Eur. Phys. J. D **42**, 333–340 (2007)
DOI: 10.1140/epjd/e2007-00024-x

THE EUROPEAN PHYSICAL JOURNAL D

Quantum state sharing of an arbitrary multiqubit state using nonmaximally entangled GHZ states

Z.-X. Man[1,a], Y.-J. Xia[1,b], and N.B. An[2,3,c]

[1] College of Physics and Engineering, Qufu Normal University, Qufu 273165, P.R. China
[2] Institute of Physics and Electronics, 10 Dao Tan, Thu Le, Ba Dinh, Hanoi, Vietnam
[3] School of Computational Sciences, Korea Institute for Advanced Study, 207-43 Cheongryangni 2-dong, Dongdaemun-gu, Seoul 130-722, Korea

Received 3rd December 2006
Published online 9 February 2007 –

Abstract. We explicitly present a scheme for quantum state sharing of an arbitrary multiqubit state using nonmaximally entangled GHZ states as the quantum channel and generalized Bell states as the measurement basis. The scheme succeeds only probabilistically with its total success probability depending on the degree of entanglement matching between the quantum channel and the generalized Bell states. Security of the scheme is guaranteed by the fact that attacks of an outside eavesdropper or/and an inside dishonest party will inevitably introduce detectable errors.

PACS. 03.67.Hk Quantum communication – 03.67.Dd Quantum cryptography – 03.65.Ud Entanglement and quantum nonlocality (e.g. EPR paradox, Bell's inequalities, GHZ states, etc.)

QICS. 21.20.+s Quantum secret sharing / data hiding

1 Introduction

In classical secret sharing (see, e.g., [1,2]) a secret information is distributed among a number of users such that certain sufficiently large sets of users are able to access the information, but any smaller sets of them can by no means gain the meaning of the shared secret. This cryptographic task has been recognized as a powerful technique in information and computer sciences which enables secure and robust communication in relevant networks. However, the challenging problem of eavesdropping cannot be defeated efficiently by the classical dealing with secret sharing because any classical secret distributions can be eavesdropped perfectly without tracks left behind. In addition, it is impossible in principle to figure out existence of dishonest users, if any. Therefore, to guarantee an absolute security one should process the task in a quantum way, making use of laws of quantum physics.

Quantum secret sharing (QSS) is the generalization of classical secret sharing [1,2] into quantum scenario firstly by using three-particle and four-particle Greenberger-Horne-Zeilinger (GHZ) states [3]. After that a great deal of QSS schemes were proposed and most of them are focused on dealing with sharing a classical secret in terms of a classical message [4–13]. Since many applications in quantum information science require distribution of quantum states, there are also a lot of QSS schemes dealing with sharing a quantum secret in terms of a quantum state (see, e.g., [14–16,18–22]). This kind of sharing quantum information is referred to as quantum state sharing (QSTS) to differentiate from the QSS of classical information. The simplest case of QSTS concerning a single-qubit state was considered in references [3,16]. In reference [3], a single-qubit state is split among two parties by means of the GHZ state served as the quantum channel and the QSTS is processed by performing Bell-state measurements. Instead of using a GHZ state as the quantum channel, in reference [16], a single-qubit state can be distributed among two parties by using two Einstein-Podolsky-Rosen (EPR) pairs [17]. However, to implement the scheme of [16] the multipartite joint measurements are demanded. Since then several schemes were proposed for QSTS of an arbitrary N-qubit state with $N \geq 2$ [19–22]. In [19,20] the QSTS schemes of an arbitrary 2-particle state were presented by using EPR pairs as the quantum channels. For instance, for Alice to securely share an arbitrary 2-qubit secret state with her two remote parties, Bob and Charlie, four EPR pairs are consumed with the condition that both Bob and Charlie should be equipped with a perfect Bell-state analyzer. In case such a condition cannot be met, i.e., when Bob and Charlie are both technically limited, the schemes in [19,20] will not work. However, if the quantum channels in terms of GHZ states are used, this case turns out to be successful [21,22] again.

[a] e-mail: manzx81@hotmail.com
[b] e-mail: yjxia@mail.qfnu.edu.cn
[c] e-mail: nbaan@kias.re.kr

Namely, though in [21,22] two GHZ states play the role of the quantum channels, Bob and Charlie are only required to carry out single-qubit von Neumann projective measurements, which are technically much easier than the joint 2-qubit Bell-state measurements. Nevertheless, it is worth noting that, in references [21,22] the quantum channel used is assumed maximally entangled. Since generation and distribution of maximally entangled states are commonly recognized as a difficult (expensive) task due to errors in the production process or/and in the process of state transmission, of more practical interest is the direct use of nonmaximally entangled states as the quantum channel to achieve a task. This important idea was indeed exploited for various cryptographic tasks such as teleportation [23–25], QSTS [26], etc. In reference [26], schemes of QSTS for a single-qubit state were presented by using nonmaximally entangled states as the quantum channels.

In this work we consider the general case of QSTS of an arbitrary N-qubit state using N nonmaximally entangled GHZ states as the quantum channel. The N-qubit secret state can be reconstructed with unit fidelity by any receiver, who is chosen randomly by the sender, provided that the other receiver agrees to collaborate. Although using nonmaximally entangled quantum channels is more practical, the price to pay for faithful QSTS is that the success probability is always less than unity, i.e., the scheme becomes probabilistic rather than deterministic. We work out explicitly which kinds of measurements/operations should be performed by the authorized parties to achieve the task with an optimal success probability. We also propose a quantum way by means of additional decoy qubits to protect the scheme from an outside eavesdropper as well as from an inside cheater.

Our paper is structured as follows. In Section 2 we present in full detail the QSTS for the case of $N = 2$, for clarity. Section 3 outlines the scheme for the general case of an arbitrary $N \geq 2$. Finally, we conclusion in Section 4.

2 Quantum state sharing of an arbitrary 2-qubit state

For clarity, let us first consider in full detail the case of $N = 2$. Suppose that Alice is a technically powerful party who is capable of producing/distributing GHZ states as well as of performing any general 2-qubit joint measurements, but her two remote parties, Bob and Charlie, are technically limited being equipped with facilities which allow only for single-qubit measurements/operations. Now, Alice has an arbitrary 2-qubit secret state

$$|S\rangle_{12} = \alpha|00\rangle_{12} + \beta|01\rangle_{12} + \gamma|10\rangle_{12} + \delta|11\rangle_{12}, \quad (1)$$

with its secrecy contained in the coefficients α, β, γ and δ ($|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$) and she wishes to send this state to Bob and Charlie in such a way that only one of them (who will be selected at random by Alice) is able to faithfully reconstruct the state with the help of the other party, regardless of possible existence of any outside eavesdropper and/or inside cheater. Such a task can be done with unit success probability if Alice, Bob and Charlie priorly share a pair of maximally entangled Bell states [19,20] or GHZ states [21,22]. To be more practical, here we are interested in the circumstances when the two shared GHZ states are nonmaximally entangled which are of the form ($i \in \{1, 2\}$)

$$|Q\rangle_{A_iB_iC_i} = \mu|000\rangle_{A_iB_iC_i} + \nu|111\rangle_{A_iB_iC_i}, \quad (2)$$

where the coefficients μ, ν satisfy the normalization condition $|\mu|^2 + |\nu|^2 = 1$ and $\mu, \nu \neq 1/\sqrt{2}$. We assume that the states $|Q\rangle_{A_iB_iC_i}$ are prepared/distributed by Alice and thus the values of μ, ν are known to her (but not necessarily known to Bob and Charlie).

As will be seen clearer later, here the usually used measurements in the standard Bell-state basis do not suit our problem. Hence, instead of the standard Bell states, we define another complete orthonormal set of four states, called generalized Bell states, which for a system of two arbitrary qubits X and Y are given by

$$|B_{00}\rangle_{XY} = a\,|00\rangle_{XY} + b\,|11\rangle_{XY}\,, \quad (3)$$
$$|B_{01}\rangle_{XY} = c\,|01\rangle_{XY} + d\,|10\rangle_{XY}\,, \quad (4)$$
$$|B_{10}\rangle_{XY} = d\,|01\rangle_{XY} - c\,|10\rangle_{XY}\,, \quad (5)$$
$$|B_{11}\rangle_{XY} = b\,|00\rangle_{XY} - a\,|11\rangle_{XY}\,, \quad (6)$$

where $|a|^2+|b|^2 = |c|^2+|d|^2 = 1$ and ${}_{XY}\langle B_{ii'}\,|B_{jj'}\rangle_{XY} = \delta_{ii'}\delta_{jj'}$. We assume that Alice is able to perform a generalized-Bell-state measurement (GBM) which is meant as a projective measurement onto one of the four generalized Bell states given by equations (3)–(6), with choice of the parameters a, b, c and d being at her disposal.

A particular issue in the secret sharing problem is that one (and only one) of Bob and Charlie may be dishonest, but Alice does not know precisely who of them is the dishonest one. The purpose of the dishonest party is to obtain Alice's secret state alone (even when he/she has not been assigned by Alice to reconstruct it) or to supply wrong information so that the other party cannot obtain the right state. These kinds of dishonesty of an inside party as well as eavesdropping of an outside party (called Eve) can be detected in our QSTS scheme which goes through several steps as follows.

Step 1. Suppose that Alice has a pair of nonmaximally entangled GHZ states in the form (2). To achieve her goal, she also prepares $4L$ (L is an integer large enough to ensure a required level of security) decoy single-qubits (served as checking qubits) $\{q_i^B, q_i^C, p_i^B, p_i^C\}$ ($i = 1, 2, ..., L$) such that $q_i^{B(C)}$ is randomly in one of the four states $\{|0\rangle, |1\rangle, |\widetilde{0}\rangle, |\widetilde{1}\rangle\}$ and $p_i^{B(C)}$ is randomly in one of the two states $\{|\widetilde{0}\rangle, |\widetilde{1}\rangle\}$, where $|\widetilde{0}\rangle$ and $|\widetilde{1}\rangle$ are the two orthonormal states in the x-basis

$$|\widetilde{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad (7)$$
$$|\widetilde{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \quad (8)$$

Then Alice randomly sends qubits $B_1, B_2, \{q_i^B\}, \{p_i^B\}$ to Bob and $C_1, C_2, \{q_i^C\}, \{p_i^C\}$ to Charlie (see Fig. 1a).

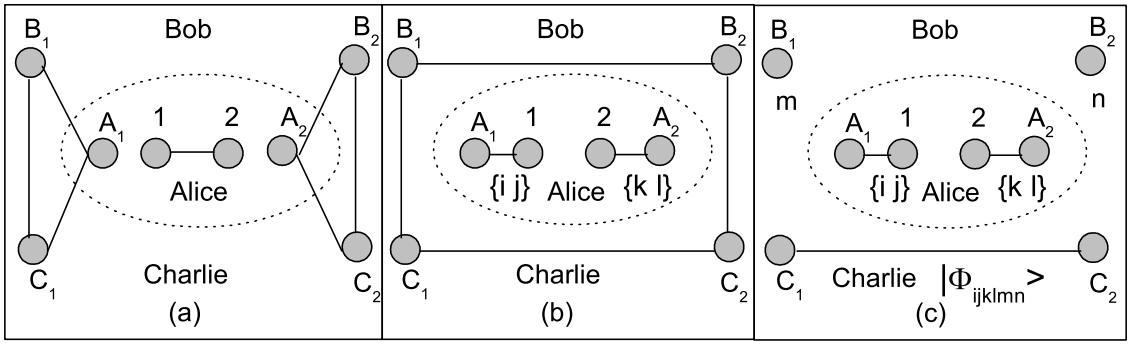

Fig. 1. A qubit is represented by a solid circle and an entanglement between qubits by solid lines. The checking qubits are omitted to avoid prolix. (a) After step 1 Alice holds a 2-qubit secret state $|S\rangle_{12}$ while Alice, Bob and Charlie share two nonmaximally entangled GHZ states $|Q\rangle_{A_1B_1C_1}$ and $|Q\rangle_{A_2B_2C_2}$; (b) after Alice's GBMs with outcomes $\{i,j\}$ and $\{k,l\}$, the qubits B_1, B_2, C_1 and C_2 become entangled with each other; (c) after Bob's single-qubit measurements on qubits B_1, B_2 with outcomes $\{m,n\}$, Charlie's two qubits are left in an entangled state $|\Phi_{ijklmn}\rangle$ that contains full information of Alice's original secret state.

It is important to note that although the qubits are sent out in a random order, the sending order is precisely known to Alice but not to anyone else.

Step 2. After Bob and Charlie confirm that they have received all the qubits, Alice reveals the position of the checking qubits $\{q_i^B\}$ and $\{q_i^C\}$ and asks Bob and Charlie to measure them in the appropriate bases (i.e., in those they have been prepared by Alice) and then announce her their results. Through a careful statistical analysis of the measurement outcomes for the checking qubits $\{q_i^B, q_i^C\}$, Alice is able to assess the error rate of secure sharing of the quantum channel. If it exceeds a predetermined threshold, she decides to abort the scheme. Otherwise, she proceeds to the next step.

Step 3. Alice makes two GBMs, one on the qubit pair $\{1, A_1\}$ and the other on $\{2, A_2\}$, with the outcomes $\{i,j\}$ and $\{k,l\}$ if she finds $|B_{ij}\rangle_{1A_1}$ and $|B_{kl}\rangle_{2A_2}$, respectively. Thanks to multipartite entanglement swapping [27], after the GBMs the four qubits B_1, B_2, C_1 and C_2 are projected onto a genuine four-partite entangled state characterized by α, β, γ and δ. That is, the information of Alice's original quantum secret state has been transferred to the state of qubits B_1, B_2, C_1 and C_2 (see Fig. 1b).

Step 4. Alice randomly selects either Bob or Charlie to reconstruct her secret state (the selection should not be learn beforehand by neither Bob nor Charlie). For concreteness, let Charlie be selected by Alice (The case when Bob is selected is similar because of the Bob-Charlie symmetry in this problem). If so, Alice asks Bob to measure all the $L+2$ remaining qubits (i.e., the two qubits B_1, B_2 and the L checking qubits $\{p_i^B\}$) in the x-basis then publicly announce all his results. Note that Bob cannot distinguish between the $L+2$ qubits but Alice can because she knows the order in which she has sent them out. Just for illustration, let the order be $\{p_1^B, p_2^B, ..., p_L^B, B_1, B_2\}$ and Bob's measurement results be $\{r_1, r_2, ..., r_L, m, n\}$ $(r_i, m, n \in \{0,1\})$ if Bob finds $|\widetilde{r_1}\rangle_{p_1^B}$, $|\widetilde{r_2}\rangle_{p_2^B}$, ..., $|\widetilde{r_L}\rangle_{p_L^B}$, $|\widetilde{m}\rangle_{B_1}$ and $|\widetilde{n}\rangle_{B_2}$, respectively. Then, through a careful analysis of the measurement results $\{r_i\}$ for the checking qubits $\{p_i^B\}$, Alice is able to assess the error rate caused by Bob's dishonesty. If it exceeds a predetermined threshold, she decides to abort the scheme. Otherwise, she accepts that Bob has not cheated, i.e., the qubit B_1 has been in the state $|\widetilde{m}\rangle_{B_1}$ and the qubit B_2 in the state $|\widetilde{n}\rangle_{B_2}$. As a consequence, Charlie's two qubits C_1 and C_2 will collapse onto the state $|\Phi_{ijklmn}\rangle_{C_1C_2}$ which is of the form

$$|\Phi_{ijklmn}\rangle_{C_1C_2} = \xi_{ijklmn}|00\rangle_{C_1C_2} + \zeta_{ijklmn}|01\rangle_{C_1C_2} + \sigma_{ijklmn}|10\rangle_{C_1C_2} + \tau_{ijklmn}|11\rangle_{C_1C_2} \quad (9)$$

where the coefficients ξ_{ijklmn}, ζ_{ijklmn}, σ_{ijklmn} and τ_{ijklmn} are determined by Alice's and Bob's measurement outcomes (see Fig. 1c). Evidently, after this step Alice's secret information has been contained in the state $|\Phi_{ijklmn}\rangle_{C_1C_2}$ of Charlie's qubits.

Step 5. Since like Bob Charlie has no idea about the order of her $L+2$ qubits $\{p_i^C\}$, C_1 and C_2, Alice publicly reveals Charlie the precise position of the qubits C_1 and C_2 followed by her and Bob's measurement outcomes (which is a classical message) in the form $\{ijklmn\}$ according to which Charlie is able to transform $|\Phi_{ijklmn}\rangle_{C_1C_2}$ to the desired state $|S\rangle_{C_1C_2}$ by applying an appropriate unitary operator $U_{ijklmn}^{C_1C_2}$ (to be specified later) on her two qubits C_1 and C_2.

Although using nonmaximally entangled quantum channels is more practical than using maximally entangled ones, the price to pay for faithful QSTS is that the success probability is always less than unity, i.e., the scheme becomes probabilistic rather than deterministic. To elucidate this point let us write the total state $|T\rangle_{12A_1B_1C_1A_2B_2C_2} = |S\rangle_{12}|Q\rangle_{A_1B_1C_1}|Q\rangle_{A_2B_2C_2}$ of the secret state and the quantum channels in terms of the generalized Bell states

Table 1. The correspondence between the coefficients ξ_{ijklmn}, ζ_{ijklmn}, σ_{ijklmn} and τ_{ijklmn} of state $|\Phi_{ijklmn}\rangle_{C_1C_2}$ (see Eq. (10)) and the measurement outcome $\{ijklmn\}$.

Case #	$ijklmn$	ξ_{ijklmn}	ζ_{ijklmn}	σ_{ijklmn}	τ_{ijklmn}
1	000000	$a^2\alpha\mu^2$	$ab\beta\mu\nu$	$ab\gamma\mu\nu$	$b^2\delta\nu^2$
2	000001	$a^2\alpha\mu^2$	$-ab\beta\mu\nu$	$ab\gamma\mu\nu$	$-b^2\delta\nu^2$
3	000010	$a^2\alpha\mu^2$	$ab\beta\mu\nu$	$-ab\gamma\mu\nu$	$-b^2\delta\nu^2$
4	000011	$a^2\alpha\mu^2$	$-ab\beta\mu\nu$	$-ab\gamma\mu\nu$	$b^2\delta\nu^2$
5	000100	$ac\beta\mu^2$	$ad\alpha\mu\nu$	$bc\delta\mu\nu$	$bd\gamma\nu^2$
6	000101	$ac\beta\mu^2$	$-ad\alpha\mu\nu$	$bc\delta\mu\nu$	$-bd\gamma\nu^2$
7	000110	$ac\beta\mu^2$	$ad\alpha\mu\nu$	$-bc\delta\mu\nu$	$-bd\gamma\nu^2$
8	000111	$ac\beta\mu^2$	$-ad\alpha\mu\nu$	$-bc\delta\mu\nu$	$bd\gamma\nu^2$
9	001000	$ad\beta\mu^2$	$-ac\alpha\mu\nu$	$bd\delta\mu\nu$	$-bc\gamma\nu^2$
10	001001	$ad\beta\mu^2$	$ac\alpha\mu\nu$	$bd\delta\mu\nu$	$bc\gamma\nu^2$
11	001010	$ad\beta\mu^2$	$-ac\alpha\mu\nu$	$-bd\delta\mu\nu$	$bc\gamma\nu^2$
12	001011	$ad\beta\mu^2$	$ac\alpha\mu\nu$	$-bd\delta\mu\nu$	$-bc\gamma\nu^2$
13	001100	$ab\alpha\mu^2$	$-a^2\beta\mu\nu$	$b^2\gamma\mu\nu$	$-ab\delta\nu^2$
14	001101	$ab\alpha\mu^2$	$a^2\beta\mu\nu$	$b^2\gamma\mu\nu$	$ab\delta\nu^2$
15	001110	$ab\alpha\mu^2$	$-a^2\beta\mu\nu$	$-b^2\gamma\mu\nu$	$ab\delta\nu^2$
16	001111	$ab\alpha\mu^2$	$a^2\beta\mu\nu$	$-b^2\gamma\mu\nu$	$-ab\delta\nu^2$
17	010000	$ac\gamma\mu^2$	$bc\delta\mu\nu$	$ad\alpha\mu\nu$	$bd\beta\nu^2$
18	010001	$ac\gamma\mu^2$	$-bc\delta\mu\nu$	$ad\alpha\mu\nu$	$-bd\beta\nu^2$
19	010010	$ac\gamma\mu^2$	$bc\delta\mu\nu$	$-ad\alpha\mu\nu$	$-bd\beta\nu^2$
20	010011	$ac\gamma\mu^2$	$-bc\delta\mu\nu$	$-ad\alpha\mu\nu$	$bd\beta\nu^2$
21	010100	$c^2\delta\mu^2$	$cd\gamma\mu\nu$	$cd\beta\mu\nu$	$d^2\alpha\nu^2$
22	010101	$c^2\delta\mu^2$	$-cd\gamma\mu\nu$	$cd\beta\mu\nu$	$-d^2\alpha\nu^2$
23	010110	$c^2\delta\mu^2$	$cd\gamma\mu\nu$	$-cd\beta\mu\nu$	$-d^2\alpha\nu^2$
24	010111	$c^2\delta\mu^2$	$-cd\gamma\mu\nu$	$-cd\beta\mu\nu$	$d^2\alpha\nu^2$
25	011000	$cd\delta\mu^2$	$-c^2\gamma\mu\nu$	$d^2\beta\mu\nu$	$-cd\alpha\nu^2$
26	011001	$cd\delta\mu^2$	$c^2\gamma\mu\nu$	$d^2\beta\mu\nu$	$cd\alpha\nu^2$
27	011010	$cd\delta\mu^2$	$-c^2\gamma\mu\nu$	$-d^2\beta\mu\nu$	$cd\alpha\nu^2$
28	011011	$cd\delta\mu^2$	$c^2\gamma\mu\nu$	$-d^2\beta\mu\nu$	$-cd\alpha\nu^2$
29	011100	$bc\gamma\mu^2$	$-ac\delta\mu\nu$	$bd\alpha\mu\nu$	$-ad\beta\nu^2$
30	011101	$bc\gamma\mu^2$	$ac\delta\mu\nu$	$bd\alpha\mu\nu$	$ad\beta\nu^2$
31	011110	$bc\gamma\mu^2$	$-ac\delta\mu\nu$	$-bd\alpha\mu\nu$	$ad\beta\nu^2$
32	011111	$bc\gamma\mu^2$	$ac\delta\mu\nu$	$-bd\alpha\mu\nu$	$-ad\beta\nu^2$
33	100000	$ad\gamma\mu^2$	$bd\delta\mu\nu$	$-ac\alpha\mu\nu$	$-bc\beta\nu^2$
34	100001	$ad\gamma\mu^2$	$-bd\delta\mu\nu$	$-ac\alpha\mu\nu$	$bc\beta\nu^2$
35	100010	$ad\gamma\mu^2$	$bd\delta\mu\nu$	$ac\alpha\mu\nu$	$bc\beta\nu^2$
36	100011	$ad\gamma\mu^2$	$-bd\delta\mu\nu$	$ac\alpha\mu\nu$	$-bc\beta\nu^2$
37	100100	$cd\delta\mu^2$	$d^2\gamma\mu\nu$	$-c^2\beta\mu\nu$	$-cd\alpha\nu^2$
38	100101	$cd\delta\mu^2$	$-d^2\gamma\mu\nu$	$-c^2\beta\mu\nu$	$cd\alpha\nu^2$
39	100110	$cd\delta\mu^2$	$d^2\gamma\mu\nu$	$c^2\beta\mu\nu$	$cd\alpha\nu^2$
40	100111	$cd\delta\mu^2$	$-d^2\gamma\mu\nu$	$c^2\beta\mu\nu$	$-cd\alpha\nu^2$
41	101000	$d^2\delta\mu^2$	$-cd\gamma\mu\nu$	$-cd\beta\mu\nu$	$c^2\alpha\nu^2$
42	101001	$d^2\delta\mu^2$	$cd\gamma\mu\nu$	$-cd\beta\mu\nu$	$-c^2\alpha\nu^2$
43	101010	$d^2\delta\mu^2$	$-cd\gamma\mu\nu$	$cd\beta\mu\nu$	$-c^2\alpha\nu^2$
44	101011	$d^2\delta\mu^2$	$cd\gamma\mu\nu$	$cd\beta\mu\nu$	$c^2\alpha\nu^2$
45	101100	$bd\gamma\mu^2$	$-ad\delta\mu\nu$	$-bc\alpha\mu\nu$	$ac\beta\nu^2$
46	101101	$bd\gamma\mu^2$	$ad\delta\mu\nu$	$-bc\alpha\mu\nu$	$-ac\beta\nu^2$
47	101110	$bd\gamma\mu^2$	$-ad\delta\mu\nu$	$bc\alpha\mu\nu$	$-ac\beta\nu^2$
48	101111	$bd\gamma\mu^2$	$ad\delta\mu\nu$	$bc\alpha\mu\nu$	$ac\beta\nu^2$
49	110000	$ab\alpha\mu^2$	$b^2\beta\mu\nu$	$-a^2\gamma\mu\nu$	$-ab\delta\gamma^2$
50	110001	$ab\alpha\mu^2$	$-b^2\beta\mu\nu$	$-a^2\gamma\mu\nu$	$ab\delta\gamma^2$
51	110010	$ab\alpha\mu^2$	$b^2\beta\mu\nu$	$a^2\gamma\mu\nu$	$ab\delta\gamma^2$
52	110011	$ab\alpha\mu^2$	$-b^2\beta\mu\nu$	$a^2\gamma\mu\nu$	$-ab\delta\gamma^2$
53	110100	$bc\beta\mu^2$	$bd\alpha\mu\nu$	$-ac\delta\mu\nu$	$-ad\gamma\nu^2$
54	110101	$bc\beta\mu^2$	$-bd\alpha\mu\nu$	$-ac\delta\mu\nu$	$ad\gamma\nu^2$
55	110110	$bc\beta\mu^2$	$bd\alpha\mu\nu$	$ac\delta\mu\nu$	$ad\gamma\nu^2$
56	110111	$bc\beta\mu^2$	$-bd\alpha\mu\nu$	$ac\delta\mu\nu$	$-ad\gamma\nu^2$
57	111000	$bd\beta\mu^2$	$-bc\alpha\mu\nu$	$-ad\delta\mu\nu$	$ac\gamma\nu^2$
58	111001	$bd\beta\mu^2$	$bc\alpha\mu\nu$	$-ad\delta\mu\nu$	$-ac\gamma\nu^2$
59	111010	$bd\beta\mu^2$	$-bc\alpha\mu\nu$	$ad\delta\mu\nu$	$-ac\gamma\nu^2$
60	111011	$bd\beta\mu^2$	$bc\alpha\mu\nu$	$ad\delta\mu\nu$	$ac\gamma\nu^2$
61	111100	$b^2\alpha\mu^2$	$-ab\beta\mu\nu$	$-ab\gamma\mu\nu$	$a^2\delta\nu^2$
62	111101	$b^2\alpha\mu^2$	$ab\beta\mu\nu$	$-ab\gamma\mu\nu$	$-a^2\delta\nu^2$
63	111110	$b^2\alpha\mu^2$	$-ab\beta\mu\nu$	$ab\gamma\mu\nu$	$-a^2\delta\nu^2$
64	111111	$b^2\alpha\mu^2$	$ab\beta\mu\nu$	$ab\gamma\mu\nu$	$a^2\delta\nu^2$

(see Eqs. (3)–(6)) and the x-basis states (see Eqs. (7) and (8)) as

$$|T\rangle_{12A_1B_1C_1A_2B_2C_2} = \frac{1}{2}\sum_{i,j,k,l,m,n=0}^{1} |B_{ij}\rangle_{1A_1}|B_{kl}\rangle_{2A_2} \times |\widetilde{m}\rangle_{B_1}|\widetilde{n}\rangle_{B_2}|\Phi_{ijklmn}\rangle_{C_1C_2}. \quad (10)$$

The explicit dependence of $|\Phi_{ijklmn}\rangle_{C_1C_2}$ on $\{ijklmn\}$ is tabulated in Table 1.

The data in Table 1 show that for given quantum channels, i.e., for given μ and ν, success of the scheme is sensitive to the parameters a, b, c and d, which Alice can choose at her will to optimize the performance. In total, there are 9 possible sets of choice for the parameters.

Choice 1. If $a, b, c, d \notin \{\mu, \nu\}$, then the scheme fails absolutely, i.e., $p_{ijklmn} \equiv 0$ for any i, j, k, l, m and n, where p_{ijklmn} denotes the success probability corresponding to the outcome $\{ijklmn\}$.

Choice 2. If $a = \nu, b = \mu$ but $c, d \notin \{\mu, \nu\}$, then the only nonzero success probabilities are $p_{0000mn} = \mu^4\nu^4/4$ for any $m, n \in \{0, 1\}$ leading to the total success probability $P = \sum_{m,n=0}^{1} p_{0000mn} = \mu^4\nu^4$.

Choice 3. If $a, b \notin \{\mu, \nu\}$ but $c = \nu, d = \mu$, then the only nonzero success probabilities are $p_{0101mn} = \mu^4\nu^4/4$ for any $m, n \in \{0, 1\}$ leading to the total success probability $P = \sum_{m,n=0}^{1} p_{0101mn} = \mu^4\nu^4$.

Choice 4. If $a, b \notin \{\mu, \nu\}$ but $c = \mu, d = \nu$, then the only nonzero success probabilities are $p_{1010mn} = \mu^4\nu^4/4$ for any $m, n \in \{0, 1\}$ leading to the total success probability $P = \sum_{m,n=0}^{1} p_{1010mn} = \mu^4\nu^4$.

Choice 5. If $a = \mu, b = \nu$ but $c, d \notin \{\mu, \nu\}$, then the only nonzero success probabilities are $p_{1111mn} = \mu^4\nu^4/4$ for any $m, n \in \{0, 1\}$ leading to the total success probability $P = \sum_{m,n=0}^{1} p_{1111mn} = \mu^4\nu^4$.

Choice 6. If $a = c = \nu$ and $b = d = \mu$, then the only nonzero success probabilities are $p_{0j0lmn} = \mu^4\nu^4/4$ for

Table 2. Correspondence between the successful measurement outcomes $\{ijklmn\}$, Charlie's collapsed states $|S'\rangle_{C_1C_2}$ and the respective unitary operators $U^{C_1C_2}_{ijklmn}$.

Case #	$ijklmn$	$\|S'\rangle_{C_1C_2}$	$U^{C_1C_2}_{ijklmn}$
1	000000	$(\alpha\|00\rangle+\beta\|01\rangle+\gamma\|10\rangle+\delta\|11\rangle)_{C_1C_2}$	$I^{C_1}\otimes I^{C_2}$
2	000001	$(\alpha\|00\rangle-\beta\|01\rangle+\gamma\|10\rangle-\delta\|11\rangle)_{C_1C_2}$	$I^{C_1}\otimes \sigma_z^{C_2}$
3	000010	$(\alpha\|00\rangle+\beta\|01\rangle-\gamma\|10\rangle-\delta\|11\rangle)_{C_1C_2}$	$\sigma_z^{C_1}\otimes I^{C_2}$
4	000011	$(\alpha\|00\rangle-\beta\|01\rangle-\gamma\|10\rangle+\delta\|11\rangle)_{C_1C_2}$	$\sigma_z^{C_1}\otimes \sigma_z^{C_2}$
5	000100	$(\beta\|00\rangle+\alpha\|01\rangle+\delta\|10\rangle+\gamma\|11\rangle)_{C_1C_2}$	$I^{C_1}\otimes \sigma_x^{C_2}$
6	000101	$(\beta\|00\rangle-\alpha\|01\rangle+\delta\|10\rangle-\gamma\|11\rangle)_{C_1C_2}$	$I^{C_1}\otimes i\sigma_y^{C_2}$
7	000110	$(\beta\|00\rangle+\alpha\|01\rangle-\delta\|10\rangle-\gamma\|11\rangle)_{C_1C_2}$	$\sigma_z^{C_1}\otimes \sigma_x^{C_2}$
8	000111	$(\beta\|00\rangle-\alpha\|01\rangle-\delta\|10\rangle+\gamma\|11\rangle)_{C_1C_2}$	$\sigma_z^{C_1}\otimes i\sigma_y^{C_2}$
9	010000	$(\gamma\|00\rangle+\delta\|01\rangle+\alpha\|10\rangle+\beta\|11\rangle)_{C_1C_2}$	$\sigma_x^{C_1}\otimes I^{C_2}$
10	010001	$(\gamma\|00\rangle-\delta\|01\rangle+\alpha\|10\rangle-\beta\|11\rangle)_{C_1C_2}$	$\sigma_x^{C_1}\otimes \sigma_z^{C_2}$
11	010010	$(\gamma\|00\rangle+\delta\|01\rangle-\alpha\|10\rangle-\beta\|11\rangle)_{C_1C_2}$	$i\sigma_y^{C_1}\otimes I^{C_2}$
12	010011	$(\gamma\|00\rangle-\delta\|01\rangle-\alpha\|10\rangle+\beta\|11\rangle)_{C_1C_2}$	$i\sigma_y^{C_1}\otimes \sigma_z^{C_2}$
13	010100	$(\delta\|00\rangle+\gamma\|01\rangle+\beta\|10\rangle+\alpha\|11\rangle)_{C_1C_2}$	$\sigma_x^{C_1}\otimes \sigma_x^{C_2}$
14	010101	$(\delta\|00\rangle-\gamma\|01\rangle+\beta\|10\rangle-\alpha\|11\rangle)_{C_1C_2}$	$\sigma_x^{C_1}\otimes i\sigma_y^{C_2}$
15	010110	$(\delta\|00\rangle+\gamma\|01\rangle-\beta\|10\rangle-\alpha\|11\rangle)_{C_1C_2}$	$i\sigma_y^{C_1}\otimes \sigma_x^{C_2}$
16	010111	$(\delta\|00\rangle-\gamma\|01\rangle-\beta\|10\rangle+\alpha\|11\rangle)_{C_1C_2}$	$i\sigma_y^{C_1}\otimes i\sigma_y^{C_2}$

any $j,l,m,n\in\{0,1\}$ leading to the total success probability $P=\sum_{j,l,m,n=0}^{1}p_{0j0lmn}=4\mu^4\nu^4$.

Choice 7. If $a=c=\mu$ and $b=d=\nu$, then the only nonzero success probabilities are $p_{1j1lmn}=\mu^4\nu^4/4$ for any $j,l,m,n\in\{0,1\}$ leading to the total success probability $P=\sum_{j,l,m,n=0}^{1}p_{1j1lmn}=4\mu^4\nu^4$.

Choice 8. If $a=d=\nu$ and $b=c=\mu$, then the only nonzero success probabilities are $p_{i0k0mn}=\mu^4\nu^4/4$ for any $i,k,m,n\in\{0,1\}$ leading to the total success probability $P=\sum_{i,k,m,n=0}^{1}p_{i0k0mn}=4\mu^4\nu^4$.

Choice 9. If $a=d=\mu$ and $b=c=\nu$, then the only nonzero success probabilities are $p_{i1k1mn}=\mu^4\nu^4/4$ for any $i,k,m,n\in\{0,1\}$ leading to the total success probability $P=\sum_{i,k,m,n=0}^{1}p_{i1k1mn}=4\mu^4\nu^4$.

After analyzing the choices above, two important observations are in order. The first one is that the scheme can never be of a 100% probability of success, i.e., it is only probabilistic. The second, more interesting, one is that the success probability is nonzero only when there exists a matching between the quantum channel (characterized by μ,ν) and the GBM (characterized by a,b,c,d). In other words, if there are no relations between μ,ν and a,b,c,d, then the scheme fails absolutely, as seen from the choice 1. However, if there exist relations between μ,ν and a,b,c,d, then the scheme succeeds probabilistically, as verified from the choices 2 to 9. Furthermore, the actual value of total success probability P is governed by the degree of matching. More precisely, if the GBM just half-matches with the quantum channel, as in the choices 2 to 5, the total success probability is just $P=\mu^4\nu^4$. Yet, Alice can increase P four times if she adjusts the parameters a,b,c,d so that they fit either one of the choices 6 to 9, which means a full-matching between the GBM and the quantum channel. Physically, the above-mentioned matching is associated with the amount of entanglement, i.e., the amount of ebit, possessed by the quantum channel and the generalized Bell states. The GBM does not match the quantum channel at all when the amount of ebit of all the four generalized Bell states differs from that of the quantum channel (choice 1). If the quantum channel and two (of the four) generalized Bell states possess the same amount of ebit, as for the choices 2 to 5, then a half-matching results. Finally, a full-matching occurs when the amount of ebit of both the quantum channel and each (of the four) generalized Bell state becomes equal, as in the choices 6 to 9. At this point we would like to emphazise the role of the GBM which is compulsorily necessary in our scheme based on nonmaximally entangled quantum channels. In fact, employing the standard Bell-state measurement (i.e., with $a=b=c=d=1/\sqrt{2}$) will always lead to a failure since this corresponds to the choice 1.

Having known of how to optimally manage the GBM let us concentrate on the choice 6 for which the total success probability is maximal (similar analysis goes with the other three optimal choices 7, 8 or 9). The correspondence between the successful measurement outcome $\{ijklmn\}$, the measurement-induced Charlie's collapsed state $|S'\rangle_{C_1C_2}$ and the respective unitary operator $U^{C_1C_2}_{ijklmn}$ that Charlie needs to apply on the $|S'\rangle_{C_1C_2}$ to convert it into the desired state $|S\rangle_{C_1C_2}$ is represented in Table 2.

From Table 2 we see that $U^{C_1C_2}_{ijklmn}=u^{C_1}_{ijklmn}\otimes v^{C_2}_{ijklmn}$ with $u^{C_1}_{ijklmn},v^{C_2}_{ijklmn}\in\{I^{C_i},\sigma_x^{C_i},i\sigma_y^{C_i},\sigma_z^{C_i}\}$ for any i,j,k,l,m,n. This implies that Charlie only needs single-qubit operations. It is interesting to notice that for this choice 6 the scheme succeeds only when $i=k=0$, i.e., right after her GBM, Alice is conclusively aware of whether the scheme would succeed or not. This fact suggests an economical management of the classical communication. Namely, the whole 6 bits $\{ijklmn\}$ of the full set of the measurement outcome need not to be published.

Instead, the parties make use of the following strategy. In step 3, after Alice performs the GBMs, if she does not obtain $i = k = 0$, she informs Bob and Charlie that the task has been failed. Otherwise, Alice continues but in step 5 she needs to announce just four bits $\{jlmn\}$ for Charlie to get the secret state using the corresponding unitary operator listed in Table 2. It is also worth noting that in our scheme knowledge of the quantum channel (i.e., the value of μ and ν) is not necessary for both Bob and Charlie. The only required technique is that they are capable of performing single-qubit von Neumann measurements and single-qubit unitary operations. Compared with the EPR pairs based schemes [19,20], where Bob and Charlie must be equipped with a Bell-state analyzer, this is an apparent advantage in situations when Bob and Charlie are technically limited.

Next we discuss on security of our protocol. In general, attacks may come from an outside eavesdropper Eve or/and from an inside dishonest party. The attempt of Eve is to get Alice's secret state by herself. Since Eve can by no means distinguish the checking qubits $\{q_i^B, q_i^C\}$ from the qubits B_1, B_2, C_1, C_2, to gain useful information, Eve must attack all of them. For example, she might capture all the qubits sent out by Alice and then sends her own fake qubits to Bob and Charlie instead. This attack should however be disclosed with a high probability in step 2 because there are no correspondences between states of the fake qubits prepared by Eve and the checking qubits $\{q_i^B, q_i^C\}$ prepared by Alice. Actually, any attacks Eve would adopt should introduce errors into the checking qubits and can thereby be detected through analyzing the error rate due to them. Concerning the inside parties, one of them may be dishonest. One aim of the dishonest party is to obtain the secret state alone even when he/she has not been assigned by Alice to reconstruct it. To achieve this goal, the dishonest party captures all the qubits sent out by Alice and then sends the other party his/her fake ones. Similar to the case of an outside Eve, because the dishonest party does not know in which states Alice's checking qubits $\{q_i^{B(C)}\}$ have been prepared, his/her fake qubits have no relations with them and therefore the attack must be detected in step 2 as well. Being aware of that, the dishonest party, when not being selected to reconstruct the secret state, may still want to derange the honest one from obtaining the correct state by cheating, i.e., by publishing the wrong measurement results. Such a kind of attack is also detectable in step 4 when Alice analyzes the published measurement results $\{r_i\}$ of the checking qubits $\{p_i^{B(C)}\}$. As a matter of fact, the chance for Eve and the dishonest party to escape from their attacks can be made arbitrarily small by increasing L, i.e., the number of the decoy checking qubits. Furthermore, if no attacks have been made at all, the probability for a party to obtain the secret state at his/her hands is just 50%, since which one of the two parties to reconstruct the state is randomly selected by Alice, as was mentioned before. If Alice's secrecy consists of a set of many different secret states, each party will on average obtain only one half of the set. Thus to access the entire Alice's secrecy the two parties still have to cooperate again at the final stage after the whole secret sharing process ends. This is another figure of merit that increases the security of the QSTS scheme.

3 Quantum state sharing of an arbitrary N-qubit state

We now generalize our scheme to the N-qubit case with an arbitrary $N \geq 2$. Suppose that Alice has an arbitrary N-qubit secret state that she would like to send to Bob and Charlie in such a way that they must cooperate in order to faithfully reconstruct this state. The secret state can generally be represented as

$$|S\rangle_{12\ldots N} = \sum_{i_1,i_2,\ldots,i_N=0}^{1} \alpha_{i_1 i_2 \ldots i_N} |i_1, i_2, \ldots, i_N\rangle_{12\ldots N}, \quad (11)$$

where $1, 2, \ldots, N$ label the N qubits in the state $|S\rangle_{12\ldots N}$ and $\sum_{i_1,i_2,\ldots,i_N=0}^{1} |\alpha_{i_1,i_2,\ldots,i_N}|^2 = 1$. The general QSTS scheme can be outlined as follows.

GS1. Alice has N nonmaximally entangled GHZ states $|Q\rangle_{A_j B_j C_j}$ in the form (2) with $j = 1, 2, ..., N$. In addition, she prepares $4L$ single checking qubits $\{q_i^B, q_i^C, p_i^B, p_i^C\}$ $(i = 1, 2, ..., L)$ such that $q_i^{B,C}$ is randomly in one of the four states $\{|0\rangle, |1\rangle, |\widetilde{0}\rangle, |\widetilde{1}\rangle\}$ and $p_i^{B,C}$ is randomly in one of the two states $\{|\widetilde{0}\rangle, |\widetilde{1}\rangle\}$. Then Alice sends out the qubits $B_1, B_2, ..., B_N, \{q_i^B\}, \{p_i^B\}$ to Bob and the qubits $C_1, C_2, ..., C_N, \{q_i^C\}, \{p_i^C\}$ to Charlie (see Fig. 2a) in a random order that she secretly records for a later use.

GS2. The same as in step 2 of the scheme for $N = 2$.

GS3. Alice makes N GBMs on the qubit pairs $\{1, A_1\}$, $\{2, A_2\}, ...,$ and $\{N, A_N\}$ with the outcomes $\{k_1, l_1\}$, $\{k_2, l_2\}, ...,$ and $\{k_N, l_N\}$ if she finds $|B_{k_1 l_1}\rangle_{1A_1}$, $|B_{k_2 l_2}\rangle_{2A_2}, ...,$ and $|B_{k_N l_N}\rangle_{NA_N}$, respectively. Due to multipartite entanglement swapping, after the N GBMs the $2N$ qubits B_1, $B_2, ..., B_N$, C_1, $C_2, ...,$ and C_N are projected onto a genuine $2N$-partite entangled state characterized by 2^N coefficients $\alpha_{i_1 i_2 \ldots i_N}$ that carry full information of Alice's original quantum secret state (see Fig. 2b).

GS4. Alice randomly selects either Bob or Charlie to reconstruct her secret state. Let Charlie be the selected one. If so, Alice asks Bob to measure the remaining $L + N$ qubits $\{p_i^B, \}, B_1, B_2, ..., B_N$ all in the x-basis then publicly announce his results. Because Alice knows the precise order in which the $L+N$ qubits have been sent out, she is able to evaluate Bob's honesty through a careful analysis of Bob's measurement results for the checking qubits $\{p_i^B\}$. If she finds out that Bob is dishonest she aborts the scheme. Otherwise, she accepts that Bob's results for the qubits B_1, $B_2, ...,$ and B_N are true which we denote by $\{m_1, m_2, ..., m_N\}$ if B_1, B_2, ..., and B_N have been found in the states

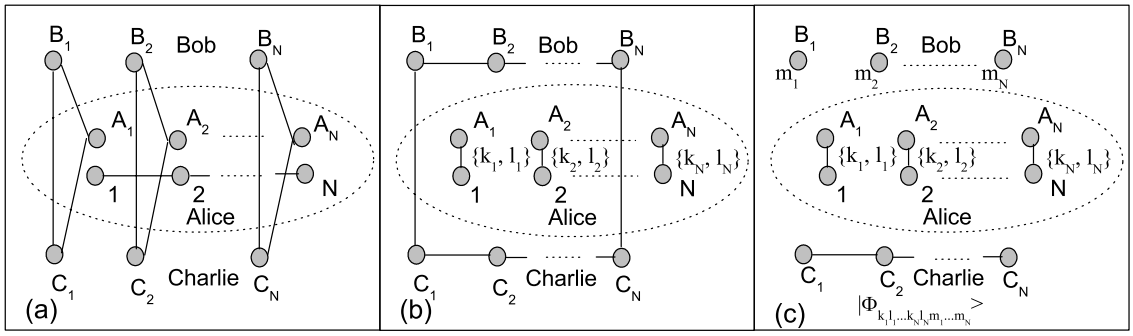

Fig. 2. A qubit is represented by a solid circle and an entanglement between qubits by solid lines. The checking qubits are omitted to avoid prolix. (a) After GS1 Alice holds a N-qubit secret state $|S\rangle_{12...N}$ while Alice, Bob and Charlie share N nonmaximally entangled GHZ states $|Q\rangle_{A_jB_jC_j}$ with $j = 1, 2, ..., N$; (b) after Alice's N GBMs with outcomes $\{k_1, l_1\}$, $\{k_2, l_2\}$, ... and $\{k_N, l_N\}$, the qubits B_1, $B_2, ..., B_N$ and C_1, $C_2, ..., C_N$ become entangled with each other; (c) after Bob's single-qubit measurements on qubits B_1, $B_2, ..., B_N$ with outcomes $\{m_1, m_2, ..., m_N\}$, Charlie's N qubits are left in an entangled state $|\Phi_{k_1l_1...k_Nl_Nm_1...m_N}\rangle_{C_1C_2...C_N}$ that contains full information of Alice's original secret state.

$|\widetilde{m_1}\rangle_{B_1}$, $|\widetilde{m_2}\rangle_{B_2}$, ..., and $|\widetilde{m_N}\rangle_{B_N}$, respectively. As a consequence, Charlie's N qubits C_1, C_2, ..., C_N will collapse onto the state $|\Phi_{k_1l_1...k_Nl_Nm_1...m_N}\rangle_{C_1C_2...C_N}$ which is of the form

$$|\Phi_{k_1l_1...k_Nl_Nm_1...m_N}\rangle_{C_1C_2...C_N} = \sum_{i_1,i_2,...,i_N=0}^{1} x_{i_1...i_N}^{k_1l_1...k_Nl_Nm_1...m_N} \times |i_1, i_2, ..., i_N\rangle_{C_1C_2...C_N} \quad (12)$$

with the coefficients $x_{i_1...i_N}^{k_1l_1...k_Nl_Nm_1...m_N}$ being determined by Alice's and Bob's measurement outcomes (see Fig. 2c).

GS5. Alice publicly broadcasts the precise position of the qubits $C_1, C_2, ..., C_N$ at Charlie's hands as well as her and Bob's measurement outcomes (which is a classical message) in the form $\{k_1l_1k_2l_2...k_Nl_Nm_1m_2...m_N\}$ according to which Charlie is able to transform $|\Phi_{k_1l_1k_2l_2...k_Nl_Nm_1m_2...m_N}\rangle_{C_1C_2...C_N}$ to the desired state $|S\rangle_{C_1C_2...C_N}$ by applying on the qubits C_1, $C_2, ..., C_N$ an appropriate unitary operator

$$U_{k_1l_1k_2l_2...k_Nl_Nm_1m_2...m_N}^{C_1C_2...C_N} = \otimes_{i=1}^{N} u(i)_{k_1l_1k_2l_2...k_Nl_Nm_1m_2...m_N}^{C_i} \quad (13)$$

with

$$u(i)_{k_1l_1k_2l_2...k_Nl_Nm_1m_2...m_N}^{C_i} \in \{I^{C_i}, \sigma_x^{C_i}, i\sigma_y^{C_i}, \sigma_z^{C_i}\}. \quad (14)$$

Clearly, as in the case $N = 2$, in the general scheme both Bob and Charlie need not to know the quantum channels and all what they need is the capacity of performing single-qubit measurements and single-qubit operations. The security of the general scheme against Eve and a dishonest party is also ensured by the checking procedures described in step GS2 and step GS4.

4 Conclusion

In conclusion, we have presented in full detail a quantum state sharing scheme of arbitrary 2-qubit state using two nonmaximally entangled three-partite GHZ states and measurements in the generalized Bell-state basis. The randomly chosen one among Bob and Charlie is able to reconstruct Alice's original secret state in cooperation with the other party with unit fidelity at the cost of less than unit success probability. For given quantum channels, i.e., for given parameters μ and ν, success of the scheme is sensitive to the generalized Bell-state measurement parameters a, b, c and d, which Alice can choose at her will to optimize the performance. Through analyzing the 9 possible choices for the parameters a, b, c and d, we have found out that the maximal total success probability $P = 4\mu^4\nu^4$ can be achieved when the generalized Bell states fully match the (nonmaximally entangled) quantum channel. In our scheme neither Bob nor Charlie need to know the quantum channels or to be capable of performing two-qubit joint measurements/operations. This is particularly favorable in circumstances when neither Bob nor Charlie are technically powerful. We have also proposed a security checking method through which not only the outsider's attacks but also the insider's cheating can be detected efficiently. Generalization to the scheme for sharing an arbitrary N-qubit with any $N \geq 2$ between $M = 2$ parties have been outlined as well. Extension to an arbitrary $M \geq 2$ parties is straightforward via $(M + 1)$-partite entangled state.

Z.X.M. and Y.J.X. are supported by the Key Program of National Natural Science Foundation of China under Grant No. 10534030, while N.B.A is supported by Vietnam Ministry of Science and Technology (under Project No. 403906) and Korea Ministry of Information and Communication.

References

1. A. Shamir, Comm. ACM **22**, 612 (1979)
2. J. Gruska, *Foundation of computing* (Thomson Computer Press, London, 1979), p. 504

3. M. Hillery, V. Buzk, A. Berthiaume, Phys. Rev. A **59**, 1829 (1999)
4. A. Karlsson, M. Koashi, N. Imoto, Phys. Rev. A **59**, 162 (1999)
5. D. Gottesman, Phys. Rev. A **61**, 012308 (2000)
6. V. Karimipour, A. Bahraminasab, S. Bagherinezhad, Phys. Rev. A **65**, 042320 (2002)
7. S. Bagherinezhad, V. Karimipour, Phys. Rev. A **67**, 044302 (2003)
8. T. Tyc, B.C. Sanders, Phys. Rev. A **65**, 042310 (2002)
9. L. Xiao, G.L. Long, F.G. Deng, J.W. Pan, Phys. Rev. A **69**, 052307 (2004)
10. G.P. Guo, G.C. Guo, Phys. Lett. A **310**, 247 (2003)
11. S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000)
12. Z.J. Zhang, Z.X. Man, Phys. Rev. A **72**, 022303 (2005); Z.J. Zhang, Y. Li, Z.X. Man, Phys. Rev. A **71**, 044301 (2005)
13. W. Tittel, H. Zbinden, N. Gisin, Phys. Rev. A **63**, 042301 (2001)
14. R. Cleve, D. Gottesman, H.K. Lo, Phys. Rev. Lett. **83**, 648 (1999)
15. A.C.A. Nascimento, Q.J. Mueller, H. Imai, Phys. Rev. A **64**, 042311 (2001)
16. Y.M. Li et al., Phys. Lett. A **324**, 420 (2004)
17. A. Einstein, B. Podolsky, N. Rosen, Phys. Rev. **47**, 777 (1935)
18. A.M. Lance et al., Phys. Rev. A **71**, 033814 (2005)
19. F.G. Deng et al., Phys. Rev. A **72**, 044301 (2005)
20. F.G. Deng et al., Eur. Phys. J. D **39**, 459 (2006)
21. F.G. Deng et al., Phys. Rev. A **72**, 022338 (2005)
22. X.H. Li et al., J. Phys. B: At. Mol. Opt. Phys. **39**, 1975 (2006)
23. W.L. Li, C.F. Li, G.C. Guo, Phys. Rev. A **61**, 034301 (2000)
24. P. Agrawal, A.K. Pati, Phys. Lett. A **305**, 12 (2002)
25. G. Gordon, G. Rigolin, Phys. Rev. A **73**, 042309 (2006)
26. G. Gordon, G. Rigolin, Phys. Rev. A **73**, 062316 (2006)
27. S. Bose, V. Vedral, P.L. Knight, Phys. Rev. A **57**, 822 (1998)