + e^{i(\varphi_1^A(k) - \varphi_2^A(k) + \varphi_1^B(\ell) - \varphi_2^B(\ell))} + e^{i(\varphi_2^A(k) - \varphi_0^A(k) + \varphi_2^B(\ell) - \varphi_0^B(\ell))}\Big]\,, \tag{3}$$

where, for instance, $\varphi_2^A(k)$ denotes the second component of the k-th vector of phases for Alice.

Note that $Q_{33} = 1$. This means that the results of the measurement obtained by Alice and Bob are strictly correlated. When Alice obtains the results $1, \alpha, \alpha^2$ Bob must register the results $1, \alpha^2, \alpha$ respectively. Thus, only the following pairs of the results are possible $\{(1,1), (\alpha, \alpha^2), (\alpha^2, \alpha)\}$ (denoted subsequently by $\{(0,0), (1,2), (2,1)\}$) and each pair of correlations occurs with the same probability equal to $\frac{1}{3}$. Let us also define the following quantity

$$S = \mathrm{Im}(-\alpha^2 Q_{11} + \alpha Q_{12} + \alpha^2 Q_{21} - \alpha^2 Q_{22})\,. \tag{4}$$

It can be shown [15], using the recently discovered Bell inequality for two qutrits [16], that according to local realistic theory S cannot exceed $\sqrt{3}$. However, when using the quantum mechanical correlation function (3), S acquires the value $\frac{2}{3}(2+\sqrt{3})$. Therefore, to violate the above Bell inequality in this case one must reduce the correlation function by the factor $\frac{6\sqrt{3}-9}{2}$ (such reduction is possible by adding the symmetric noise to the system). It has been proved [17] that the above Bell inequality gives necessary and sufficient conditions for local realism in this case.

After the transmission has taken place, Alice and Bob publicly announce the vectors of phase shifts that they have chosen for each particular measurement and divide the measurements into two separate groups: a first group for which they have used the vectors $\vec{\varphi}_1^A$, $\vec{\varphi}_2^A$ and $\vec{\varphi}_1^B$, $\vec{\varphi}_2^B$, and a second group for which they have used $\vec{\varphi}_3^A, \vec{\varphi}_3^B$. Subsequently, Alice and Bob announce in public the results of the measurements they have obtained but only within the first group. In this way they can compute the value of S. If this value is not equal to $\frac{2}{3}(2+\sqrt{3})$ it means that the qutrits have somehow been disturbed. The source of this disturbance can be either an eavesdropper or noise. In case of no disturbance the results from the second group allow them, due to the mentioned correlations, to generate a ternary cryptographic key. For instance when Alice gets the sequence of values, say $(1, \alpha, 1, \alpha^2, \alpha^2, 1, \cdots)$ then Bob must get the following sequence of results, $(1, \alpha^2, 1, \alpha, \alpha, 1, \cdots)$.

EAVESDROPPING

Let us consider a symmetric incoherent attack in which the eavesdropper (Eve) controls the source that produces pairs of qutrits used by Alice and Bob to generate the cryptographic key. Naturally, if Eve wants to acquire any information about the key, she must introduce some disturbance to the state of the qutrits. Her only chance

of being undetected is to hide herself behind what, to Alice and Bob, may look like an environmental noise in the channel. We assume that the noise is symmetrical in the sense that the correlation function in the presence of it reads

$$Q_{noise}(\vec{\phi},\vec{\psi}) = VQ(\vec{\phi},\vec{\psi}), \tag{5}$$

where $0 \leq V \leq 1$. This requirement can only be fulfilled if the reduced state for Alice and Bob (after tracing out Eve's degrees of freedom) is of the form

$$\varrho_{AB} = A|\psi\rangle\langle\psi| + B|\chi_1\rangle\langle\chi_1| + C|\chi_2\rangle\langle\chi_2| + \frac{D}{9} I\otimes I, \tag{6}$$

where the real (not necessarily all positive) numbers $A+B+C+D=1$, and where the maximally entangled orthogonal states $|\chi_k\rangle$ $(k=1,2)$ read

$$\begin{aligned} |\chi_1\rangle &= \frac{1}{\sqrt{3}}(|00\rangle + \alpha|11\rangle + \alpha^2|22\rangle) \\ |\chi_2\rangle &= \frac{1}{\sqrt{3}}(|00\rangle + \alpha^2|11\rangle + \alpha|22\rangle). \end{aligned} \tag{7}$$

This choice of states stems from the fact that only the above states generate correlation functions that are proportional to $Q(\vec{\phi},\vec{\psi})$. To be more specific, the state $|\chi_1\rangle$ gives the correlation function $\alpha Q(\vec{\phi},\vec{\psi})$ whereas the state $|\chi_2\rangle$ gives the correlation function $\alpha^2 Q(\vec{\phi},\vec{\psi})$. Thus, if we compute the correlation function on the state ϱ_{AB}, we arrive at the following formula

$$\begin{aligned} Q_{noise}(\vec{\phi},\vec{\psi}) &= AQ(\vec{\phi},\vec{\psi}) + \alpha BQ(\vec{\phi},\vec{\psi}) + \alpha^2 CQ(\vec{\phi},\vec{\psi}) \\ &= (A+\alpha B+\alpha^2 C)Q(\vec{\phi},\vec{\psi}). \end{aligned} \tag{8}$$

From Eq.(5), we obtain the condition $A+\alpha B+\alpha^2 C = V$, which is only possible if $B=C$ (V is real).

Eve can prepare the reduced density operator (6) by preparing an entangled state of the form,

$$\begin{aligned} |\psi_{ABE}\rangle &= \sqrt{\frac{F}{3}}(|00\rangle|E_{00}\rangle + |11\rangle|E_{11}\rangle + |22\rangle|E_{22}\rangle) \\ &+\sqrt{\frac{G}{6}}(|01\rangle|E_{01}\rangle + |10\rangle|E_{10}\rangle + |20\rangle|E_{20}\rangle \\ &+|02\rangle|E_{20}\rangle + |12\rangle|E_{12}\rangle + |21\rangle|E_{21}\rangle), \end{aligned} \tag{9}$$

where $\{|kl\rangle\}$ are the computational basis states of the two qutrits, and $\{|E_{kl}\rangle\}$ are states of ancilla. Without loss of generality, we can assume that they are normalized (which implies that $F+G=1$). Note that the most general state of the joint system of Alice's and Bob's qutrits and Eve's ancilla reads $\sum_{kl=0}^{2}|kl\rangle|E_{kl}\rangle$. However, Eq. (6) and the requirement that $\varrho_{AB} = \mathrm{Tr}_E(|\psi_{ABE}\rangle\langle\psi_{ABE}|)$ imposes the following conditions on the states of the ancilla

$$\begin{aligned} F\langle E_{kk}|E_{ll}\rangle &= A-B \\ \langle E_{kl}|E_{mn}\rangle &= \delta_{kl}, k\neq l, \end{aligned} \tag{10}$$

Denoting $\langle E_{kk}|E_{ll}\rangle$ by λ we arrive at the following set of conditions

$$\begin{aligned} A+2B+D &= 1 \\ A-B &= F\lambda \\ D &= \frac{3}{2}(1-F). \end{aligned} \tag{11}$$

Eve's strategy is the following. She prepares the state (9), sends the qutrits to Alice and Bob and keeps her ancilla. She then waits for public communication between Alice and Bob. When the settings of Alice's and Bob's apparatus (phase shifts) are revealed, Eve adopts the following algorithm: (i) If the chosen settings are not the ones used for the key generation she ignores the ancilla; (ii) If the settings are the ones for which the key is generated, i.e., $\vec{\varphi}_3^A, \vec{\varphi}_3^B$, she identifies the ancilla state.

Let us first find the transformed state in case (ii), i.e., the state $|\tilde{\psi}_{ABE}\rangle = U_A(\vec{\varphi}_3^A)\otimes U_B(\vec{\varphi}_3^B)\otimes I|\psi_{ABE}\rangle$. A straightforward computation yields

$$|\tilde{\psi}_{ABE}\rangle = \sum_{a,b=0}^{2}|ab\rangle|\tilde{E}_{ab}\rangle, \tag{12}$$

where the un-normalized states $|\tilde{E}_{ab}\rangle$ read

$$\begin{aligned} |\tilde{E}_{ab}\rangle &= \frac{1}{3}\Bigg(\sqrt{\frac{F}{3}}\sum_{k=0}^{2}\alpha^{(a+b)k}e^{i(\varphi_k^A(3)+\varphi_k^B(3))}|E_{kk}\rangle \\ &+ \sqrt{\frac{G}{6}}\sum_{m\neq n}\alpha^{am+bn}e^{i(\varphi_m^A(3)+\varphi_n^B(3))}|E_{mn}\rangle\Bigg) \end{aligned} \tag{13}$$

Note that (12) can also be written more conveniently as

$$\begin{aligned} |\tilde{\psi}_{ABE}\rangle &= \Big(|00\rangle|\tilde{E}_{00}\rangle + |12\rangle|\tilde{E}_{12}\rangle + |21\rangle|\tilde{E}_{21}\rangle\Big) + \Big(|11\rangle|\tilde{E}_{11}\rangle + |20\rangle|\tilde{E}_{20}\rangle + |02\rangle|\tilde{E}_{02}\rangle\Big) \\ &+ \Big(|22\rangle|\tilde{E}_{22}\rangle + |10\rangle|\tilde{E}_{10}\rangle + |01\rangle|\tilde{E}_{01}\rangle\Big), \end{aligned} \tag{14}$$

where we have grouped the terms into three orthogonal subspaces associated with Alice and Bob generating the correct key $\{(0,0),(1,2),(2,1)\}$, and the two incorrect keys, $\{(1,1),(2,0),(0,2)\}$ or $\{(2,2),(1,0),(0,1)\}$. Note also that the ancilla states of one subspace are orthogonal to the ancilla states of the other subspaces.

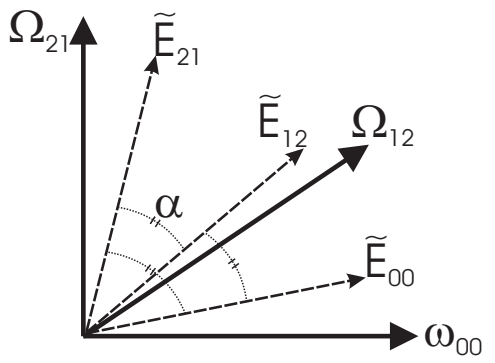

FIG. 2: The optimal three-state discrimination procedure for states in the first subspace. The angle between each of the states is $\alpha = \arccos\tilde{\lambda}_1$.

The probability that Eve projects into the subspaces spanned by the states $\{|\tilde{E}_{00}\rangle, |\tilde{E}_{12}\rangle, |\tilde{E}_{21}\rangle\}$, $\{|E_{11}\rangle, |E_{20}\rangle, |E_{02}\rangle\}$ and $\{|E_{22}\rangle, |E_{10}\rangle, |E_{01}\rangle\}$ are

$$\begin{aligned} P_0 &= 3\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle = \frac{1+2F\lambda}{3} \\ P_1 &= 3\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle = \frac{1-F\lambda}{3} \\ P_2 &= 3\langle\tilde{E}_{22}|\tilde{E}_{22}\rangle = \frac{1-F\lambda}{3}, \end{aligned} \tag{15}$$

respectively. We have considered the fact that the states within each bracket in Eq.(14) have the same norms with the same mutual scalar products. Moreover, these scalar products are all real.

Eve now has to determine the state of her ancilla, given that Alice and Bob have projected the whole state into one of three subspaces associated with the three cases. These subspaces are orthogonal so that Eve can, in principle, determine without error, which of these cases Alice and Bob have.

The three ancilla vectors in each subspace corresponding to the result obtained by Alice and Bob are symmetric and equiprobable. This makes Eve's task of discrimination easier as this case has an analytic optimal solution [18] using the so-called "square-root measurement". We define the operator $\Phi = \sum_{ab} |\tilde{E}_{ab}\rangle\langle\tilde{E}_{ab}|$, where $\{|\tilde{E}_{ab}\rangle\}$ are the ancilla states spanning the subspace associated with Alice and Bob's measurement outcomes. Since we are discriminating 3 vectors in a 3-dimensional space, the optimum measurement directions, $|\omega_{ab}\rangle = \Phi^{-\frac{1}{2}}|\tilde{E}_{ab}\rangle$ are orthogonal, hence Eve simply performs a projective measurement on her ancilla (Fig. 2).

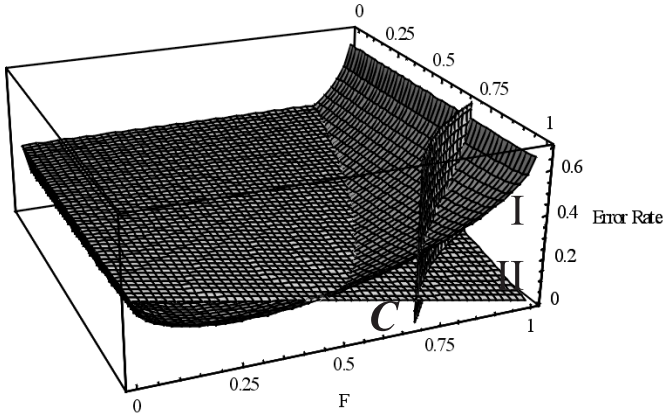

FIG. 3: Three Dimensional Plots of the Error Rates

Thus, Eve's error rate is given by

$$\mathcal{E}_{\rm Eve} = \sum_{i=0}^{3} P_i(1-W_i) \tag{16}$$

where W_i, $(i=1,2,3)$ is the probability of correctly identifying the three states of the ancilla in the i-th subspace. These probabilities are given by

$$W_i = \left(\frac{1}{3}\sqrt{1+2\tilde{\lambda}_i} + \frac{2}{3}\sqrt{1-\tilde{\lambda}_i}\right)^2 \tag{17}$$

where

$$\tilde{\lambda}_1 = \frac{1}{2}\frac{3F+4F\lambda-1}{1+2F\lambda} \tag{18}$$

$$\begin{aligned} \tilde{\lambda}_2 &= \frac{1}{2}\frac{3F-2F\lambda-1}{1-F\lambda} \\ &= \tilde{\lambda}_3 \end{aligned} \tag{19}$$

Due to the symmetry of the noise introduced by Eve, the error rate between Alice and Bob determined using Eq.(6) and the conditions in Eq.(11) is

$$\mathcal{E}_{\rm AB} = \frac{2(1-F\lambda)}{3} \tag{20}$$

We also note that whenever Eve eavesdrops, the correlation function obtained by Alice and Bob is reduced by $F\lambda$. Therefore, if this factor is less than $\frac{6\sqrt{3}-9}{2}$, the Bell inequality is not violated [5] and so Alice and Bob will abort the protocol. This implies that Eve must keep this factor above this value.

Fig.3 shows the three dimensional plots of the error rates of Eve as a function of the parameters F and λ (labeled by surface I) as well as the error rate between Alice and Bob (labeled by surface II). The region in which the factor $F\lambda$ is greater than the threshold value ($V_0 = (6\sqrt{3}-9)/2$) is demarcated by the "wall" labeled $\mathcal{C}$. In

the region bounded by $F\lambda \geq V_0$, the error rate of Eve is always greater than the error rate between Alice and Bob.

An alternative approach to test the security of the protocol against such incoherent symmetric attack is to consider the mutual information between Alice and Eve and compare it with the mutual information between Alice and Bob. The mutual information between Alice and Eve is given by the following expression

$$\begin{aligned}
\mathcal{I}_{\rm AE} &= H(A) + H(E) - H(A;E) \\
&= \log 3 - 3\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle \log\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle - 6\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle \log\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle \\
&\quad -\Big[-3\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle W_1 \log\Big(\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle W_1\Big) - 6\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle (1-W_1)^2 \log\Big(\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle (1-W_1)^2\Big) \\
&\quad -6\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle W_2 \log\Big(\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle W_2\Big) - 12\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle (1-W_2)^2 \log\Big(\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle (1-W_2)^2\Big)\Big], \qquad (21)
\end{aligned}$$

where H is the Shannon entropy. The mutual information between Alice and Bob is

$$\mathcal{I}_{\rm AE} = 2\log 3 + \frac{1}{3}(1+F\lambda)\{\log(1+F\lambda) - \log 9\} + \frac{2}{3}(1-F\lambda)\{\log(1-F\lambda) - \log 9\}. \qquad (22)$$

Fig. 4 shows the plan elevation of the 3-dimensional plots of the mutual information as a function of the parameters F and λ. The line of intersection between $\mathcal{I}_{\rm AE}$ and $\mathcal{I}_{\rm AB}$ clearly lies behind the wall separating the region in which the Bell inequality is violated from the region ($R1$) in which local realistic description is possible ($R2$). In the region $R1$, $\mathcal{I}_{\rm AB} > \mathcal{I}_{\rm AE}$. From numerical calculation, the maximum value of V for which Eve's mutual information equals Alice and Bob's is 0.6629. Thus, Alice and Bob have a buffer region in which to operate securely from this kind of attack by Eve.

To summarize, we have presented a cryptographic protocol using qutrits which is resistant to a form of symmetric, incoherent attacks. The qutrit Bell inequality provides a sufficient condition for secure communication. However, this attack may not be optimal so the Bell inequality may prove to be necessary.

D.K., C.H. Oh and L.C.K. acknowledge financial support provided under the ASTAR Grant No. 012-104-0040. D.K.L.O acknowledges the support of CESG (UK) and QAIP grant IST-1999-11234.

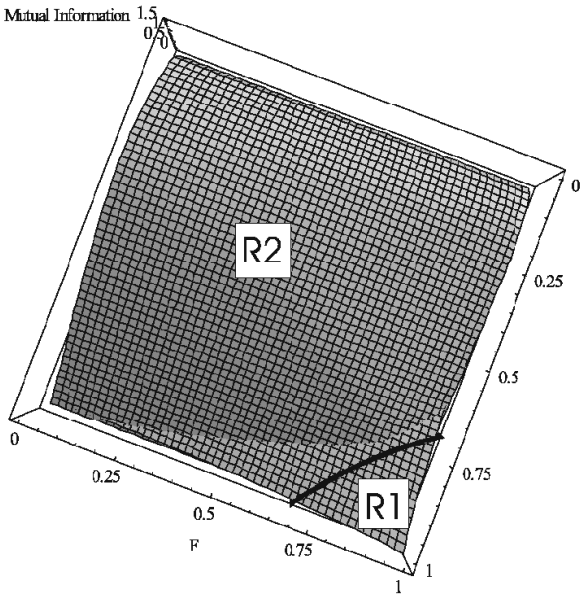

FIG. 4: Plan elevation of 3-dimensional plot of mutual information between Alice-Bob and Alice-Eve.

[1] C.E. Shannon, Bell Syst. Tech. J., **28** 656 (1949).
[2] D. Brußand C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2001).
[3] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).
[5] D. Kaszlikowski, L. C. Kwek, J.-L. Chen, M. Żukowski and C. H. Oh, quant-ph//0106010.
[6] D. Collins, N. Gisin, N. Linden, S. Massar, S. Popescu, quant-ph//0106024.
[7] T. Durt, D. Kaszlikowski, and M. Żukowski, private communication (2000).
[8] J. Schwinger, Proc. Nat. Acad. Sc. **46**, 570 (1960).
[9] I. D. Ivanovic, J. Phys. A **14**, 3241 (1981).
[10] W. K. Wooters, Found. Phys. **16**, 391 (1986).
[11] C. Mattle, M. Michler, H. Weinfurter, A. Zeilinger and

M. Żukowski, Appl. Phys. B **60**, S111 (1995).
[12] M. Reck, PhD Thesis (supervisor: A. Zeilinger) (University of Innsbruck, 1996, unpublished).
[13] M. Reck, A. Zeilinger, H. J. Bernstein and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[14] I. Jex, S. Stenholm and A. Zeilinger, Opt. Comm. **117**, 95 (1995).
[15] Jing-Ling Chen, D. Kaszlikowski, L. C. Kwek and C. H. Oh.
[16] D. Kaszlikowski, L. C. Kwek, Jing Ling Chen, M. Żukowski, and C. H. Oh, Phys. Rev. A **65**, 032118 (2002).
[17] J.L. Chen, D. Kaszlikowski, L.C. Kwek, C.H. Oh and M. Zukowski, Phys. Rev. A, **64**, 052109 (2001).
[18] A. Chefles, *Contemporary Physics* **41**, 401 (2000).