Communications in Physics, Vol. 23, No. 2 (2013), pp. 97-106

NONMAXIMAL ENTANGLEMENT CAN MAKE JOINT REMOTE STATE PREPARATION ABSOLUTELY SECURE

CAO THI BICH AND NGUYEN BA AN
Center for Theoretical Physics, Institute of Physics,
Vietnam Academy of Science and Technology
10 Dao Tan, Ba Dinh, Hanoi, Vietnam
Email: ctbich@iop.vast.ac.vn; nban@iop.vast.ac.vn

Received 01 April 2013;
Accepted for publication 21 May 2013

Abstract. *Joint remote state preparation is a multiparty global quantum task in which several parties are assigned to jointly prepare a quantum state for a remote party. Although various protocols have been proposed so far, none of them are absolutely secure in the sense that the legitimate parties (the preparers plus the receiver) can by no means identify the state to be prepared even if they all collude with each other. Here we resolve this drawback by employing the quantum channel in terms of nonmaximally entangled states whose parameters are kept secret to all the participants but used to split the information in a judicious way so that not only absolute security in the above-mentioned sense is achieved but also the performance is the simplest possible.*

I. INTRODUCTION

Entanglement owns spooky action at distance and thus is a crucial resource in quantum information processing and quantum computing: it can be used to test fundamental laws of quantum physics, to provide unconditional security in quantum communication, to teleport unknown quantum states, to enhance capacity of quantum channels, to make inefficient algorithms efficient and so on (see, e.g., the book [1] and references therein). It was widely believed that global quantum operations are best performed via maximal entanglement, while utilization of nonmaximal entanglement is often regarded reluctant: a prior local filtering (*Procrustean* method) or a special procedure (entanglement distillation method) may need to be applied to probabilitically obtain a maximally entangled state from a nonmaximally entangled one or some n maximally entangled states from a much larger number k ($k \gg n$) of nonmaximally entangled ones [2]. However, this is not always true. There exist certain information-theoretic tasks for which nonmaximally rather than maximally entangled states turn out to be the right choice. For example, some remote generalized measurements [3] and nonlocal gates [4] do require nonmaximal entanglement. In light of a counter-intuitive fact that less entanglement may outperform more entanglement [5], the authors of Ref. [6] employ a d-level nonmaximally entangled state for superdense coding and point out that states with less entanglement can have a greater

deterministic communication capacity than other more entangled states. The effect of nonmaximally entangled states is so strong in multiple linear optical teleportation [7] that the total success probability becomes higher than that via maximally entangled ones and can be even further increased by selecting the nonmaximally entangled states in an adaptive manner [8]. Furthermore, high-fidelity long-distance atomic-state teleportation can also be carried out even via currently available optical cavities if, instead of maximally entangled states, one uses a nonmaximally entangled state with its amplitude tailored properly to fully compensate for the damping factors due to the state mapping [9]. Recently, quantum secure direct communication and quantum key distribution exploit nonmaximal entanglement as well to avoid encoding in terms of nonorthogonal quantum states [10, 11]: the security is guaranteed by the quantum-mechanical impossibility of local unitary transformations between certain nonmaximally entangled states.

In this paper, we discover one more positive aspect of nonmaximal entanglement: it can boost security of the so-called joint remote state preparation (JRSP) [12–16] to the highest level. JRSP is an interesting multiparty quantum task that has recently attracted attention in the quantum information community from both theoretical [12–21] and experimental architecture [22] points of view. In contrast to the well-known remote state preparation (RSP) [23] in which one party has complete classical knowledge of a quantum state $|\Psi\rangle$ to be faithfully prepared at a remote party's location, in JRSP there are several inferiors who are assigned by a superior to jointly prepare the state $|\Psi\rangle$ for a remote receiver. The superior knows the state $|\Psi\rangle$ but the inferiors do not. So the superior can secretly split the information of the state $|\Psi\rangle$ into pieces each of which is given to an inferior to exclude leakage of full information about $|\Psi\rangle$ to any of the inferiors. Both maximally and nonmaximally entangled states have been used as the quantum channel for JRSP and the security level of all the existing protocols [12–22] is that any subgroup of the inferiors cannot exactly identify the state $|\Psi\rangle$ but all the inferiors together can. Like in blind quantum computation [24], it is highly desirable also for JRSP to have absolute security in the sense that neither an individual nor the entire group of the participants (i.e., all the inferiors plus the receiver) can precisely infer the sate $|\Psi\rangle$. Here, we shall show that to reach this goal nonmaximally entangled states should be used in parallel with an appropriate information splitting. Interestingly and surprisingly enough, the judicious information splitting that leads to the highest level of security is accompanied by simpler execution and higher success probability in comparison with that leading to a lower level of security. We shall illustrate those features by considering JRSP with two inferiors (called preparers in what follows) for arbitrary single- and two-qubit states using minimum physical resource.

II. ABSOLUTELY SECURE PROTOCOLS

First, we consider the single-qubit case. Let

$$|\Psi_1\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{1}$$

with complex numbers α, β satisfying the normalization condition $|\alpha|^2 + |\beta|^2 = 1$, be the state the two preparers Alice and Bob are required (by their superior) to jointly prepare for a remote receiver Charlie. The JRSP of state (1) can be done via two entangled

pairs [13, 16], but the minimum quantum resource is a single tripartite entangled state of the form [12–14]

$$|Q_1\rangle_{ABC} = (\mu\,|000\rangle + \nu\,|111\rangle)_{ABC}, \tag{2}$$

where μ, ν are complex numbers satisfying the normalization condition $|\mu|^2 + |\nu|^2 = 1$. Without loss of generality we assume that $|\mu| > |\nu|$. The qubit A (B, C) is distributed to Alice (Bob, Charlie). Suppose that the complete data set $S = \{\alpha, \beta\}$ characterizing the state $|\Psi_1\rangle$ is split (by the superior) into two subsets: one is $S_A = \{a, b\}$ with a, b arbitrary real numbers, which is given to Alice, and the other is $S_B = \{\overline{x}, \overline{y}\}$ with $\overline{x}, \overline{y}$ some complex numbers, which is given to Bob. Usually, a, b, $\overline{x}$ and $\overline{y}$ are chosen so that [12, 13]

$$\alpha = a\overline{x},\ \beta = b\overline{y}. \tag{3}$$

Transparently, such an information splitting forbids Alice alone or Bob alone to derive α, β (i.e., to identify $|\Psi_1\rangle$) but allows them together to do so. Here, to avoid this disadvantage, we on purpose employ the nonmaximally entangled quantum channel $|Q_1\rangle$, Eq. (2), whose parameters μ, ν are not disclosed (by the superior) to Alice and Bob, but are explicitly used for the information splitting in the following way

$$\begin{aligned} \overline{x} &= f_x(a, b, \alpha, \beta, \mu, \nu), \\ \overline{y} &= f_y(a, b, \alpha, \beta, \mu, \nu), \end{aligned} \tag{4}$$

where $f_{x(y)}(a, b, \alpha, \beta, \mu, \nu)$ are some well-defined functions of their arguments. Hence, even when Alice and Bob negotiate with each other they are unable to calculate α, β because they have no idea about μ and ν. Of course, this important feature does not arise in the case of maximal entanglement for which $\mu = \nu = 1/\sqrt{2}$. Actually, the nonmaximally entangled quantum channel (2) was employed already in several previous works [12–16], in which, however, μ and ν were not exploited at all for information splitting. In fact, there are many ways to define $f_{x(y)}(a, b, \alpha, \beta, \mu, \nu)$ and in theory these functions could be tailored so as to obtain the highest success probability. Such an optimization procedure is however not easy in general. So, as an example and for concreteness, let us set $f_x(a, b, \alpha, \beta, \mu, \nu) = \alpha/(a\sqrt{\mu})$ and $f_y(a, b, \alpha, \beta, \mu, \nu) = \beta/(b\sqrt{\nu})$, i.e.,

$$\overline{x} = \frac{\alpha}{a\sqrt{\mu}},\ \overline{y} = \frac{\beta}{b\sqrt{\nu}}. \tag{5}$$

With the knowledge of $S_A = \{a, b\}$ Alice measures qubit A in the basis

$$\begin{pmatrix} |u_1\rangle_A \\ |u_2\rangle_A \end{pmatrix} = \frac{1}{\sqrt{a^2 + b^2}} \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \begin{pmatrix} |0\rangle_A \\ |1\rangle_A \end{pmatrix}, \tag{6}$$

while with the knowledge of $S_B = \{\overline{x}, \overline{y}\}$ Bob measures qubit B in the basis

$$\begin{pmatrix} |v_1\rangle_B \\ |v_2\rangle_B \end{pmatrix} = \frac{1}{\sqrt{|\overline{x}|^2 + |\overline{y}|^2}} \begin{pmatrix} \overline{x}^* & \overline{y}^* \\ \overline{y} & -\overline{x} \end{pmatrix} \begin{pmatrix} |0\rangle_B \\ |1\rangle_B \end{pmatrix}. \tag{7}$$

The quantum channel state $|Q_1\rangle_{ABC}$ can then be reexpressed as

$$|Q_1\rangle_{ABC} = \sum_{n=1}^{2} \sum_{m=1}^{2} |u_m\rangle_A\, |v_n\rangle_B\, |D_{mn}\rangle_C\,, \tag{8}$$

which implies that if Alice finds $|u_m\rangle_A$ and Bob finds $|v_n\rangle_B$ then Charlie's qubit is projected onto the (unnormalized) state $|D_{mn}\rangle_C$. In the case of $m = n = 1$, we have

$$|D_{11}\rangle_C = \frac{(\mu a\overline{x}\,|0\rangle + \nu b\overline{y}\,|1\rangle)_C}{\sqrt{(a^2+b^2)(|\overline{x}|^2+|\overline{y}|^2)}}, \tag{9}$$

which, by virtue of Eqs. (5), becomes

$$|D_{11}\rangle_C = \frac{(\sqrt{\mu}\alpha\,|0\rangle + \sqrt{\nu}\beta\,|1\rangle)_C}{\sqrt{(a^2+b^2)(|\overline{x}|^2+|\overline{y}|^2)}}. \tag{10}$$

As in all the previous protocols using nonmaximally entangled quantum channel, the JRSP protocol fails unless the receiver Charlie knows the values of μ and ν. We thus suppose that the superior discloses μ and ν to Charlie. If so, Charlie takes an ancillary qubit C' prepared in state $|0\rangle_{C'}$ and applies on C and C' a two-qubit gate $U_{CC'}(\nu/\mu)$, where $U_{XY}(s)$ has the form (in the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}_{XY}$)

$$U_{XY}(s) = \begin{pmatrix} \sqrt{s} & 0 & 0 & \sqrt{1-|s|} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \sqrt{1-|s|} & 0 & 0 & -\sqrt{s^*} \end{pmatrix}. \tag{11}$$

Because

$$U_{CC'}(\frac{\nu}{\mu})\,|D_{11}\rangle_C\,|0\rangle_{C'} = \frac{\sqrt{\nu}\,|\Psi_1\rangle_C\,|0\rangle_{C'} + \sqrt{\mu(|\mu|-|\nu|)/|\mu|}\alpha\,|1\rangle_C\,|1\rangle_{C'}}{\sqrt{(a^2+b^2)(|\overline{x}|^2+|\overline{y}|^2)}}, \tag{12}$$

if Charlie measures C' and finds $|0\rangle_{C'}$, then qubit C is collapsed into the desired state $|\Psi_1\rangle_C$, with the probability

$$\overline{P}_1 = \frac{|\nu|}{(a^2+b^2)(|\overline{x}|^2+|\overline{y}|^2)}. \tag{13}$$

Note that with the information splitting (5) the requirement that Charlie knows μ and ν is necessary for her to construct the right gate $U_{CC'}(\nu/\mu)$. This, however, creates opportunity for the three participants (Alice, Bob and Charlie) to cooperate to deduce α, β from Eqs. (5), namely, $\alpha = a\overline{x}\sqrt{\mu}$ and $\beta = b\overline{y}\sqrt{\nu}$. To get rid of such a drawback (i.e., to achieve absolute security in the sense mentioned in the abstract), we do not let any of the three participants know μ and ν. Then, even the receiver joins the preparers in an attempt to learn full information about the state to be prepared, they all remain powerless. Yet, the JRSP would work by splitting information in a way different from (5). Concretely, now S_A remains the same, i.e., $S_A = \{a, b\}$, but S_B should be changed to $S_B = \{x, y\}$ with

$$x = \frac{\alpha}{a\mu},\ y = \frac{\beta}{b\nu}. \tag{14}$$

Alice will measure qubit A in the same basis determined by (6), but the basis for Bob to measure qubit B is determined by Eq. (7) in which $\overline{x}, \overline{y}$ should be replaced by x, y, respectively. It is straightforward to verify that if Alice finds $|u_1\rangle_A$ and Bob finds $|v_1\rangle_B$

then Charlie will get qubit C in the right state $|\Psi_1\rangle_C$ without doing anything. The probability for this to happen is

$$P_1 = \frac{1}{(a^2+b^2)(|x|^2+|y|^2)}. \tag{15}$$

Intuitively, one deems that P_1 would be lower than $\overline{P}_1$. Yet, the fact turns the other way around. From Eqs. (5), (13), (14) and (15) it follows that

$$\frac{P_1}{\overline{P}_1} - 1 = \frac{|x|^2(|\mu|-|\nu|)}{|\nu|(|x|^2+|y|^2)} > 0, \tag{16}$$

implying that P_1 is always higher than $\overline{P}_1$. This result is rather surprising since the latter method for JRSP is much simpler (no ancillas, no two-qubit quantum gates, no measurements are required at Charlie's station), provides absolute security (not only the two preparers but also all the three participants together are unable to identity $|\Psi_1\rangle$) and, at the same time, succeeds with a probability higher than that by the former method which makes use of the information splitting (5) with μ, ν known to Charlie. Such triple benefit arises from the usage of the nonmaximally entangled state (2) along with the judicious information splitting (14).

To assess achievable values of the success probability P_1 we set $b = a\mu|\beta|/(\nu|\alpha|)$ and $|\mu|^2 = 1/2+\varepsilon$ ($|\nu|^2 = 1/2-\varepsilon$) with $0 < \varepsilon < 1/2$. Then

$$P_1 = \frac{\varepsilon^2 - 1/4}{2(2|\alpha|^2-1)\varepsilon - 1}. \tag{17}$$

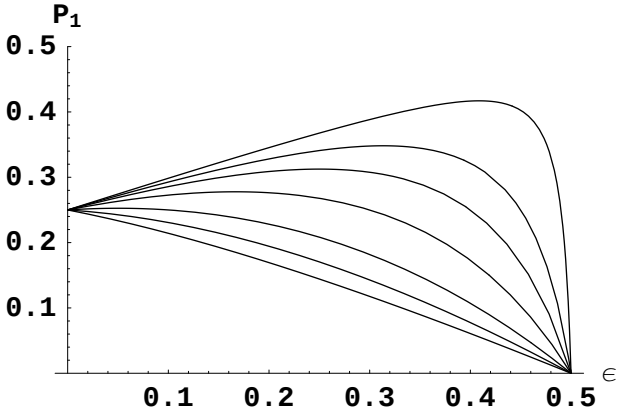

Fig. 1. The success probability P_1, Eq. (17), as a function of ε for $|\alpha|^2 = 0.2$, 0.4, 0.6, 0.8, 0.9, 0.95 and 0.99, upwards.

In Fig. 1 we plot P_1 of Eq. (17) as a function of ε for several values of $|\alpha|^2$. As seen from Fig. 1, in the limit of $\varepsilon \to 0$ (i.e., $|Q_1\rangle$ tends to the maximally entangled state $(|000\rangle + |111\rangle)/\sqrt{2}$) $P_1 \to 1/4$, while in the limit of $\varepsilon \to 1/2$ (i.e., $|Q_1\rangle$ tends to the separable state $|000\rangle$) $P_1 \to 0$. However, P_1 may exceed 1/4 for a fixed value of ε if $|\alpha|^2 > (1+2\varepsilon)/2$.

Next, we consider JRSP of the most general two-qubit state

$$|\Psi_2\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\,, \tag{18}$$

with complex numbers α, β, γ and δ satisfying the normalization condition $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. Possible quantum channels may be served by four entangled pairs [17], two entangled trios [18] or one six-qubit cluster state [19]. Here we are concerned with the most economical quantum resource that consists only of three nonmaximally entangled pairs [20]

$$\begin{aligned} |Q_2\rangle_{A_1B_1A_2C_1B_2C_2} &= (\mu\,|00\rangle + \nu\,|11\rangle)_{A_1B_1} \\ &\otimes(\mu\,|00\rangle + \nu\,|11\rangle)_{A_2C_1} \\ &\otimes(\mu\,|00\rangle + \nu\,|11\rangle)_{B_2C_2}, \end{aligned} \tag{19}$$

of which qubits A_1, A_2 belong to Alice, qubits B_1, B_2 to Bob and qubits C_1, C_2 to Charlie. Clearly, the state $|\Psi_2\rangle$ is fully characterized by the data set $S = \{\alpha, \beta, \gamma, \delta\}$. Let us consider two data subsets $S_A = \{a, b, c, d\} \in R$ and $S_B = \left\{\overline{x}, \overline{y}, \overline{z}, \overline{t}\right\} \in \mathcal{C}$. Generally, the information can be split as

$$\begin{aligned} \overline{x} &= f_x(a, b, c, d, \alpha, \beta, \gamma, \delta, \mu, \nu), \\ \overline{y} &= f_y(a, b, c, d, \alpha, \beta, \gamma, \delta, \mu, \nu), \\ \overline{z} &= f_z(a, b, c, d, \alpha, \beta, \gamma, \delta, \mu, \nu), \\ \overline{t} &= f_t(a, b, c, d, \alpha, \beta, \gamma, \delta, \mu, \nu), \end{aligned} \tag{20}$$

with $f_{x(y,z,t)}(a, b, c, d, \alpha, \beta, \gamma, \delta, \mu, \nu)$ being some well-defined functions of their arguments.

First we analyze the method in which μ, ν are kept secret to the two preparers but disclosed to the receiver and choose $f_{x(y,z,t)}(a, b, c, d, \alpha, \beta, \gamma, \delta, \mu, \nu)$ to have the following information splitting

$$\begin{aligned} \overline{x} &= \frac{d\nu\alpha - c\mu\gamma}{\mu^2\nu\Delta},\ \overline{y} = \frac{d\nu\beta - c\mu\delta}{\mu^2\nu\Delta}, \\ \overline{z} &= \frac{a\mu\gamma - b\nu\alpha}{\mu\nu^2\Delta},\ \overline{t} = \frac{a\mu\delta - b\nu\beta}{\mu\nu^2\Delta}, \end{aligned} \tag{21}$$

with a, b, c, d satisfying the condition $\Delta = ad - bc \neq 0$ to avoid mathematical singularity in Eqs. (21).

Alice measures qubits A_1, A_2 in a basis determined by the data subset $S_A = \{a, b, c, d\}$:

$$\begin{pmatrix} |u_1\rangle_{A_1A_2} \\ |u_2\rangle_{A_1A_2} \\ |u_3\rangle_{A_1A_2} \\ |u_4\rangle_{A_1A_2} \end{pmatrix} = \frac{1}{\sqrt{a^2 + b^2 + c^2 + d^2}} \begin{pmatrix} a & b & c & d \\ b & -a & d & -c \\ c & -d & -a & b \\ d & c & -b & -a \end{pmatrix} \begin{pmatrix} |00\rangle_{A_1A_2} \\ |01\rangle_{A_1A_2} \\ |10\rangle_{A_1A_2} \\ |11\rangle_{A_1A_2} \end{pmatrix}. \tag{22}$$

Note that the condition $\Delta \neq 0$ has a physical meaning. It means that Alice's measurement is a single collective two-qubit one, but not two individual single-qubit ones, i.e., state

$|u_m\rangle_{A_1A_2}$ for any $m \in \{1,2,3,4\}$ should not be a product state. As for Bob, he measures qubits B_1, B_2 in a basis determined by the data subset $S_B = \{\overline{x}, \overline{y}, \overline{z}, \overline{t}\}$:

$$\begin{pmatrix} |v_1\rangle_{B_1B_2} \\ |v_2\rangle_{B_1B_2} \\ |v_3\rangle_{B_1B_2} \\ |v_4\rangle_{B_1B_2} \end{pmatrix} = \frac{1}{\sqrt{|\overline{x}|^2+|\overline{y}|^2+|\overline{z}|^2+|\overline{t}|^2}} \begin{pmatrix} \overline{x}^* & \overline{y}^* & \overline{z}^* & \overline{t}^* \\ \lambda\overline{x}^* & \lambda\overline{y}^* & -\overline{z}^*/\lambda & -\overline{t}^*/\lambda \\ \overline{y} & -\overline{x} & \overline{t} & -\overline{z} \\ \lambda\overline{y} & -\lambda\overline{x} & -\overline{t}/\lambda & \overline{z}/\lambda \end{pmatrix} \begin{pmatrix} |00\rangle_{B_1B_2} \\ |01\rangle_{B_1B_2} \\ |10\rangle_{B_1B_2} \\ |11\rangle_{B_1B_2} \end{pmatrix} \tag{23}$$

with

$$\lambda = \sqrt{\frac{|\overline{z}|^2+|\overline{t}|^2}{|\overline{x}|^2+|\overline{y}|^2}} \tag{24}$$

to ensure the unitarity of the transformation (23). The state $|Q_2\rangle_{A_1B_1A_2C_1B_2C_2}$ can be rewritten in terms of $|u_m\rangle_{A_1A_2}$ and $|v_n\rangle_{B_1B_2}$ as

$$|Q_2\rangle_{A_1B_1A_2C_1B_2C_2} = \sum_{n=1}^{4}\sum_{m=1}^{4} |u_m\rangle_{A_1A_2} |v_n\rangle_{B_1B_2} |R_{mn}\rangle_{C_1C_2}. \tag{25}$$

The JRSP may succeed when Alice finds $|u_1\rangle_{A_1A_2}$ and Bob finds $|v_1\rangle_{B_1B_2}$ in which case

$$\begin{aligned} |R_{11}\rangle_{C_1C_2} \;=\; & \frac{1}{\sqrt{(a^2+b^2+c^2+d^2)(|\overline{x}|^2+|\overline{y}|^2+|\overline{z}|^2+|\overline{t}|^2)}} \\ & \times \left[\mu^2(a\mu\overline{x}+c\nu\overline{z})\,|00\rangle + \mu\nu(c\nu\overline{t}+a\mu\overline{y})\,|01\rangle \right. \\ & \left. + \mu\nu(b\mu\overline{x}+d\nu\overline{z})\,|10\rangle + \nu^2(d\nu\overline{t}+b\mu\overline{y})\,|11\rangle\right]_{C_1C_2}. \end{aligned} \tag{26}$$

Substituting Eqs. (21) into Eq. (26) yields

$$|R_{11}\rangle_{C_1C_2} = \frac{[\mu\alpha\,|00\rangle + \nu\beta\,|01\rangle + \mu\gamma\,|10\rangle + \nu\delta\,|11\rangle]_{C_1C_2}}{\sqrt{(a^2+b^2+c^2+d^2)(|\overline{x}|^2+|\overline{y}|^2+|\overline{z}|^2+|\overline{t}|^2)}}. \tag{27}$$

To transform state (27) to the target state $|\Psi_2\rangle_{C_1C_2}$ Charlie applies the two-qubit gate $U_{C_2C_3}(\nu^2/\mu^2)$ (see Eq. (11)) on qubit C_2 and an ancillary qubit C_3 that she prepared in state $|0\rangle_{C_3}$. Since

$$U_{C_2C_3}(\frac{\nu^2}{\mu^2})\,|R_{11}\rangle_{C_1C_2}\,|0\rangle_{C_3} = \frac{\nu\,|\Psi_2\rangle_{C_1C_2}\,|0\rangle_{C_3} + \frac{\mu}{|\mu|}\sqrt{|\mu|^2-|\nu|^2}(\alpha\,|0\rangle+\gamma\,|1\rangle)_{C_1}\,|11\rangle_{C_2C_3}}{\sqrt{(a^2+b^2+c^2+d^2)(|\overline{x}|^2+|\overline{y}|^2+|\overline{z}|^2+|\overline{t}|^2)}}, \tag{28}$$

if Charlie measures the ancilla in the computational basis and finds $|0\rangle_{C_3}$, then the state of the two unmeasured qubits C_1 and C_2 becomes $|\Psi_2\rangle_{C_1C_2}$ as desired, with the probability

$$\overline{P}_2 = \frac{|\nu|^2}{(a^2+b^2+c^2+d^2)(|\overline{x}|^2+|\overline{y}|^2+|\overline{z}|^2+|\overline{t}|^2)}. \tag{29}$$

As was recognized above in the case of single-qubit states, Charlie should not need know about the quantum channel and can still obtain the target state. In the case of two-qubit states this may be realized if the information $S = \{\alpha, \beta, \gamma, \delta\}$ is split wisely. We therefore

analyze another method in which μ, ν are hidden from all the three participants. This method could be successful in such a way that the receiver Charlie does not need doing anything. Namely, instead of $S_B = \left\{\overline{x}, \overline{y}, \overline{z}, \overline{t}\right\}$ defined by Eqs. (21), the superior can choose $S_B = \{x, y, z, t\}$ with

$$\begin{aligned} x =& \frac{d\nu\alpha - c\mu\gamma}{\mu^3\nu\Delta},\ y = \frac{d\nu\beta - c\mu\delta}{\mu^2\nu^2\Delta}, \\ z =& \frac{a\mu\gamma - b\nu\alpha}{\mu^2\nu^2\Delta},\ t = \frac{a\mu\delta - b\nu\beta}{\mu\nu^3\Delta}. \end{aligned} \tag{30}$$

Now the basis for Bob to measure qubits B_1, B_2 has the same form as in Eq. (23) but with $\overline{x}$, $\overline{y}$, $\overline{z}$ and $\overline{t}$ replaced by x, y, z and t, respectively. If so, when Alice finds $|u_1\rangle_{A_1A_2}$ and Bob finds $|v_1\rangle_{B_1B_2}$, the target state $|\Psi_2\rangle_{C_1C_2}$ appears automatically at Charlie's. The corresponding success probability reads

$$P_2 = \frac{1}{(a^2+b^2+c^2+d^2)(|x|^2+|y|^2+|z|^2+|t|^2)}, \tag{31}$$

which is, surprisingly, always higher than $\overline{P}_2$ because

$$\frac{P_2}{\overline{P}_2} - 1 = \frac{\left(|x|^2+|z|^2\right)\left(|\mu|^2-|\nu|^2\right)}{|\nu|^2(|x|^2+|y|^2+|z|^2+|t|^2)} > 0. \tag{32}$$

To evaluate possible values of P_2 we set $a = b = c = -d$, $\mu = \cos\theta$ and $\nu = \sin\theta$ with $0 < \theta < \pi/4$. Then, for a class of two-qubit states with $\alpha = i\beta = \gamma = (i\cos\varphi)/\sqrt{3}$ and $\delta = \sin\varphi$, we have

$$\begin{aligned} P_2 \ =\ & 6\{[3+\cos(2\theta)-\sin(4\theta)]\cos^2\varphi\csc^4\theta\sec^6\theta \\ & -4\sqrt{3}\cos\varphi\csc^5\theta\sec\theta\sin\varphi + 6\csc^6\theta\sin^2\varphi \\ & +6\csc^4\theta\sec^2\theta\sin^2\varphi + 16\sqrt{3}\csc^3(2\theta)\sin(2\varphi)\}^{-1}, \end{aligned} \tag{33}$$

where $\zeta = \theta - \pi/4$. Figure 2 is a plot of P_2 given by Eq. (33) as a function of θ for several values of φ. In the limit of $\theta \to \pi/4$ (i.e., $|Q_2\rangle$ tends to a maximally entangled state) $P_2 \to 1/16$, while in the limit of $\theta \to 0$ (i.e., $|Q_1\rangle$ tends to a separable state) $P_2 \to 0$. However, P_2 may exceed $1/16$ for a certain range of θ and φ.

III. CONCLUSION

In conclusion, we have proposed JRSP protocols which are absolutely secure in the sense that all the participants, even when they are in connivance with each other, are unable to retrieve the full information of the state to be prepared, from the partial informations that they are allowed to know. This is achieved by exploiting the quantum channel in terms of nonmaximally entangled states combined with a proper way to split the secret information. The key idea is to hide from all the participants (i.e., the preparers plus the receiver) the quantum channel's characteristic parameters which are however taken judiciously into account in the information splitting. By doing so not only the security is boosted to the highest level but the protocols' execution is also the simplest: the receiver does not need any ancillas nor any operations/measurements, as opposed to any other existing protocols. Furthermore, in the JRSP protocols proposed in this paper,

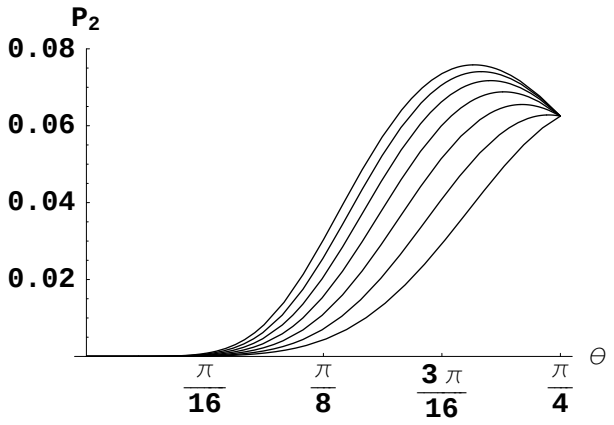

Fig. 2. The success probability P_2, Eq. (33), as a function of θ for $\varphi = \pi/3$, $\pi/4$, $\pi/5$, $\pi/6$, $\pi/7$, $\pi/8$ and $\pi/9$, upwards.

not only the quantum resource, but also the number of bits for classical communication is minimum. Just one bit per preparer is required to inform the measurement outcome: '1' if $m = 1$ ($n = 1$) and '0' otherwise. The JRSP is by itself state-dependent. Here we are interested in the most general quantum states characterized by complex coefficients. Nevertheless, there are possibilities to trade off the resources from different contexts. For example, if the coefficients of the state to be prepared are all real or for an ensemble of some special states, the measurement bases for the preparers may be simplified so as to significantly increase the success probability [20]. Existing protocols for JRSP of multiqubit states [21] can also be made absolutely secure with resort to the strategy of using nonmaximal entanglement combined with proper information splitting as described in this paper.

ACKNOWLEDGMENTS

The authors are grateful to N. V. Don for his contribution in the initial stage of this work.

REFERENCES

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computaion and Quantum Information* (Cambridge Univertity Press, Cambridge, 2000).
[2] C. H. Bennett, H. J. Bernstein, S. Popescu and B. Schumacher, *Phys. Rev. A* **53** (1996) 2046.
[3] B. Reznik *quant-ph/0203055* (2002).
[4] B. Groisman and B. Reznik, *Phys. Rev. A* **71** (2005) 032322.
[5] M. Horodecki , A. Sen De , U. Sen and K. Horodecki, *Phys. Rev. Lett.* **90** (2003) 047902.
[6] S. Mozes, J. Oppenheim and B. Reznik, *Phys. Rev. A* **71** (2005) 012311.
[7] J. Modlawska and A. Grudka, *Phys. Rev. Lett.* **100** (2008) 110503.
[8] J. Modlawska and A. Grudka, *Phys. Rev. A* **79** (2009) 064302.
[9] G. Chimczak and R. Tannas, *Phys. Rev. A* **79** (2009) 042311.
[10] K. Shimiza, K. Tamaki and H. Fukasaka, *Phys. Rev. A* **80** (2009) 022323.
[11] G. Gordon and G. Rigolin, *Opt. Commun.* **283** (2010) 184.

[12] Y. Xia, J. Song and H. S. Song, *J. Phys. B: At. Mol. Opt. Phys.* **40** (2007) 3719.
[13] N. B. An and J. Kim, *J. Phys. B: At. Mol. Opt. Phys.* **41** (2008) 095501.
[14] N. B. An and J. Kim, *Int. J. Quant. Inf.* **6** (2008) 1051.
[15] C. T. Bich, N. V. Don and N. B. An, *Int. J. Theor. Phys.* **51** (2012) 2272.
[16] Y. Su, X. B. Chen and Y. X. Yang, *Int. J. Quant. Inf.* **10** (2012) 1250006.
[17] N. B. An, *J. Phys. B: At. Mol. Opt. Phys.* **42** (2009) 125501.
N. B. An, C. T. Bich and N. V. Don, *Phys. Lett. A* **375** (2011) 3570.
N. V. Don, C. T. Bich and N. B. An, *Commun. Phys.* **22** (2012) 193.
[18] X. Q. Xiao and J. M. Liu,. *J. Phys. B: At. Mol. Opt. Phys.* **44** (2011) 075501.
H. H. Liu, L. Y. Cheng, X. Q. Shao, L. L. Sun, S. Zhang and K. H. Yeon, *Int. J. Theor. Phys.* **50** (2011) 3023.
[19] N. B. An, *Commun. Phys.* **19** (2009) 1.
D. Wang, X. W. Zha and Q. Lan, *Opt. Commun.* **284** (2011) 5853.
[20] N. B. An, C. T. Bich and N. V. Don, *J. Phys. B: At. Mol. Opt. Phys.* **44** (2011) 135506.
[21] K. Hou, J. Wang, Y. L. Lu and S. H. Shi, *Int. J. Theor. Phys.* **48** (2009) 2005.
M. X. Luo, X. B. Chen, S. Y. Ma, Y. X. Yang and Z. M. Hu, *J. Phys. B: At. Mol. Opt. Phys.* **43** (2010) 065501.
M. X. Luo, X. B. Chen, S. Y. Ma, X. X. Niu and Y. X. Yang, *Opt. Commun.* **283** (2010) 4796.
N. B. An, *Opt. Commun.* **283** (2010) 4113.
Q. Q. Chen, Y. Xia, J. Song and N. B. An, *Phys. Lett. A* **374** (2010) 4483.
Q. Q. Chen, Y. Xia and N. B. An, *Opt. Commun.* **284** (1011) 2617.
Q. Q. Chen, Y. Xia and J. Song, *Opt. Commun.* **284** (2011) 5031.
Z. Y. Wang, *Int. J. Quant. Inf.* **9** (2011) 809.
Y. B. Zhan, B. L. Hu and P. C. Ma, *J. Phys. B: At. Mol. Opt. Phys.* **44** (2011) 095501.
Q. Q. Chen, Y. Xia and J. Song, *J. Phys. A: Math. Theor.* **45** (2012) 055303.
L. R. Long, P. Zhou, Z. Li and C. L. Yin, *Int. J. Theor. Phys.* **51** (2012) 2438.
P. Zhou, *J. Phys. A: Math. Theor.* **45** (2012) 215305.
K. Y. Yang and Y. Xia, *Int. J. Theor. Phys.* **51** (2012) 1647.
Y. Xia, Q. Q. Chen and N. B. An, *J. Phys. A: Math. Theor.* **45** (2012) 335306.
M. X. Luo and Y. Deng, *Int. J. Theor. Phys.* **51** (2012) 3027.
D. Wang and L. Ye, *Int. J. Theor. Phys.* **51** (2012) 3376.
X. W. Guan, X. B. Chen and Y. X. Yang, 2012 *Int. J. Theor. Phys.* **51** (1012) 3575.
Q. Q. Chen, Y. Xia and N. B. An, *Phys. Scr.* **87** (2013) 025005.
[22] M. X. Luo, X. B. Chen, Y. X. Yang and X. X. Niu, *Quantum Inf. Process.* **11** (2012) 751.
[23] H. K. Lo, *Phys. Rev.A* **62** (2000) 012313.
A. K. Pati, *Phys. Rev. A* **63** (2000) 014302.
C. H. Bennett, D. P., DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal and W. K. Wootters, *Phys. Rev. Lett.* **87** (2001) 077902.
N. B. An, C. T. Bich, N. V. Don and J. Kim, *Adv. Nat. Sci.: Nanosci. Nanotechnol.* **2** (2011) 035009.
[24] A. Broadbent, J. Fitzsimons and E. Kashefi, *Proceedings of the 50th Annual IEEE Symposium on Foumdation of Computer Science, 2009* (FOCS) 517.
S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger and P. Walther, *Science* **335** (2012) 303.