Quantum secret sharing with Greenberger Horne Zeilinger states

Comfort Sekga and Mhlambululi Mafu

Department of Physics and Astronomy, Botswana International University of Science and Technology, P/Bag 16, Palapye, Botswana

Abstract. We propose a scheme for sharing an unknown three-particle quantum state to n agents by using Greenberger-Horne-Zeilinger states. Firstly, we introduce the five party quantum state sharing scheme of arbitrary three particle unknown quantum states where Alice starts by sharing four Greenberger-Horne-Zeilinger entangled states with her four agents and performs three Greenberger-Horne-Zeilinger state measurements on her particles followed by two single particle measurements on the X basis. One of the agents Bob1 performs standard single measurement on her particle and three other agents each perform unitary transformations on their particles to recover the unknown state. Subsequently, we propose the generalized multiparty quantum state sharing scheme for an arbitrary three particle state.

1. Introduction

Quantum secret sharing (QSS) is a useful procedure of quantum information which involves the splitting and distribution of a secret message to untrusted agents who have to collaborate to recover the message [1]. A certain subset of agents can recover the message whilst other participants cannot get the full information about it. QSS is divided into two areas, the first is based on sharing classical secret information which is distributed among all agents with help of quantum mechanics. The second area deals with the distribution of quantum information with the secret being an arbitrary unknown quantum state [2]. This distribution of quantum state was referred as quantum state sharing (QSTS) by Lance *et. al* in 2004 [3]. QSTS has wide range of applications which include joint sharing of quantum money, quantum error correction and quantum information networks [4].

To date, various protocols of QSTS have been realized both experimentally and theoretically exploiting quantum resources such as Bell states [5] and Greenberger-Horne-Zeilinger (GHZ) states [6]. The first QSS scheme was proposed by Hillery *et. al* which used three and four particle GHZ state to distribute private message to two and three agents respectively [1]. Thereafter, Einstein, Podolsky and Rosen (EPR) pair of entangled states has been extensively used to share an arbitrarily unknown single and two-particle quantum state. Deng *et. al* proposed a scheme with an ordered n pairs of EPR states for multiparty quantum secret splitting [7]. Recently, Yuan *et. al* developed a protocol for tripartite QSTS of an arbitrary unknown quantum state which has the advantage of consuming less quantum and classical resources [8].

In this work, we propose a scheme for sharing an unknown three-particle quantum state to n agents by using GHZ states. In section II, we introduce the five party quantum state sharing scheme of arbitrary three particle unknown quantum state, where Alice starts by sharing four GHZ entangled states with her four agents, and performs three GHZ state measurements on her

particles followed by two single particle measurements on the X basis. One of the agents, Bob1, performs a single measurement on her particle and the three other agents each perform unitary transformations on their particles to recover the unknown state. This is followed by section III where we propose the generalized multiparty quantum state sharing scheme for an arbitrary three particle state. In this section, we show that our proposed scheme fairly performs better than other existing schemes. Finally, we provide concluding remarks in the last section.

2. Five party QSTS of an arbitrary three particle unknown state using GHZ states
In our proposed scheme, Alice shares an arbitrary three particle of an unknown quantum state with four agents referred to as Bob1, Bob2, Bob3 and Bob4 as shown in the steps in Figure 1. Bob4 acts as the controller whilst the remaining three parties act as retrievers of the unknown state. They each have to perform a unitary transformation to their particles to recover the state. The unknown quantum state is expressed as;

$$|\Psi\rangle_{x,y,z} = (a|000\rangle + b|011\rangle + c|101\rangle + d|001\rangle + e|110\rangle + f|010\rangle + g|100\rangle + h|111\rangle)_{xyz}, \quad (1)$$

where x, y and z are three particles in the state $|\Psi\rangle$ and a, b, c, d, e, f, g and h are complex numbers that satisfy the normalization condition

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 + |e|^2 + |f|^2 + |g|^2 + |h|^2 = 1. \quad (2)$$

For sharing an arbitrary three qubit state, Alice first share four 3 particle-GHZ states $|\phi\rangle$ with her four agents as indicated on the first block in Figure 1. Specifically, the three particle-GHZ states used to distribute the unknown quantum state can be described as follows:

$$|\phi\rangle_{i,j,k} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle), \quad (3)$$

where i, j and k represent particles in the state. After sharing the 4 GHZ states, Bob1, Bob2, Bob3 and Bob4 are in possession of particle 3, 6, 9 and 12 respectively whilst Alice retains other particles. She then applies the Controlled-Not (CNOT) gate operation on four particles $y, z, 10$ and 11. In the proposed scheme, y and z acts as control particles whilst 10 and 11 are target particles. The whole system of 15 particles held by Alice and her agents can be written as

$$(CNOT_{y_c,11_t})(CNOT_{z_c,10_t})|\Phi\rangle_{x,y,z,1,2,3,4,5,6,7,8,9,10,11,12} = (CNOT_{y_c,11_t})(CNOT_{z_c,10_t})\big[|\Psi\rangle_{x,y,z} \otimes |\phi\rangle_{1,2,3} \otimes |\phi\rangle_{4,5,6} \otimes |\phi\rangle_{7,8,9} \otimes |\phi\rangle_{10,11,12} \quad (4)$$

where y_c, z_c represents the control particles and $10_t, 11_t$ correspond to the target particles.

Thereafter, Alice carries out three GHZ state measurements on the particles $(x, 1, 2), (y, 4, 5)$ and $(z, 7, 8)$ respectively as illustrated in second block of Figure 1. Alice's measurement results can be described by the three-particle GHZ states which can be generalised as $|\phi\rangle^{jk+} = \frac{1}{\sqrt{2}}(|0jk\rangle + |1\bar{j}\bar{k}\rangle)$, $|\phi\rangle^{jk-} = \frac{1}{\sqrt{2}}(|0jk\rangle - |1\bar{j}\bar{k}\rangle)$ where $j, k \in \{0, 1\}$, $\bar{j} = 1-j$ and $\bar{k} = 1-k$. Without loss of generality, if Alice's measurements results are $|\phi\rangle^{00+}$ which occurs with probability $\frac{1}{8} \times \frac{1}{8} \times \frac{1}{8} = \frac{1}{512}$ then the collapsed state of the remaining particles can be written as

$$\begin{aligned}|\varphi\rangle_{3,6,9,10_{t'},11_{t'},12} &= {}^{+00}_{x,1,2}\langle\phi| \otimes {}^{+00}_{y,4,5}\langle\phi| \otimes {}^{+00}_{x,7,8}\langle\phi|\Phi\rangle_{x,y,z,1,2,3,4,5,6,7,8,9,10_{t'},11_{t'},12} \\ &= \frac{1}{4}(a|000000\rangle + a|000111\rangle + b|011110\rangle + b|011001\rangle + c|101101\rangle + c|101010\rangle \\ &+ d|001010\rangle + d|001101\rangle + e|110100\rangle + e|110011\rangle + f|010100\rangle + f|010011\rangle \\ &+ g|100000\rangle + g|100111\rangle + h|111110\rangle + h|111001\rangle), \end{aligned} \quad (5)$$

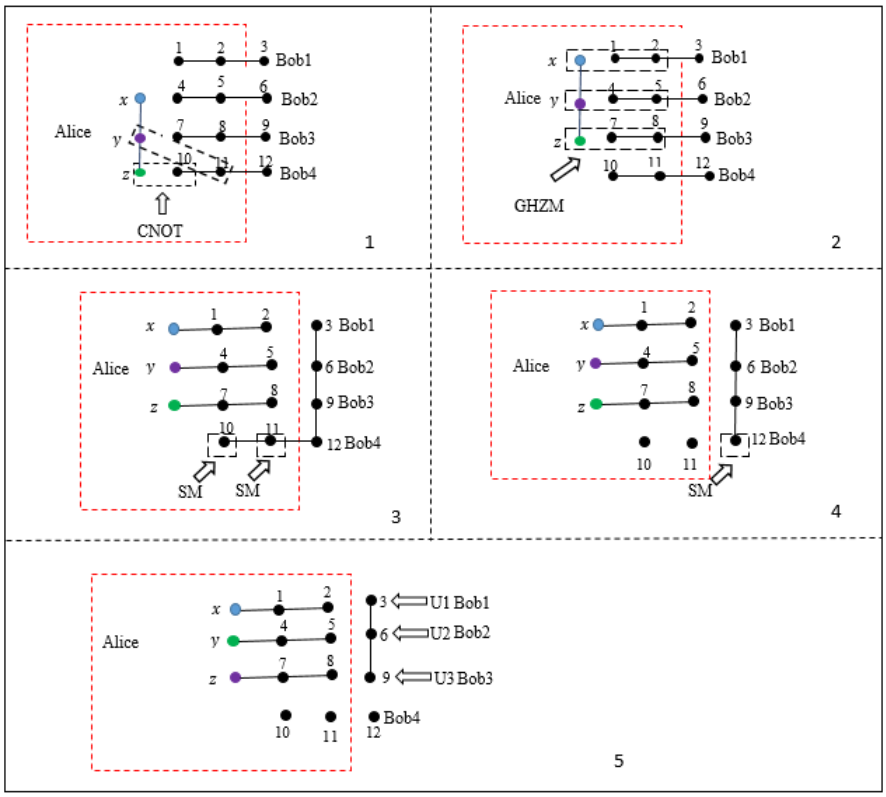

Figure 1. The steps for the proposed five party QSTS of unknown three particle quantum state. In block 1 Alice starts by sharing 4 GHZ states with Bob1, Bob2, Bob3 and Bob4 and then performs a Controlled-Not gate operation (CNOT) on particles $(y, 11)$, $(z, 10)$. In block 2 Alice then carries out GHZ state measurement (GHZM) on particles $(x, 1, 2)$, $(y, 4, 5)$ and $(z, 7, 8)$. In block 3 Alice executes single particle measurements(SM) on particle 10 and 11. In block 4 Bob4 performs a single particle measurement(SM) on particle 12. Finally, in block 5 Bob1, Bob2 and Bob3 perform unitary operations (U1, U2 and U3) on their particles.

where t' represents the state of qubits after CNOT operation. Alice then executes two single measurements on particles 10 and 11 with the basis X $\{|+x\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle), |-x\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle\}$ (ref. block 3 of Figure 1). If she obtains $|+x\rangle$ as her measurement result, then the collapsed state becomes

$$
\begin{aligned}
|\Psi\rangle_{3,6,9,12} &= {}_{10_{t'}}\langle +x|_{11_{t'}}\langle +x|\varphi\rangle_{3,6,9,10_{t'},11_{t'},12} \\
&= \frac{1}{4}(a|0000\rangle + a|0001\rangle + b|0110\rangle + b|0111\rangle + c|1011\rangle + c|1010\rangle + c|0010\rangle + d|0011\rangle \\
&+ e|1100\rangle + e|1101\rangle + f|0100\rangle + f|0101\rangle + g|1000\rangle + g|1001\rangle + h|1110\rangle + h|1111\rangle).
\end{aligned} \tag{6}
$$

Alice reveals her measurement results to her agents via a classical channel. To reconstruct the original state, Bob4 performs a single measurement on the standard basis and publicly informs Bob1, Bob2 and Bob3 about his results as shown in block 4 of Figure 1. Bob1, Bob2 and Bob3 then collaborate to recover the unknown state by performing appropriate unitary transformations on their particles. This is depicted in block 5 of Figure 1. The required unitary operators are $(\sigma_z, \sigma_x, \mathbb{1})$, where $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$, $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$ and $\mathbb{1} = |0\rangle\langle 0| + |1\rangle\langle 1|$.

For instance, if Alice's measurement results are $|\phi\rangle^{00+}_{x,1,2}, |\phi\rangle^{00+}_{y,4,5}, |\phi\rangle^{00+}_{x,7,8}, |-x\rangle_{10}, |+x\rangle_{11}$ and Bob's results are $|1\rangle_{12}$, then the collapsed state can be described as

$$|\Phi\rangle_{3,6,9} = \frac{1}{2\sqrt{2}}(-a|000\rangle + b|011\rangle - c|101\rangle - d|001\rangle + e|110\rangle + f|010\rangle - g|100\rangle + h|111\rangle)_{3,6,9}. \quad (7)$$

To recover the original state then Bob1, Bob2 and Bob3 have to perform the following unitary operations $(\mathbb{1} \otimes \sigma_z\sigma_x \otimes \mathbb{1})|\Phi\rangle_{3,6,9}$, that is, Bob1 and Bob3 have to do nothing on their particle whilst Bob2 has to do the phase flip operation followed by the bit flip on his particle. This can be explicitly shown as;

$$(\mathbb{1} \otimes |0\rangle\langle 1| - |1\rangle\langle 0| \otimes \mathbb{1})(-a|000\rangle + b|011\rangle - c|101\rangle - d|001\rangle + e|110\rangle + f|010\rangle - g|100\rangle + h|111\rangle)_{3,6,9}, \quad (8)$$

which gives,

$$|\Phi\rangle_{3,6,9} = (a|010\rangle + b|101\rangle + c|111\rangle + d|011\rangle + e|100\rangle + f|000\rangle + g|110\rangle + h|101\rangle)_{3,6,9},$$

which is the original state sent by Alice to her agents.

3. QSTS of an Arbitrary m-Particle State with n Agents

Subsequently, this three-particle scheme can be generalised to the case of sharing m-particle state with n agents (as shown in Figure 2). Alice start by sharing n GHZ states with Bob$i$ $(i = 1, \ldots, n)$ and hence the whole system can be written as

$$|\Psi\rangle \equiv \Big(\sum_{i_1,\ldots,i_m=0}^{1} \alpha_{i_1,\ldots,i_m} |i_{1,\ldots,i_m}\rangle_{x_1,x_2,\ldots,x_m} \Big) \otimes |\phi\rangle_{1,2,3} \otimes |\phi\rangle_{4,5,6} \otimes \cdots \otimes |\phi\rangle_{3n-2,3n-1,3n}, \quad (9)$$

where $x_1, x_2, \ldots, x_m$ are the m particles in the unknown state.

Alice then carries out $2(n-m)$ CNOT operations where $x_2, x_3, \ldots, x_m$ acts as control particles and $3(m+1)-2, 3(m+1)-1, 3(m+2)-2, 3(m+2)-1, \ldots, 3n-2, 3n-1$ are target particles. After that, she performs m GHZ state measurements followed by $2(n-m)$ single particle measurements on her particles as illustrated in Figure 2. Consequently, the unknown state is transferred into the particles in the possession of her agents. The controllers then executes $(n-m)$ single particle measurements in the standard basis and publishes their results. The m agents collaborate to recover the unknown state by performing the unitary operations to their particles(see Figure 2).

In our scheme, the quantum channel is set up using the decoy-photon technique to detect eavesdropping as explained in Ref. [5]. In order to check the presence of an adversary in the channel, a fraction of states from a total sequence of GHZ states shared by Alice and her agents is measured in the X and standard (Z) basis to estimate the error rates. If the error rate is above the tolerable limit the protocol is aborted, otherwise pure GHZ states can be obtained through entanglement purification. To prevent the controllers from performing intercept-resend attack, Alice prepares decoy GHZ states and randomly inserts them in a sequence of GHZ states used for secret sharing. The decoy states are measured in the X and Z basis. The results are published by both Alice and agents to estimate error rates and any malicious action by agents will introduce errors in the results. The proportion of the decoy photons is so negligible that the intrinsic efficiency of qubits in our scheme approaches 100% as given by,

$$\eta_q \equiv \frac{q_u}{q_t}, \quad (10)$$

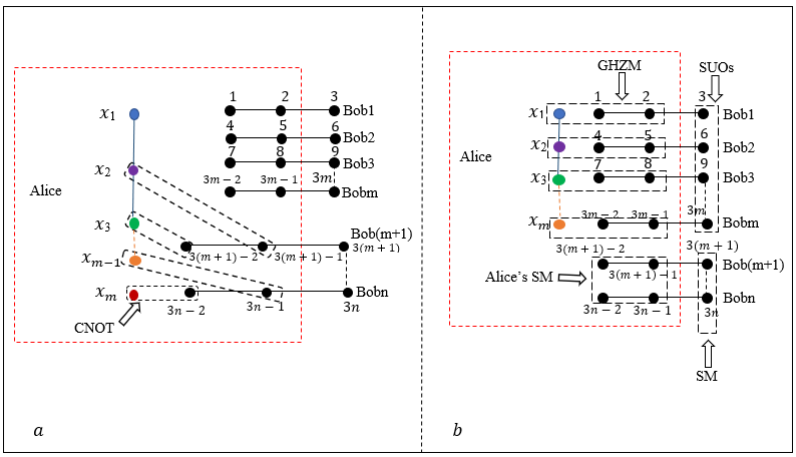

Figure 2. The principles of our proposed QSTS scheme of an arbitrary m-particle state. a) Alice performs $2(n-m)$ CNOT operations where $x_2, x_3, \ldots, x_m$ acts as control particles and $3(m+1)-2, 3(m+1)-1, 3(m+2)-2, 3(m+2)-1, \ldots, 3n-2, 3n-1$ are target particles. b) Alice performs m GHZ state measurements (GHZM) and $2(n-m)$ single particle measurements (SM). Controllers carries out $(n-m)$ single particle measurements and other agents performs single particle unitary operations (SUOs) to recover the unknown state.

where q_u is the number of useful qubits in the QSTS and q_t is the number of transmitted qubits [9]. The total efficiency of QSTS scheme is defined as

$$\eta_t = \frac{q_s}{q_u + b_t}, \tag{11}$$

where q_s is the number of qubits that consists of the quantum information to be shared, q_u is the number of useful qubits in the QSTS and b_t is the number of classical bits transmitted. In our scheme $q_u = 3n$, $q_s = m$ and $b_t = 3n$ which comes from 1 bit for each single particle measurement, of which there are $3(n-m)$, plus 3 bits for each GHZ measurement, of which there are m measurements. Therefore, the total efficiency of our scheme, $\eta_t = m/6n$. This is equivalent to $1/8$ for our five party QSTS where $m = 3$ and $n = 4$. This efficiency is greater than that in the QSTS scheme by Deng et al [7, 10] as depicted in Table 1. Though the schemes in reference [7, 10] uses EPR pairs which are easier to prepare practically as compared to GHZ states in our scheme, they involve a lot operations performed by parties which increase the difficulty of the schemes. For instance, Alice needs to perform 10 joint GHZ states measurements in Ref. [7] which is practically difficult to implement in the present moment. The scheme by Sheng et al in Ref. [6] has better efficiency as compared to our scheme. However, considering the fact that 6 GHZ states are needed to be prepared, our scheme is more convenient in terms of resource consumption as only 4 GHZ states are required.

Moreover, there are other existing schemes which uses non maximally entangled states which are robust against environmental effects as well as easier to implement [11]. However, these schemes are asymmetric, therefore only one agent can retrieve the unknown state as compared to our symmetric scheme in which any of the agents can act as a receiver.

4. Conclusion

In this work we presented a scheme for sharing an unknown three particle state with n agents by using GHZ states. Our scheme shows that three particle state can be reconstructed by agents

Table 1. The comparison between our scheme and the other previous schemes for sharing three particle state and two particle state with five parties. QR-quantum resources, NO-necessary operations, CR-Classical resources, GHZM-GHZ state joint measurement, BM-Bell state measurement, SM- single particle measurement, Single particle unitary operation, η_t-total efficiency.

Schemes	QR	NO	CR	η_t
Sheng et al[6]	6 GHZ States	3 GHZM, 9 SMs and 3SUOs	15 bits	1/6
Deng et al[7]	8 EPR pairs	10 GHZM, 6 SMs and 2 SUOs	10 bits	1/13
Deng et al[10]	5 EPR pairs	5 BMs and 3 SUOs	10 bits	1/10
Our scheme	4 GHZ States	3 GHZM, 3 SMs and 3 SUOs	12 bits	1/8

with 100% probability provided that they act honestly. Our scheme uses less quantum resources as only n-GHZ states are required and has few quantum operations achieving the total efficiency of $\eta_t = m/6n$. Further, we proposed the generalized multiparty quantum state sharing scheme for an arbitrary three particle state. Our proposed schemes indicate a better performance than existing schemes and also uses less resources.

Acknowledgements
The authors would like to acknowledge with thanks the funding from Botswana International University of Science and Technology Research Initiation Grant R00015.

References

[1] Hillery M, Bužek V and Berthiaume A 1999 *Physical Review A* **59** 1829
[2] Cerf N J, Leuchs G and Polzik E S 2007 *Quantum information with continuous variables of atoms and light* (Imperial College Press)
[3] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 *Physical Review Letters* **92** 177903
[4] Shi R H, Huang L S, Yang W and Zhong H 2011 *Quantum Information Processing* **10** 231–239
[5] Xi-Han L, Fu-Guo D and Hong-Yu Z 2007 *Chinese Physics Letters* **24** 1151
[6] Sheng Y B, Deng F G and Zhou H Y 2008 *The European Physical Journal D* **48** 279–284
[7] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Physics Letters A* **354** 190–195
[8] Yuan H, Liu Y M, Zhang W and Zhang Z J 2008 *Journal of Physics B: Atomic, Molecular and Optical Physics* **41** 145506
[9] Cabello A 2000 *Physical Review Letters* **85** 5635
[10] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics* **39** 459–464
[11] Jiang M, Huang X, Zhou L, Zhou Y and Zeng J 2012 *Chinese Science Bulletin* **57** 1089–1094