Quantum Information and Computation, Vol. 18, No. 13&14 (2018) 1125–1142

PROPOSAL FOR DIMENSIONALITY TESTING IN QUANTUM PRIVATE QUERY

ARPITA MAITRA
Centre for Theoretical Studies, Indian Institute of Technology Kharagpur Kharagpur-721302, India [a]

BIBHAS ADHIKARI
Department of Mathematics, Indian Institute of Technology Kharagpur Kharagpur-721302, India [b]

SATYABRATA ADHIKARI
Department of Applied Mathematics, Delhi Technological University Delhi-110042, India [c]

Received July 13, 2018
Revised October 3, 2018

Recently, dimensionality testing of a quantum state has received extensive attention (Acín et al. Phys. Rev. Letts. 2006, Scarani et al. Phys. Rev. Letts. 2006). Security proofs of existing quantum information processing protocols rely on the assumption about the dimension of quantum states in which logical bits are encoded. However, removing such assumption may cause security loophole. In the present paper, we show that this is indeed the case. We choose two players' quantum private query protocol by Yang et al. (Quant. Inf. Process. 2014) as an example and show how one player can gain an unfair advantage by changing the dimension of subsystem of a shared quantum system. To resist such attack we propose dimensionality testing in a different way. Our proposal is based on CHSH like game. As we exploit CHSH like game, it can be used to test if the states are product states for which the protocol becomes completely vulnerable.

Keywords: Dimensionality, Qubit-Qutrit Entangled States, CHSH test, Quantum Private Query
Communicated by: S Braunstein & M Mosca

1 Introduction

Testing the dimension of a quantum state has generated a lot of interest recently [1, 2]. Existing quantum information related protocols presume the dimension of the system involved. Removing such assumption may result into security loophole. For example, in a QKD protocol, if one encodes photon polarisation, one must be sure that other properties of the photon, such as spectral line, spatial mode or temporal mode etc. do not change as well [3]. Extra dimensions may carry side-channel information that can be exploited by an eavesdropper. It may happen that the manufacturer of the encryption device herself/himself uses this to insert

[a] *arpita76b@gmail.com*
[b] *bibhas.adhikari@gmail.com*
[c] *tapisatya@gmail.com*

a security backdoor. Thus it has redirected the thoughts to derive bounds for the security proofs of quantum information processing protocols on weaker constraints, i.e., removing the trustworthiness regarding the dimension of the system.

In this direction, detection of the dimension of an unknown quantum system based on a set of conditional probabilities have become a prominent research area [4, 5, 6]. Successful experimental tests are also carried out for testing dimension of a quantum system [7, 8]. However, all these attempts are proposed in a prepare-measurement set up with/without the aid of dimension witnesses [9, 10].

In this paper we develop a CHSH like game which helps in determining the degrees of freedom of the subsystems of an entangled bipartite system. We consider a shared entangled state of the form

$$|\Psi\rangle_{BA} = \frac{1}{\sqrt{2}}(|0\rangle_B |\phi_0\rangle_A + |1\rangle_B |\phi_1\rangle_A). \tag{1}$$

N many states of this form are shared between two legitimate parties Bob and Alice where $\langle\phi_0|\phi_1\rangle_A \neq 0$. Here, $\{|0\rangle_B, |1\rangle_B\}$ denote the computational basis for Bob's qubits and $|\phi_l\rangle_A, l = 0, 1$ denotes qutrits with two degrees of freedom at the place of Alice. Precisely, by the words "two degrees of freedom of a qutrit" we try to convey that the qutrit $|\phi\rangle_l$ is in the span of $\{|i\rangle_A, |j\rangle_A\}, i, j \in \{0, 1, 2\}$. That is, the state is the superposition of any two basis vectors out of the three. The subscripts A and B stand for Alice and Bob respectively.

The dimension testing problem which we consider in this paper certifies whether both $|\phi_0\rangle_A, |\phi_1\rangle_A$ are lying in the same subspace of $\mathbb{C}^3$ or in different subspaces of $\mathbb{C}^3$. Explicitly, the game certifies if $|\phi_0\rangle_A$ and $|\phi_1\rangle_A$ are the superposition of same $\{|i\rangle_A, |j\rangle_A\}$ or the values of i, j differ for the states. We solve the problem by defining a CHSH like game. The proposed game is based on a function which generally familiar as embedded XOR function [11]. We calculate the winning probability of the game for product and entangled states. We notice that the winning probability of the game differs for product state from entangled one. We also notice that if the sub-systems of the entangled pair are not in the same Hilbert space then the winning probability changes abruptly. Observing this success probability one can certify if the states are in a desired form.

This dimension detection problem is motivated by the following reason. Many quantum information retrieval protocols exploit entangled states of the form (1) to establish a secret key between two legitimate partners Bob and Alice. Such a protocol typically starts with sending out a sequence of subsystems of the bipartite systems from Bob to Alice. After sending the states to Alice, Bob measures his qubits sequentially in $\{|0\rangle_B, |1\rangle_B\}$ basis, whereas Alice measures her qubits either in $\{|\phi_0\rangle_A, |\phi_0^\perp\rangle_A\}$ basis or in $\{|\phi_1\rangle_A, |\phi_1^\perp\rangle_A\}$ basis randomly. If the measurement result of Alice gives $|\phi_0^\perp\rangle$, she concludes that the raw key bit at Bob's end must be 1. If it is $|\phi_1^\perp\rangle$, the raw key bit must be 0. Bob and Alice execute classical post-processing so that Alice's information on the key reduces to one bit or more. Bob knows the whole key, whereas Alice generally knows several bits of the key. For example, in the quantum private query protocol due to Yang et al. [12], if we set $|\phi_0\rangle_A = \cos(\frac{\theta}{2})|0\rangle + \sin(\frac{\theta}{2})|1\rangle$ and $|\phi_1\rangle_A = \cos(\frac{\theta}{2})|0\rangle - \sin(\frac{\theta}{2})|1\rangle, 0 < \theta < \pi/2$, then it can be shown that the success probability of Alice to guess a bit in the raw key becomes $\frac{1}{2}\sin^2\theta$. Now, if Bob has lack of resources to generate $|\Psi\rangle_{AB}$ and he borrows the states from a third party, say Charlie, then the situation would be different. In fact, if Alice is mistrustful and has a tie with Charlie, then there may exist a possibility that the states $|\phi_l\rangle_A, l = 0, 1$ are not qubits. Rather, the states $|\phi_l\rangle_A$ may

be of higher dimensional which may benefit Alice. We show that this is indeed possible and thus the key generation in quantum private query protocol (QPQ) proposed by Yang et al. is insecure without the certification of the dimension of the Alice's sub-system.

In order to acquire knowledge about the dimension of Alice's particle, Bob needs to perform certain quantum measurements. Since the dimension of Alice's state is unknown to Bob and he has to devise measurement operators for detecting whether it is a qubit or qutrit, we consider *Orbital Angular Momentum* (OAM) along with the state of polarization of a photon. In case of qutrit, we define two bases. In one basis, we consider $|0\rangle = |H, +m\rangle$, $|1\rangle = |V, +m\rangle$ and $|2\rangle = |H, -m\rangle$ and in another basis we consider $|0\rangle = |H, +m\rangle$, $|1\rangle = |V, +m\rangle$ and $|2\rangle = |V, -m\rangle$; where H (V) denotes horizontal (vertical) polarization and $m = \pm 1$ stands for orbital angular momentum (OAM) of a photon. Bob switches over these two bases randomly. The reason of such switching is discussed in section 3. The motivation of defining the basis vectors in this way is to show that the proposed methodology is not practically impossible. In this regard, one may wonder why we consider qutrit but not a ququart which covers the whole space of dimension 4. We observe that even using a qutrit the cheater may gain sufficiently. This motivates us to deal with qutrits as the cheater has no incentive to go for another extra dimension, i.e., for quart when he/she already gains from lower dimension.

We observe if Alice's subsystems remain in the same subspace of $\mathbb{C}^3$, i.e., if Alice's subsystems are the superposition of $\{|0\rangle, |1\rangle\}$ or $\{|1\rangle, |2\rangle\}$ or $\{|0\rangle, |2\rangle\}$, then the protocol by Yang et al. maintains the same success probability described above. However, if Alice's subsystems are in two different subspaces the situation alters. In this case, Alice may achieve greater success probability for small values of θ. Thus Bob has to apply his measurement operators for detection the subspaces of Alice's qutrits. Note that this situation never arises if Alice's subsystem will be a qubit as there is no possibility for different subspaces. That is why the certification test performed by Bob at his place is named as "dimensionality testing".

Moreover, the procedure we exploit for dimension certification in the above mentioned protocol can also detect a more powerful attack as follows. In this attack model Charlie may supply N product states of the form $|l\rangle_B |\phi_l\rangle_A$, where $l \in \{0, 1\}$, to Bob. At the same time he provides the full information of l to Alice. As Bob measures his states only in $\{|0\rangle, |1\rangle\}$ basis, Alice gets the full information about the raw key. Though such type of attack was not considered in [13], however, the methodology they used certifies automatically if the states are entangled and hence remove the possibility of such attack. We show that the CHSH like game proposed in the paper is capable of defending such an attack.

One should note that our methodology is designed for one server and one client model. This does not consider one server and multi-clients situation where a cheater uses a scheme which will provide exactly as much information for the ordinary clients as they are entitled to (otherwise he will be caught very soon), and only the favoured clients, who know the scheme may profit. Here, the favoured client Alice ties up with the third party Charlie to cheat Bob (the server).

The contribution and organization of this paper are as follows. In Section 2, we define a qubit-qutrit entangled state $|\Psi\rangle_{BA}$ which guarantees higher success probability to Alice to guess a bit in the raw key for the QPQ protocol proposed by Yang et al. In Section 3, we develop a CHSH like game for detection of dimension of Alice's subsystem, rather it is more appropriate to say, a CHSH game for detection of the subspaces of Alice's subsystems. We

also propose a set up for generating $|\Psi\rangle_{BA}$ by exploiting the existing quantum logic gates defined for $\mathbb{C}^3$ in section 4.

2 Qubit-qutrit entangled state

In this section we show how the success probability for guessing a raw key bit in the key generation protocol proposed by Yang et al. gets influenced if we replace qubit-qubit entangled state with a qubit-qutrit entangled state. Let us consider equation (1)

$$|\Psi\rangle_{BA} = \frac{1}{\sqrt{2}}(|0\rangle_B |\phi_0\rangle_A + |1\rangle_B |\phi_1\rangle_A)$$

where,

$$\begin{aligned}
|\phi_0\rangle_A &= \cos\gamma\cos\delta\,|i\rangle + (\cos\theta\sin\delta - \sin\theta\sin\gamma\cos\delta)\,|i+1\rangle \\
&+ (\sin\theta\sin\delta + \cos\theta\sin\gamma\cos\delta)\,|i+2\rangle \\
|\phi_1\rangle_A &= (\cos\theta\sin\delta - \sin\theta\sin\gamma\cos\delta)\,|i\rangle + \cos\gamma\cos\delta\,|i+1\rangle \\
&- (\sin\theta\sin\delta + \cos\theta\sin\gamma\cos\delta)\,|i+2\rangle\,,
\end{aligned}$$

where, $|i+j\rangle \implies |i+j \mod 3\rangle$, $i,j = \{0,1,2\}$ and $0 \le \theta,\gamma,\delta \le \pi/2$. Note that $|\phi_0\rangle_A$ and $|\phi_1\rangle_A$ need not be orthogonal.

Now we discuss the key generation protocol [12] using this shared qubit-qutrit entangled state. After sharing the states, Bob measures his qubits in $\{|0\rangle_B, |1\rangle_B\}$ basis, whereas Alice measures her qutrits either in $\{|\phi_0\rangle_A, |\phi_0'\rangle_A, |\phi_0''\rangle_A\}$ basis or in $\{|\phi_1\rangle_A, |\phi_1'\rangle_A, |\phi_1''\rangle_A\}$ basis randomly, where,

$$\begin{aligned}
|\phi_0'\rangle_A &= -\cos\gamma\sin\delta\,|i\rangle + (\sin\theta\sin\gamma\sin\delta + \cos\theta\cos\delta)\,|i+1\rangle \\
&+ (\sin\theta\cos\delta - \sin\delta\cos\theta\sin\gamma)\,|i+2\rangle\,, \\
|\phi_0''\rangle_A &= -\sin\gamma\,|i\rangle - \sin\theta\cos\gamma\,|i+1\rangle \\
&+ \cos\theta\cos\gamma\,|i+2\rangle\,, \\
|\phi_1'\rangle_A &= (\sin\theta\sin\gamma\sin\delta + \cos\theta\cos\delta)\,|i\rangle - \cos\gamma\sin\delta\,|i+1\rangle \\
&- (\sin\theta\cos\delta - \sin\delta\cos\theta\sin\gamma)\,|i+2\rangle\,, \\
|\phi_1''\rangle_A &= -\sin\theta\cos\gamma\,|i\rangle - \sin\gamma\,|i+1\rangle \\
&- \cos\theta\cos\gamma\,|i+2\rangle\,.
\end{aligned}$$

If the measurement outcome of Alice is $|\phi_0'\rangle$ or $|\phi_0''\rangle$, she concludes that the raw key bit at Bob's end is 1. If it is $|\phi_1'\rangle$ or $|\phi_1''\rangle$, the raw key bit is 0. In this case, the success probability

of Alice when Bob measures $|0\rangle$ becomes

$$\begin{aligned}
\Pr(A=0,B=0) &= \Pr(B=0)\Pr(A=0|B=0)\\
&= \frac{1}{2}[\Pr(A=\phi_1'|B=0)+\Pr(A=\phi_1''|B=0)]\\
&= \frac{1}{2}\big[(\sin\theta\sin\gamma\cos\gamma\sin 2\delta\\
&+ \cos\theta\cos\gamma\cos 2\delta-\sin\theta\cos\theta\sin\gamma\cos 2\delta\\
&- \sin^2\theta\sin\delta\cos\delta+\cos^2\theta\sin^2\gamma\sin\delta\cos\delta)^2\\
&+ (\sin\theta\cos\delta\cos 2\gamma+\cos\theta\sin\gamma\sin\delta\\
&+ \sin\theta\cos\theta\cos\gamma\sin\delta+\cos^2\theta\sin\gamma\cos\gamma\cos\delta)^2\big].
\end{aligned}$$

Similarly, the success probability of Alice when Bob measures $|1\rangle$ is given by

$$\begin{aligned}
\Pr(A=1,B=1) &= \frac{1}{2}\big[(\sin\theta\sin\gamma\cos\gamma\sin 2\delta\\
&+ \cos\theta\cos\gamma\cos 2\delta-\sin\theta\cos\theta\sin\gamma\cos 2\delta\\
&- \sin^2\theta\sin\delta\cos\delta+\cos^2\theta\sin^2\gamma\sin\delta\cos\delta)^2\\
&+ (\sin\theta\cos\delta\cos 2\gamma+\cos\theta\sin\gamma\sin\delta\\
&+ \sin\theta\cos\theta\cos\gamma\sin\delta+\cos^2\theta\sin\gamma\cos\gamma\cos\delta)^2\big].
\end{aligned}$$

Hence the total success probability of Alice to guess a bit correctly can be calculated as follows

$$\begin{aligned}
\Pr(A=B) &= \frac{1}{2}.[\Pr(A=\phi_1'|B=0)+\Pr(A=\phi_1''|B=0)]\\
&+ \frac{1}{2}.[\Pr(A=\phi_0'|B=1)+\Pr(A=\phi_0''|B=1)]\\
&= [\Pr(A=\phi_0'|B=1)+\Pr(A=\phi_0''|B=1)]\\
&= (\sin\theta\sin\gamma\cos\gamma\sin 2\delta+\cos\theta\cos\gamma\cos 2\delta\\
&- \sin\theta\cos\theta\sin\gamma\cos 2\delta-\sin^2\theta\sin\delta\cos\delta\\
&+ \cos^2\theta\sin^2\gamma\sin\delta\cos\delta)^2+(\sin\theta\cos\delta\cos 2\gamma\\
&+ \cos\theta\sin\gamma\sin\delta+\sin\theta\cos\theta\cos\gamma\sin\delta\\
&+ \cos^2\theta\sin\gamma\cos\gamma\cos\delta)^2.
\end{aligned}$$

If we put $\delta=\pi/2$, the success probability of Alice to guess a key bit correctly becomes $\cos^2\theta(1+\sin^2\theta)=1-\sin^4\theta$ for any $0\le\theta,\gamma\le\pi/2$.

The success probabilities are drawn in Figure. 1 both for the qubit-qubit and qubit-qutrit (for $\delta=\pi/2$) entangled states. Note that when qubit-qutrit entangled pairs are exploited, Alice gains (in terms of probability) for any value of θ ranging from 0 to 1.1 (approximately). This observation demands Bob to verify and test the dimension of the quantum particle shared with Alice.

In this regard one may argue that for large value of $\theta\in\{0,\frac{\pi}{2}\}$ Alice can gain larger probability value and hence large number of raw key bits than what she is entitled for. Thus Charlie might not change the dimension of Alice's subsystem, rather he manipulates the

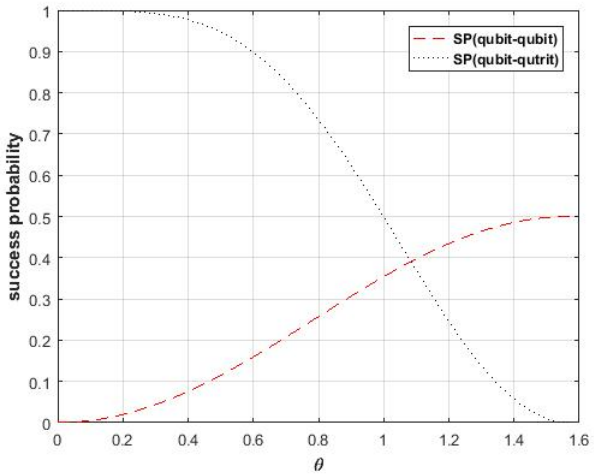

Fig. 1. Success probability for Yang's QPQ protocol for qubit-qubit and qubit-qutrit (setting $\delta = \frac{\pi}{2}$) shared entangled state

value of θ. This type of cheating can be easily detected by exploiting the methodology of [13]. However, if Charlie changes the dimension of the system in the motivation to favour Alice, Bob can not detect the attack by the existing methodology of [13] and hence the proposed attack remains undetected for a given value of θ.

We now show that if Alice's subsystems are lying in same sub-space of $\mathbb{C}^3$, the success probability remains same as the success probability of qubit-qubit system. Let us consider

$$|\Phi\rangle_{BA} = \frac{1}{\sqrt{2}}(|0\rangle_B |\phi_0\rangle_A + |1\rangle_B |\phi_1\rangle_A)$$

where,

$$\begin{aligned} |\phi_0\rangle_A &= \cos\frac{\theta}{2}|i\rangle + \sin\frac{\theta}{2}|i+1\rangle \\ |\phi_1\rangle_A &= \cos\frac{\theta}{2}|i\rangle - \sin\frac{\theta}{2}|i+1\rangle, \end{aligned}$$

and $0 < \theta < \pi/2, i \in \{0,1,2\}$. Note that if Bob's particle is measured in $\{|0\rangle_B, |1\rangle_B\}$ basis then the state of Alice's particle lies in one of the fundamental two dimensional subspaces of $\mathbb{C}^3$. Now we determine the success probability of Alice to guess a bit of the raw key as follows.

Proceeding a similar way described by Yang et al. [12], first Bob measures his qubits in $\{|0\rangle_B, |1\rangle_B\}$ basis. If Bob obtains $|0\rangle_B$ or $|1\rangle_B$, Alice's state becomes $|\phi_0\rangle_A$ or $|\phi_1\rangle_A$ respectively. Now let Alice performs measurements on her particle using the bases $\mathcal{A}_0 = \{|\phi_0\rangle_A, |\phi_0'\rangle_A, |\phi_0''\rangle_A\}$ and $\mathcal{A}_1 = \{|\phi_1\rangle_A, |\phi_1'\rangle_A, |\phi_1''\rangle_A\}$, choosing one of them uniformly at random, where $|\phi_l'\rangle_A$ is in the superposition of $|i\rangle, |i+1\rangle$ and orthogonal to $|\phi_l\rangle_A$ and $|\phi_l''\rangle_A$. If Bob obtains $|0\rangle_B$ and Alice chooses $\mathcal{A}_0$, she shall get $|\phi_0\rangle_A$ with probability 1 and never gets $|\phi_0'\rangle_A, |\phi_0''\rangle_A$; whereas if she chooses $\mathcal{A}_1$, she shall obtain $|\phi_1\rangle_A$ with probability $\cos^2\theta$ otherwise $|\phi_1'\rangle_A$ with probability $\sin^2\theta$ and never gets $|\phi_1''\rangle_A$. This is because

$$|\phi_0\rangle_A = \cos\theta|\phi_1\rangle_A + \sin\theta|\phi_1'\rangle_A.$$

Now we summarize the conditional probabilities in the following table, where $B = 0, 1$ means Bob gets $|0\rangle_B$ and $|1\rangle_B$ respectively.

	$B=0$	$B=1$
$A = \|\phi_0\rangle_A$	$\frac{1}{2}$	$\frac{1}{2}\cos^2\theta$
$A = \|\phi_0'\rangle_A$	0	$\frac{1}{2}\sin^2\theta$
$A = \|\phi_0''\rangle_A$	0	0
$A = \|\phi_1\rangle_A$	$\frac{1}{2}\cos^2\theta$	$\frac{1}{2}$
$A = \|\phi_1'\rangle_A$	$\frac{1}{2}\sin^2\theta$	0
$A = \|\phi_1''\rangle_A$	0	0

We define the rule to determine the key as follows. If Alice gets $|\phi_0'\rangle_A$, she outputs 1, and when she gets $|\phi_1'\rangle_A$, she outputs 0. Thus, the success probability of Alice to guess a bit in raw key can be written as

$$\begin{aligned}
\Pr(A=B) &= \Pr(A=0,B=0)+\Pr(A=1,B=1)\\
&= \Pr(B=0)\Pr(A=0|B=0)+\Pr(B=1)\Pr(A=1|B=1)\\
&= \frac{1}{2}\Pr(A=\phi_1^{\perp}|B=0)+\frac{1}{2}\Pr(A=\phi_0^{\perp}|B=1)\\
&= \frac{\sin^2\theta}{2}.
\end{aligned}$$

Thus we conclude that the proposed qubit-qutrit state $|\Phi\rangle_{BA}$ provides the same success probability when the state of Alice's shared particle is in one of the fundamental subspaces of $\mathbb{C}^3$. This result facilitates us to define a set of measurement operators for Bob who can test whether Alice's qutrit is in the desired space. Once a dimension test determines that $|\phi_0\rangle_A$ and $|\phi_1\rangle_A$ are lying in the same two dimensional subspace of $\mathbb{C}^3$, Yang et al. protocol can be continued for key generation with the shared entangled state of the form of eqn (1).

3 CHSH like game for dimensionality testing

In this section we propose a methodology to determine if the states of Alice's particles, $|\phi_0\rangle_A, |\phi_1\rangle_A$ (see equation (1)) are in the superposition of same orthonormal states $\{|i\rangle_A, |j\rangle_A\}$, $i, j \in \{0, 1, 2\}$, or in the superposition of different orthonormal states. For example, one is the superposition of $\{|0\rangle, |2\rangle\}$ and another is the superposition of $\{|1\rangle, |2\rangle\}$ and so on. Exploiting the methodology described here we also can certify if the shared states are product states.

In our context, Bob performs a CHSH like game to detect the dimensionality of Alice's subsystem at his place. We should emphasize again that why we call this "dimensionality testing". This is because if Alice's system is qubit, then there will be no possibility to lie the subsystems of Alice in two different subspaces. This only happens when we consider higher dimension.

Similar to the standard CHSH game, we require two black boxes as initial set up. One box is labeled as X whereas another is labeled as Y. Note that here Bob possesses both the boxes. Like the CHSH game, we assume that during the game, the boxes do not communicate among themselves. Box X can take an input $x \in \{0, 1\}$ and box Y can take another input $y \in \{0, 1\}$. After taking the inputs, X produces a bit $a \in \{0, 1\}$ and Y produces a trit $b \in \{0, 1, 2\}$. We now define a function $f(a, b)$ such that $f(a, b) = 1$ if $a \neq b$ and $f(a, b) = 0$ if $a = b$.

The game will win if and only if $f(a,b) = x \wedge y$. For classical deterministic strategy the winning probability of the game is $\frac{3}{4}$. However, the winning probability differs if we assume that the boxes share some quantum states between themselves. In the following subsections we will show how it differs for product state, entangled state with sub-systems lying in same subspaces of dimension 3 and entangled state with sub-systems lying in different subspaces of dimension 3.

3.1 Winning probability for product states

Consider, Bob gets N product states from Charlie. Let among these N states, $\frac{N}{2}$ states are of the form $|0\rangle|\phi_0\rangle$ and remaining $\frac{N}{2}$ are of the form $|1\rangle|\phi_1\rangle$, where $|\phi_0\rangle = \cos\frac{\theta}{2}|i\rangle + \sin\frac{\theta}{2}|i+1\rangle$ and $|\phi_1\rangle = \cos\frac{\theta}{2}|i\rangle - \sin\frac{\theta}{2}|i+1\rangle$, $i \in \{0,1,2\}$ and $|i+1\rangle = |i+1 \bmod 3\rangle$. From these N states, Bob chooses n states uniformly at random. He then fixes a quantum strategy as follows.

If $x = 0$, X measures the 1st particle in $\{|0\rangle, |1\rangle\}$ basis, if it is 1, the particle is measured in $\{|+\rangle, |-\rangle\}$ basis, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. If the measurement result would be $|0\rangle$ or $|+\rangle$, X outputs 0. If the measurement result would be $|1\rangle$ or $|-\rangle$, X outputs 1.

If $y = 0$, Y measures the 2nd particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis, if it is 1, the particle is measured in $\{|0''\rangle, |1''\rangle, |2''\rangle\}$ basis, where $|0'\rangle = \frac{1}{\sqrt{2}}(\cos\frac{\pi}{8}|i\rangle + \sin\frac{\pi}{8}|i+1\rangle)$, $|1'\rangle = \frac{1}{\sqrt{2}}(\sin\frac{\pi}{8}|i\rangle - \cos\frac{\pi}{8}|i+1\rangle)$, $|2'\rangle = |i+2\rangle$ and $|0''\rangle = \frac{1}{\sqrt{2}}(\cos\frac{3\pi}{8}|i\rangle + \sin\frac{3\pi}{8}|i+1\rangle)$, $|1''\rangle = \frac{1}{\sqrt{2}}(\sin\frac{3\pi}{8}|i\rangle - \cos\frac{3\pi}{8}|i+1\rangle)$, $|2''\rangle = |i+2\rangle$; $|i+2\rangle = |i+2 \mod 3\rangle$. If the measurement result would be $|0'\rangle$ or $|0''\rangle$, Y outputs 0. If the measurement result would be $|1'\rangle$ or $|1''\rangle$, Y outputs 1. If it is $|2'\rangle$ or $|2''\rangle$, Y outputs 2.

In this case, winning probability becomes

$$\begin{aligned}
\Pr(f(a,b) = x \wedge y) \quad &= \quad \Pr((x,y) = (0,0)\ \&\ ((a,b) = (0,0)\ \textit{or}\ (1,1))) \\
&+ \quad \Pr((x,y) = (0,1)\ \&\ ((a,b) = (0,0)\ \textit{or}\ (1,1))) \\
&+ \quad \Pr((x,y) = (1,0)\ \&\ ((a,b) = (0,0)\ \textit{or}\ (1,1))) \\
&+ \quad \Pr((x,y) = (1,1)\ \&\ ((a,b) = (0,1)\ \textit{or}\ (0,2) \\
&\textit{or} \quad (1,0)\ \textit{or}\ (1,2)))
\end{aligned}$$

From Figure A.1 of appendix, we get $\Pr(f(a,b) = x \wedge y) = \frac{1}{2}(1 + \frac{1}{2\sqrt{2}}\sin\theta)$.

3.2 Winning probability for entangled state with sub-systems lying in same subspaces

Let Bob gets N entangled pairs of the form $\frac{1}{\sqrt{2}}(|0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle)$, where $|\phi_0\rangle = \cos\frac{\theta}{2}|i\rangle + \sin\frac{\theta}{2}|i+1\rangle$ and $|\phi_1\rangle = \cos\frac{\theta}{2}|i\rangle - \sin\frac{\theta}{2}|i+1\rangle$ from Charlie. He then chooses n states among these N entangled pairs uniformly at random and follows the quantum strategy as described above. In such a case, the winning probability $\Pr(f(a,b) = x \wedge y)$ becomes $\frac{1}{2}(1 + \frac{1}{2\sqrt{2}} + \frac{1}{2\sqrt{2}}\sin\theta)$ (Figure B.1 of appendix).

3.3 Winning probability for entangled states with subsystem lying in different subspaces

Let Bob gets N entangled pairs of the form $\frac{1}{\sqrt{2}}(|0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle)$, where $|\phi_0\rangle = \cos\theta|i+1\rangle + \sin\theta|i+2\rangle$ and $|\phi_1\rangle = \cos\theta|i\rangle - \sin\theta|i+2\rangle$ from Charlie. Bob then chooses n states from these N states randomly. If Bob decides to follow the same strategy as described above, the winning probability $\Pr(f(a,b) = x \wedge y)$ becomes $\frac{1}{4}(1+\cos^2\theta)$ (Figure C.1 of appendix).

Thus, observing the winning probability of the game Bob can differentiate if the states are product states, entangled with sub-systems lying in same subspaces or entangled with sub-systems lying in different subspaces. Figure 2 shows the winning probabilities with varying θ for the above three cases.

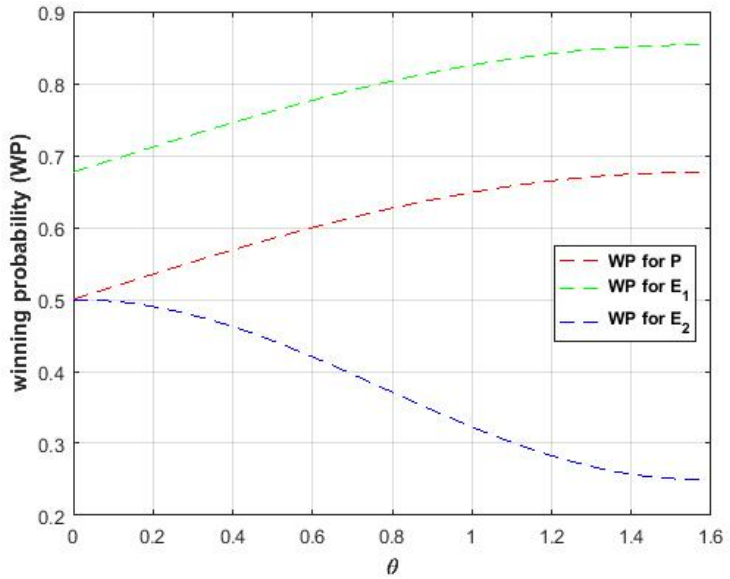

Fig. 2. red curve: Winning probability (WP) of tilted CHSH game with θ for product states (P); green curve: WP for entangled state with sub-systems lying in same subspace (E_1); blue curve: WP for entangled state with sub-systems lying in different subspaces (E_2)

From Figure 2, it can be easily seen that the winning probability of the game while using the entangled state with subsystem lying in the same subspace exceeds the classical winning probability $\frac{3}{4}$, for most of the values of θ. On the other hand, the winning probability of the game is always less than $\frac{3}{4}$ when product state and the entangled state with subsystem lying in different subspaces are used in the protocol.

It is mandatory to mention here that for each case, for half of the particle-pairs, we consider $\{|0\rangle, |1\rangle, |2\rangle\}$ as $\{|H,+1\rangle, |V,+1\rangle, |H,-1\rangle\}$ and for half of the particle-pairs we consider $\{|0\rangle, |1\rangle, |2\rangle\}$ as $\{|H,+1\rangle, |V,+1\rangle, |V,-1\rangle\}$. This is because Bob does not know which encoding has been used by Charlie. So it is possible that Charlie exploits $\{|H,+1\rangle, |V,+1\rangle, |V,-1\rangle\}$ basis and Bob uses $\{|H,+1\rangle, |V,+1\rangle, |H,-1\rangle\}$ basis. In such case, Bob gets the probability similar to qubit-qubit case i.e., when Alice's subsystems lie in same subspace of $\mathbb{C}^3$, hence gets deceived easily. However, if Bob switches between $\{|H,+1\rangle, |V,+1\rangle, |H,-1\rangle\}$ basis and

$\{|H,+1\rangle, |V,+1\rangle, |V,-1\rangle\}$ basis randomly, he will detect the dimension of Alice's subsystem successfully.

Hence, after getting the entangled states from a third party vendor, say Charlie, Bob chooses n entangled states randomly. Then he performs above mentioned dimensionality testing with these randomly chosen n states. If the proposed test certifies that $|\phi_0\rangle_A$ and $|\phi_1\rangle_A$ are in the desired subspaces, Bob goes for QPQ protocol with remaining states.

In this regard, one may wonder if instead of testing the states locally, this dimensionality test can be performed non-locally. In that case, the game should be defined as follows. Charlie (the third party) supplies the qubit-qutrit states to Bob and Alice respectively. Bob then randomly chooses a fraction of the supplied states and tells Alice to play the game for those states. Depending on the outcome of the game Bob decides if they further proceed for quantum private query phase.

In the proposed protocol, Bob has to switch over two bases. So in case of non-local game Alice has to inform when to choose what basis. Like Quantum Key Distribution (QKD), one may discuss the bases after measurement. However, unlike QKD, QPQ is considered as a mistrustful cryptography. In QPQ Alice may behave as a malicious party. So it should not be expected from her to communicate the true value of the output. Moreover, she might not be forced to measure the particles in the defined bases. She may choose some other bases which may replicate the probability value. The detail analysis regarding the security in case of non-local game is out of scope for the current paper. This might be our future research goal.

We present our proposed algorithm for dimensionality testing in Algorithm 1.

In the following section we explain how is it possible to create such an entangled pair defined in eqn (1) exploiting quantum gates defined for $\mathbb{C}^3$.

4 Preparation of qubit-qutrit entangled system using quantum logic gates

In this section, we propose how to generate qubit-qutrit entangled pair using quantum logic gates.

Assume that both the qubit and qutrit are initially in a vacuum mode and the initial qubit-qutrit state is given by

$$|\mu\rangle_{BA} = |0\rangle_B \otimes |0\rangle_A .$$

Our goal is to use different quantum gates to generate entanglement in qubit-qutrit system which is initially in a product state.

Recall that the rotation operator R for a qutrit system can be written as $R = R_x(\theta)R_y(\gamma)$ $R_z(\delta)$ due to Euler decomposition, where $R_x(\theta)$, $R_y(\gamma)$ and $R_z(\delta)$ denote the rotation operators about x-axis, y-axis and z-axis respectively. The operators $R_x(\theta)$, $R_y(\gamma)$ and $R_z(\delta)$ can be realized in experiment by optical elements such as beam splitters and a π-phase shifter.

Now define a unitary operator U which acts on the computational basis state of six di-

Algorithm 1 Our Proposed protocol for dimensionality testing

1. Bob starts with n number of entangled states chosen randomly from N number of entangled states supplied by a third party vendor.

2. For rounds $i \in \{1, \cdots, n\}$

   (a) Bob chooses $x_i \in \{0, 1\}$ and $y_i \in \{0, 1\}$ uniformly at random.

   (b) If $x_i = 0$, he measures the first particle of the entangled state in $\{|0\rangle, |1\rangle\}$ basis and if $x_i = 1$, he measures that in $\{|+\rangle, |-\rangle\}$ basis (defined above).

   (c) Similarly, if $y_i = 0$, Bob measures the second particle of the entangled state in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis and if $y_i = 1$, he measures that in $\{|0''\rangle, |1''\rangle, |2''\rangle\}$ basis (defined above).

   (d) The output is recorded as $a_i \in \{0, 1\}$ and $b_i \in \{0, 1, 2\}$ for the first and the second particle respectively. The encoding for $a_i(b_i)$ is as follows.

   - For the first particle of each pair, $a_i = 0$ if the measurement result is $|0\rangle$ or $|+\rangle$; it is 1 if the result is $|1\rangle$ or $|-\rangle$.
   - For the second particle of each pair, $b_i = 0$ if the measurement result is $|0'\rangle$ or $|0''\rangle$; it is 1, if the measurement result is $|1'\rangle$ or $|1''\rangle$; it is 2, if the measurement result is $|2'\rangle$ or $|2''\rangle$.

   (e) For the test round $i = n$, define

$$f(a_i, b_i) = \begin{cases} 1 & \text{if } a_i \neq b_i \\ 0 & \text{if } otherwise. \end{cases}$$

3. For $i = n$, define

$$Y_i = \begin{cases} 1 & \text{if } f(a_i, b_i) = x_i \wedge y_i \\ 0 & \text{if } otherwise. \end{cases}$$

4. If $\frac{1}{n}\sum_i Y_i < \frac{1}{2}(1 + \frac{1}{2\sqrt{2}} + \frac{1}{2\sqrt{2}}\sin\theta)$, Bob aborts the protocol.

5. Conditioning on the event that the local CHSH test at Bob's place has been successful, Bob proceeds for the private query phase as described in [12].

mensional Hilbert space such that

$$\begin{aligned} U|00\rangle &= |00\rangle, \\ U|01\rangle &= |01\rangle, \\ U|02\rangle &= |02\rangle, \\ U|10\rangle &= |11\rangle, \\ U|11\rangle &= |10\rangle, \\ U|12\rangle &= -|12\rangle. \end{aligned}$$

Therefore, the explicit form of the unitary operator is given by

$$U = |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| + |02\rangle\langle 02| - |12\rangle\langle 12|.$$

Now, the desired state of the form equation (1) can be obtained from $|\mu\rangle_{BA}$ in two steps as follows.

- Apply the unitary operator $H \otimes R$ on $|\mu\rangle_{BA}$ such that we obtain $|\omega\rangle_{BA} = (H \otimes R)\,|\mu\rangle_{BA}$, where H denotes the Hadamard gate for qubits.
- Apply the operator U on $|\omega\rangle_{BA}$ to obtain $|\Psi\rangle_{BA} = U\,|\omega\rangle_{BA}$.

Indeed, by writing R in the computation basis, it is easy to verify that

$$|\Psi\rangle_{BA} = \frac{1}{\sqrt{2}}(|0\rangle_B \otimes |\phi_0\rangle_A + |1\rangle_B \otimes |\phi_1\rangle_A),$$

where,

$$\begin{aligned} |\phi_0\rangle_A &= \cos\gamma\cos\delta|0\rangle_A + (\cos\theta\sin\delta - \sin\theta\sin\gamma\cos\delta)|1\rangle_A + (\sin\theta\sin\delta + \cos\theta\sin\gamma\cos\delta)|2\rangle_A \\ |\phi_1\rangle_A &= (\cos\theta\sin\delta - \sin\theta\sin\gamma\cos\delta)|0\rangle_A + \cos\gamma\cos\delta|1\rangle_A - (\sin\theta\sin\delta + \cos\theta\sin\gamma\cos\delta)|2\rangle_A. \end{aligned}$$

5 Conclusion

Existing quantum information processing protocols assume a certain dimension of the system. It is intuitively commented that removing such assumption may cause security flaw in quantum information tasking. However, till date, no such protocol is found which can prove this conjecture. In the present draft, we find that there exist at least one key generation protocol which suffers from the removal of such assumption. In this regard, we pick up quantum private query protocol by Yang et al. and show how one party can gain more information than suggested by the protocol by changing the dimension of his/her subsystem. In this initiative, we propose titled CHSH game to certify the dimension of the subsystems of shared quantum system. Along with the certification of dimensionality, the game is enable to certify if the states are entangled.

Acknowledgments

The authors like to thank the anonymous reviewers for excellent comments that substantially improved the editorial as well as technical presentation of this paper.

References

1. Acín, Antonio and Gisin, Nicolas and Masanes, Lluis, *Physical Review Letters*, **97**, 12, 120405, 2006
2. Brunner, Nicolas and Pironio, Stefano and Acín, Antonio and Gisin, Nicolas and Méthot, André Allan and Scarani, Valerio, *Physical Review Letters*, **100**, 21, 210503, 2008
3. Scarani, Valerio and Gisin, Nicolas and Brunner, Nicolas and Masanes, Lluis and Pino, Sergi and Acín, Antonio, *Physical Review A*, **74**, 4, 042339, 2006
4. Wehner, Stephanie and Christandl, Matthias and Doherty, Andrew C, *Physical Review A*, **78**, 6, 062112, 2008
5. Gallego, Rodrigo and Brunner, Nicolas and Hadley, Christopher and Acín, Antonio, *Physical Review Letters*, **105**, 23, 230501, 2010
6. Junge, Marius and Palazuelos, Carlos, *Communications in Mathematical Physics*, **306**, 3, 695–746, 2011
7. Hendrych, Martin and Gallego, Rodrigo and Mičuda, Michal and Brunner, Nicolas and Acín, Antonio and Torres, Juan P, *Nature Physics*, **8**, 8, 588–591, 2012
8. Ahrens, Johan and Badzig, Piotr and Cabello, Adán and Bourennane, Mohamed, *Nature Physics*, **8**, 8, 592–595, 2012
9. Brunner, Nicolas and Navascués, Miguel and Vértesi, Tamás, *Physical Review Letters*, **110**, 15, 150501, 2013
10. Bowles, Joseph and Quintino, Marco Túlio and Brunner, Nicolas, *Physical Review Letters*, **112**, 14, 140407, 2014
11. Dov Gordon, S and Hazay, Carmit, and Katz, Jonathan and Lindell, Yehuda, *Journal of the ACM (JACM)*, **58**, 6, 24:1–24:37, 2011
12. Yang, Yu-Guang and Sun, Si-Jia and Xu, Peng and Tian, Ju, *Quantum Information Processing*, **13**, 3, 805–813, 2014
13. Maitra, Arpita and Paul, Goutam and Roy, Sarbani, *Physical Review A*, **95**, 4, 042344, 2017

Appendix A Conditional probability for product state

Let us consider a situation where Charlie supplies $\frac{N}{2}$ product states of the form $|0\rangle|\phi_0\rangle$ and $\frac{N}{2}$ product states of the form $|1\rangle|\phi_1\rangle$, where $|\phi_0\rangle = \cos\frac{\theta}{2}|i\rangle + \sin\frac{\theta}{2}|i+1\rangle$ and $|\phi_1\rangle = \cos\frac{\theta}{2}|i\rangle - \sin\frac{\theta}{2}|i+1\rangle$. Now, we analyze the case by case scenario below.

A.1 Case 1*: (x=0, y=0)*

In this case Bob randomly chooses n states from N states and measures his first particle in $\{|0\rangle, |1\rangle\}$ basis and second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis. For $\frac{1}{2}$ of the cases, for the first particle he obtains $|0\rangle$ with probability 1 and in that case the second particle will be $|\phi_0\rangle$. When he measures the second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis, he obtains $|0'\rangle$ with probability $\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{\pi}{8} + \sin\frac{\theta}{2}\sin\frac{\pi}{8})^2$, $|1'\rangle$ with probability $\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{\pi}{8} - \sin\frac{\theta}{2}\cos\frac{\pi}{8})^2$. In such case, he never gets $|2'\rangle$. Similarly, for $\frac{1}{2}$ of the cases, Bob gets $|1\rangle$ with probability 1 and in that case the second particle will be $|\phi_1\rangle$. When he measures the second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis, he obtains $|0'\rangle$ with probability $\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{\pi}{8} - \sin\frac{\theta}{2}\sin\frac{\pi}{8})^2$, $|1'\rangle$ with probability $\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{\pi}{8} + \sin\frac{\theta}{2}\cos\frac{\pi}{8})^2$ and never gets $|2'\rangle$.

A.2 Case 2*: (x=0, y=1)*

Bob measures his first particle in $\{|0\rangle, |1\rangle\}$ basis and second particle in $\{|0''\rangle, |1''\rangle, |2''\rangle\}$ basis. This case is similar to case 1. Conditional probabilities $\Pr(a, b|0, 1)$ are shown in figure A.1.

A.3 Case 3: (x=1, y=0)

Bob measures his first particle in $\{|+\rangle, |-\rangle\}$ basis and second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis. For the state of the form $|0\rangle|\phi_0\rangle$, Bob obtains $|+\rangle$ with probability $\frac{1}{2}$ and $|-\rangle$ with probability $\frac{1}{2}$. In both the cases the second particle will be $|\phi_0\rangle$. For the state in form $|1\rangle|\phi_1\rangle$, Bob obtains $|+\rangle$ with probability $\frac{1}{2}$ and $|-\rangle$ with probability $\frac{1}{2}$. And for both the cases the second particle will be $|\phi_1\rangle$. Thus, the conditional probability $\Pr(0, 0|1, 0) = \Pr(M = |0'\rangle\,||+\rangle, |\phi_0\rangle) + \Pr(M = |0'\rangle\,||+\rangle, |\phi_1\rangle)$, $\Pr(0, 1|1, 0) = \Pr(M = |1'\rangle\,||+\rangle, |\phi_0\rangle) + \Pr(M = |1'\rangle\,||+\rangle, |\phi_1\rangle)$ and $\Pr(0, 2|1, 0) = \Pr(M = |2'\rangle\,||+\rangle, |\phi_0\rangle) + \Pr(M = |2'\rangle\,||+\rangle, |\phi_1\rangle)$, where M is the measurement result for the second particle. Similarly, the conditional probability $\Pr(1, 0|1, 0) = \Pr(M = |0'\rangle\,||-\rangle, |\phi_0\rangle) + \Pr(M = |0'\rangle\,||-\rangle, |\phi_1\rangle)$, $\Pr(1, 1|1, 0) = \Pr(M = |1'\rangle\,||-\rangle, |\phi_0\rangle) + \Pr(M = |1'\rangle\,||-\rangle, |\phi_1\rangle)$ and $\Pr(1, 2|1, 0) = \Pr(M = |2'\rangle\,||-\rangle, |\phi_0\rangle) + \Pr(M = |2'\rangle\,||-\rangle, |\phi_1\rangle)$. We accumulate all these conditional probabilities $\Pr(a, b|1, 0)$ in figure A.1.

A.4 Case 4: (x=1, y=1)

Bob measures his first particle in $\{|+\rangle, |-\rangle\}$ basis and second particle in $\{|0''\rangle, |1''\rangle, |2''\rangle\}$ basis. This case is similar to case 3. Conditional probabilities $\Pr(a, b|1, 1)$ are shown in figure A.1.

Fig. A.1. Conditional probability of (a, b) given (x, y) for product states

(x, y)	(a, b)	$\Pr((a, b) \mid (x, y))$
(0, 0)	(0, 0)	$\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{\pi}{8} + \sin\frac{\theta}{2}\sin\frac{\pi}{8})^2$
	(0, 1)	$\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{\pi}{8} - \sin\frac{\theta}{2}\cos\frac{\pi}{8})^2$
	(0, 2)	0
	(1, 0)	$\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{\pi}{8} - \sin\frac{\theta}{2}\sin\frac{\pi}{8})^2$
	(1, 1)	$\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{\pi}{8} + \sin\frac{\theta}{2}\cos\frac{\pi}{8})^2$
	(1, 2)	0
(0, 1)	(0, 0)	$\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{3\pi}{8} + \sin\frac{\theta}{2}\sin\frac{3\pi}{8})^2$
	(0, 1)	$\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{3\pi}{8} - \sin\frac{\theta}{2}\cos\frac{3\pi}{8})^2$
	(0, 2)	0
	(1, 0)	$\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{3\pi}{8} - \sin\frac{\theta}{2}\sin\frac{3\pi}{8})^2$
	(1, 1)	$\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{3\pi}{8} + \sin\frac{\theta}{2}\cos\frac{3\pi}{8})^2$
	(1, 2)	0
(1, 0)	(0, 0)	$\frac{1}{2}(\cos^2\frac{\theta}{2}\cos^2\frac{\pi}{8} + \sin^2\frac{\theta}{2}\cos^2\frac{\pi}{8})$
	(0, 1)	$\frac{1}{2}(\cos^2\frac{\theta}{2}\sin^2\frac{\pi}{8} + \sin^2\frac{\theta}{2}\cos^2\frac{\pi}{8})$
	(0, 2)	0
	(1, 0)	$\frac{1}{2}(\cos^2\frac{\theta}{2}\cos^2\frac{\pi}{8} + \sin^2\frac{\theta}{2}\sin^2\frac{\pi}{8})$
	(1, 1)	$\frac{1}{2}(\cos^2\frac{\theta}{2}\sin^2\frac{\pi}{8} + \sin^2\frac{\theta}{2}\cos^2\frac{\pi}{8})$
	(1, 2)	0
(1, 1)	(0, 0)	$\frac{1}{2}(\cos^2\frac{\theta}{2}\sin^2\frac{\pi}{8} + \sin^2\frac{\theta}{2}\cos^2\frac{\pi}{8})$
	(0, 1)	$\frac{1}{2}(\cos^2\frac{\theta}{2}\cos^2\frac{\pi}{8} + \sin^2\frac{\theta}{2}\sin^2\frac{\pi}{8})$
	(0, 2)	0
	(1, 0)	$\frac{1}{2}(\cos^2\frac{\theta}{2}\sin^2\frac{\pi}{8} + \sin^2\frac{\theta}{2}\cos^2\frac{\pi}{8})$
	(1, 1)	$\frac{1}{2}(\cos^2\frac{\theta}{2}\cos^2\frac{\pi}{8} + \sin^2\frac{\theta}{2}\sin^2\frac{\pi}{8})$
	(1, 2)	0

Appendix B Conditional probability for entangled state with sub-systems lying in same subspace

Let us assume that Charlie supplies N entangled pairs of the form $\frac{1}{\sqrt{2}}(|0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle)$, where $|\phi_0\rangle = \cos\frac{\theta}{2}|i\rangle + \sin\frac{\theta}{2}|i+1\rangle$ and $|\phi_1\rangle = \cos\frac{\theta}{2}|i\rangle - \sin\frac{\theta}{2}|i+1\rangle$. Now, we analyze the case by case scenario below.

B.1 Case 1*: (x=0, y=0)*

In this case Bob chooses n states uniformly at random from N states and measures his first particle in $\{|0\rangle, |1\rangle\}$ basis and second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis. For the first particle he obtains $|0\rangle$ with probability $\frac{1}{2}$ and in this case the second particle collapses to $|\phi_0\rangle$. When Bob measures the second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis, he obtains $|0'\rangle$ with probability $\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{\pi}{8} + \sin\frac{\theta}{2}\sin\frac{\pi}{8})^2$, $|1'\rangle$ with probability $\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{\pi}{8} - \sin\frac{\theta}{2}\cos\frac{\pi}{8})^2$ and never gets $|2'\rangle$. Similarly, when Bob measures his first particle as $|1\rangle$, the second particle collapses to $|\phi_1\rangle$. In this case, the probabilities of getting $|0'\rangle$, $|1'\rangle$ and $|2'\rangle$ are given in figure B.1.

B.2 Case 2*: (x=0, y=1)*

Bob measures his first particle in $\{|0\rangle, |1\rangle\}$ basis and second particle in $\{|0''\rangle, |1''\rangle, |2''\rangle\}$ basis. This case is similar to case 1. Conditional probabilities $\Pr(a, b|0, 1)$ are shown in figure B.1.

B.3 Case 3*: (x=1, y=0)*

Bob measures his first particle in $\{|+\rangle, |-\rangle\}$ basis and second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis. When he measures the first particle in $\{|+\rangle, |-\rangle\}$ basis he gets $|+\rangle$ with probability $\cos^2\frac{\theta}{2}$ and $|-\rangle$ with probability $\sin^2\frac{\theta}{2}$. In the first case, the second particle collapses to $|0\rangle$. And in the second case, the second particle collapses to $|1\rangle$. When Bob measures the second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis, $|0'\rangle$ is obtained with probability $\cos^2\frac{\pi}{8}$, $|1'\rangle$ is obtained with probability $\sin^2\frac{\pi}{8}$and Bob never obtains $|2'\rangle$. Similarly, for $|1\rangle$, Bob obtains $|0'\rangle$ with probability $\sin^2\frac{\theta}{2}$, $|1'\rangle$ with probability $\cos^2\frac{\theta}{2}$ and never gets $|2'\rangle$. Conditional probabilities $\Pr(a, b|1, 0)$ are shown in figure B.1.

B.4 Case 4*: (x=1, y=1)*

Bob measures his first particle in $\{|+\rangle, |-\rangle\}$ basis and second particle in $\{|0''\rangle, |1''\rangle, |2''\rangle\}$ basis. This case is similar to case 3. Conditional probabilities $\Pr(a, b|1, 1)$ are shown in figure B.1.

Appendix C Conditional probability for entangled state with sub-systems lying in different subspace

Let us assume that Charlie supplies N entangled pairs of the form $\frac{1}{\sqrt{2}}(|0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle)$, where $|\phi_0\rangle = \cos\theta|i+1\rangle + \sin\theta|i+2\rangle$ and $|\phi_1\rangle = \cos\theta|i\rangle - \sin\theta|i+2\rangle$. Now, we analyze the case by case scenario below.

C.1 Case 1*: (x=0, y=0)*

In this case Bob chooses n states among these N states uniformly at random and measures the first particle in $\{|0\rangle, |1\rangle\}$ basis and second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis. For the first particle he obtains $|0\rangle$ with probability $\frac{1}{2}$ and in this case the second particle collapses to $|\phi_0\rangle$. When Bob measures the second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis, he obtains $|0'\rangle$ with probability $\cos^2\theta\sin^2\frac{\pi}{8}$, $|1'\rangle$ with probability $\cos^2\theta\cos^2\frac{\pi}{8}$ and $|2'\rangle$ with probability $\sin^2\theta$. Similarly, when Bob measures the first particle as $|1\rangle$, the second particle collapses to $|\phi_1\rangle$.

Fig. B.1. Conditional probability of (a, b) given (x, y) for entangled states with sub-systems in same space

(x, y)	(a, b)	$\Pr((a, b) \mid (x, y))$
(0, 0)	(0, 0)	$\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{\pi}{8} + \sin\frac{\theta}{2}\sin\frac{\pi}{8})^2$
	(0, 1)	$\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{\pi}{8} - \sin\frac{\theta}{2}\cos\frac{\pi}{8})^2$
	(0, 2)	0
	(1, 0)	$\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{\pi}{8} - \sin\frac{\theta}{2}\sin\frac{\pi}{8})^2$
	(1, 1)	$\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{\pi}{8} + \sin\frac{\theta}{2}\cos\frac{\pi}{8})^2$
	(1, 2)	0
(0, 1)	(0, 0)	$\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{\pi}{8} + \sin\frac{\theta}{2}\cos\frac{\pi}{8})^2$
	(0, 1)	$\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{\pi}{8} - \sin\frac{\theta}{2}\sin\frac{\pi}{8})^2$
	(0, 2)	0
	(1, 0)	$\frac{1}{2}(\cos\frac{\theta}{2}\sin\frac{\pi}{8} - \sin\frac{\theta}{2}\cos\frac{\pi}{8})^2$
	(1, 1)	$\frac{1}{2}(\cos\frac{\theta}{2}\cos\frac{\pi}{8} + \sin\frac{\theta}{2}\sin\frac{\pi}{8})^2$
	(1, 2)	0
(1, 0)	(0, 0)	$\cos^2\frac{\pi}{8}\cos^2\frac{\theta}{2}$
	(0, 1)	$\sin^2\frac{\pi}{8}\cos^2\frac{\theta}{2}$
	(0, 2)	0
	(1, 0)	$\sin^2\frac{\pi}{8}\sin^2\frac{\theta}{2}$
	(1, 1)	$\cos^2\frac{\pi}{8}\sin^2\frac{\theta}{2}$
	(1, 2)	0
(1, 1)	(0, 0)	$\sin^2\frac{\pi}{8}\cos^2\frac{\theta}{2}$
	(0, 1)	$\cos^2\frac{\pi}{8}\cos^2\frac{\theta}{2}$
	(0, 2)	0
	(1, 0)	$\cos^2\frac{\pi}{8}\sin^2\frac{\theta}{2}$
	(1, 1)	$\sin^2\frac{\pi}{8}\sin^2\frac{\theta}{2}$
	(1, 2)	0

In this case the probabilities of getting $|0'\rangle$, $|1'\rangle$ and $|2'\rangle$ are given in figure C.1.

C.2 Case 2*: (x=0, y=1)*

Bob measures his first particle in $\{|0\rangle, |1\rangle\}$ basis and second particle in $\{|0''\rangle, |1''\rangle, |2''\rangle\}$ basis. This case is similar to case 1. Conditional probabilities $\Pr(a, b|0, 1)$ are shown in figure C.1.

C.3 Case 3*: (x=1, y=0)*

Bob measures his first particle in $\{|+\rangle, |-\rangle\}$ basis and second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis. When he measures the first particle in $\{|+\rangle, |-\rangle\}$ basis he gets $|+\rangle$ with probability $\frac{1}{2}.\cos^2\theta$ and $|-\rangle$ with probability $\frac{1}{2}(1+\sin^2\theta)$. In the first case, the second particle collapses to $\frac{1}{\sqrt{2}}(|i\rangle + |i+1\rangle)$. And in the second case, the second particle collapses to $\frac{1}{\sqrt{2(1+\sin^2\theta)}}(-\cos\theta\,|i\rangle + \cos\theta\,|i+1\rangle + 2\sin\theta\,|i+2\rangle)$. Now, Bob measures the second particle in $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ basis. In the first case, he gets $|0'\rangle$ with probability $\frac{1}{2}\cos^2\theta(\cos\frac{\pi}{8}+\sin\frac{\pi}{8})^2$, $|1'\rangle$ with probability $\frac{1}{2}\cos^2\theta(\sin\frac{\pi}{8}-\cos\frac{\pi}{8})^2$ and never gets $|2'\rangle$. For the second case, Bob obtains $|0'\rangle$ with probability $\frac{1}{2}\cos^2\theta(\sin\frac{\pi}{8}-\cos\frac{\pi}{8})^2$, $|1'\rangle$ with probability $\frac{1}{2}\cos^2\theta(\cos\frac{\pi}{8}+\sin\frac{\pi}{8})^2$ and $|2'\rangle$ with probability $\sin^2\theta$. All these conditional probabilities $\Pr(a, b|1, 0)$ are shown in figure C.1.

C.4 Case 4*: (x=1, y=1)*

Bob measures his first particle in $\{|+\rangle, |-\rangle\}$ basis and second particle in $\{|0''\rangle, |1''\rangle, |2''\rangle\}$ basis. This case is similar to case 3. Conditional probabilities $\Pr(a, b|1, 1)$ are shown in figure C.1.

Fig. C.1. Conditional probability of (a, b) given (x, y) for entangled states with sub-systems in different subspaces

(x, y)	(a, b)	$\Pr((a, b) \mid (x, y))$
(0, 0)	(0, 0)	$\frac{1}{2}\cos^2\theta\sin^2\frac{\pi}{8}$
	(0, 1)	$\frac{1}{2}\cos^2\theta\cos^2\frac{\pi}{8}$
	(0, 2)	$\frac{1}{2}\sin^2\theta$
	(1, 0)	$\frac{1}{2}\cos^2\theta\cos^2\frac{\pi}{8}$
	(1, 1)	$\frac{1}{2}\cos^2\theta\sin^2\frac{\pi}{8}$
	(1, 2)	$\frac{1}{2}\sin^2\theta$
(0, 1)	(0, 0)	$\frac{1}{2}\cos^2\theta\cos^2\frac{\pi}{8}$
	(0, 1)	$\frac{1}{2}\cos^2\theta\sin^2\frac{\pi}{8}$
	(0, 2)	$\frac{1}{2}\sin^2\theta$
	(1, 0)	$\frac{1}{2}\cos^2\theta\sin^2\frac{\pi}{8}$
	(1, 1)	$\frac{1}{2}\cos^2\theta\cos^2\frac{\pi}{8}$
	(1, 2)	$\frac{1}{2}\sin^2\theta$
(1, 0)	(0, 0)	$\frac{1}{4}\cos^2\theta(\cos\frac{\pi}{8}+\sin\frac{\pi}{8})^2$
	(0, 1)	$\frac{1}{4}\cos^2\theta(\sin\frac{\pi}{8}-\cos\frac{\pi}{8})^2$
	(0, 2)	0
	(1, 0)	$\frac{1}{4}\cos^2\theta(\sin\frac{\pi}{8}-\cos\frac{\pi}{8})^2$
	(1, 1)	$\frac{1}{4}\cos^2\theta(\cos\frac{\pi}{8}+\sin\frac{\pi}{8})^2$
	(1, 2)	$\sin^2\theta$
(1, 1)	(0, 0)	$\frac{1}{4}\cos^2\theta(\cos\frac{\pi}{8}+\sin\frac{\pi}{8})^2$
	(0, 1)	$\frac{1}{4}\cos^2\theta(\sin\frac{\pi}{8}-\cos\frac{\pi}{8})^2$
	(0, 2)	0
	(1, 0)	$\frac{1}{4}\cos^2\theta(\sin\frac{\pi}{8}-\cos\frac{\pi}{8})^2$
	(1, 1)	$\frac{1}{4}\cos^2\theta(\cos\frac{\pi}{8}+\sin\frac{\pi}{8})^2$
	(1, 2)	$\sin^2\theta$