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 Hadamard basis. One of the agents Bob1 performs 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 multiple agents. The split message is sent to untrusted parties 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 one is based on sharing classical information with the secret distributed among all agents with help of quantum mechanics [2]. The second area deals with the distribution of quantum information with the secret being an arbitrary unknown quantum state [3]. This distribution of quantum state was referred as quantum state sharing (QSTS) by Lance *et. al* in 2004 [4]. QSTS has wide range of applications which include joint sharing of quantum money, quantum error correction and quantum information networks [5]. Various protocols of QSTS have been realized both experimentally and theoretically. These protocols exploit various quantum resources which includes entanglement to distribute an arbitrary single particle, two particle and multiple particle state [6, 7, 8].

To date several entangled states such as Bell states [5, 9] and GHZ states [10] have been featured in QSTS protocols. The first QSS scheme was proposed by Hillery *et. al* which used three and four particle Greenberger-Horne-Zeilinger (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 [11]. 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 [12].

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 Hadamard 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 particle 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. The three particle-GHZ states can be generalized as follows:

$$\begin{aligned}
|\phi^{\pm}\rangle_{1,2} &= 1/2\sqrt{2}(|000\rangle \pm |111\rangle) \\
|\phi^{\pm}\rangle_{3,4} &= 1/2\sqrt{2}(|011\rangle \pm |100\rangle) \\
|\phi^{\pm}\rangle_{5,6} &= 1/2\sqrt{2}(|101\rangle \pm |010\rangle) \\
|\phi^{\pm}\rangle_{7,8} &= 1/2\sqrt{2}(|001\rangle \pm |110\rangle).
\end{aligned} \quad (3)$$

Assuming that all 3 particle-GHZ states prepared by Alice are

$$|\phi^{\pm}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle), \quad (4)$$

then the whole system of 15 particles can be written as

$$\begin{aligned}
|\Phi\rangle_{xyz123456789101112} &= |\psi\rangle_{xyz} \otimes |\phi^{+}\rangle_{123} \otimes |\phi^{+}\rangle_{456} \otimes |\phi^{+}\rangle_{789} \otimes |\phi^{+}\rangle_{101112} \\
&= |\psi\rangle_{xyz}(a|000\rangle + b|011\rangle + c|101\rangle + d|001\rangle + e|110\rangle + f|010\rangle + g|100\rangle \\
&+ h|111\rangle)_{xyz} \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{123} \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{456} \\
&\otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{789} \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{101112}.
\end{aligned} \quad (5)$$

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 CNOT gate

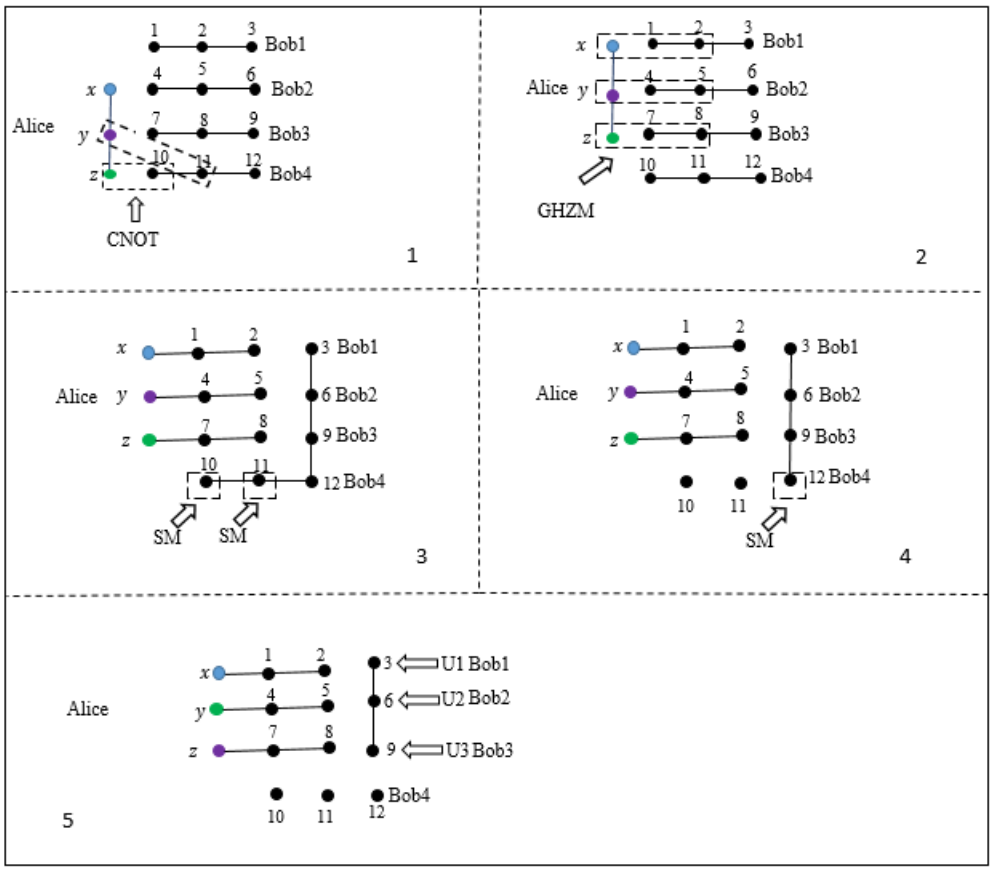

Figure 1. The steps for the proposed five party QSTS of unknown three particle quantum state. In block 1 Alice starts by sharing 4 GHZ states with Bob1, Bob2, Bob3 and Bob4 and then performs a Controlled-Not gate operation (CNOT) on particles $(y, 11)$, $(z, 10)$. In block 2 Alice then carries out GHZ 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.

operation on four particles $x, y, 10$ and 11. In the proposed scheme, x and y acts as control particles whilst 10 and 11 are 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. Without loss of generality, if Alice's measurements results are $|\phi^+\rangle$ then the collapsed state of the remaining particles can be written as

$$\begin{aligned}|\Psi\rangle_{369101112} &= {}_{x12}\langle\phi^+| \otimes {}_{y45}\langle\phi^+| \otimes {}_{x78}\langle\phi|\Psi\rangle_{123456789101112} \\ &= (a|000000\rangle + a|000111\rangle + b|011110\rangle + b|011001\rangle + c|101101\rangle + c|101010\rangle \\ &+ d|001010\rangle + d|001101\rangle + e|110100\rangle + e|110011\rangle + f|010100\rangle + f|010011\rangle \\ &+ g|100000\rangle + g|100111\rangle + h|111110\rangle + h|111001\rangle. \end{aligned} \quad (6)$$

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

$$\begin{aligned}|\Phi\rangle_{36912} &= {}_{10}\langle+x|_{11}\langle+x|\Phi\rangle_{369101112} \\ &= (a|0000\rangle + a|0001\rangle + b|0110\rangle + b|0111\rangle + c|1011\rangle + c|1010\rangle + c|0010\rangle + d|0011\rangle \\ &+ e|1100\rangle + e1101 + f0100 + f0101 + g|1000\rangle + g|1001\rangle + h|1110\rangle + h|1111\rangle. \end{aligned} \quad (7)$$

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 $|\phi^+\rangle_{x12}, |\phi^+\rangle_{y45}, |\phi^+\rangle_{x78}, |-x\rangle_{10}, |+x\rangle_{11}$ and Bob's results are $|1\rangle_{12}$, then the collapsed state can be described as

$$|\Phi\rangle_{369} = (-a|000\rangle + b|011\rangle - c|101\rangle - d|001\rangle + e|110\rangle + f|010\rangle - g|100\rangle + h|111\rangle)_{369}. \quad (8)$$

To recover the original state then Bob1, Bob2 and Bob3 have to perform the following unitary operations $(\mathbb{1} \otimes \sigma_z\sigma_x \otimes \mathbb{1})$, 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;

Bob1's operation:

$$(|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes (-a|000\rangle + b|011\rangle - c|101\rangle - d|001\rangle + e|110\rangle + f|010\rangle - g|100\rangle + h|111\rangle)_{369}$$

This yields;

$$(-a|000\rangle + b|011\rangle - c|101\rangle - d|001\rangle + e|110\rangle + f|010\rangle - g|100\rangle + h|111\rangle)_{369}.$$

Bob2 has to carry out the phase flip and bit flip on his particle,

$$(|0\rangle\langle 1| - |1\rangle\langle 0|) \otimes (-a|000\rangle + b|011\rangle - c|101\rangle - d|001\rangle + e|110\rangle + f|010\rangle - g|100\rangle + h|111\rangle)_{369},$$

which gives,

$$|\Phi\rangle_{369} = (a|010\rangle + b|101\rangle + c|111\rangle + d|011\rangle + e|100\rangle + f|000\rangle + g|110\rangle + h|101\rangle)_{369},$$

which is the original states 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

$$\begin{aligned}|\Psi\rangle \equiv (\sum_{ij\ldots k} \alpha_{\underbrace{ij\ldots k+}_{m}} |\underbrace{ij\ldots k+}_{m}\rangle_{x1x2\ldots xm}) \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{123} \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{456} \otimes \\ \cdots \otimes \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)_{n-2,n-1,n}, \end{aligned} \quad (9)$$

where $i, j, \ldots, k \in \{0, 1\}andx1, x2, \ldots, xm$ are the m particles in the unknown state.

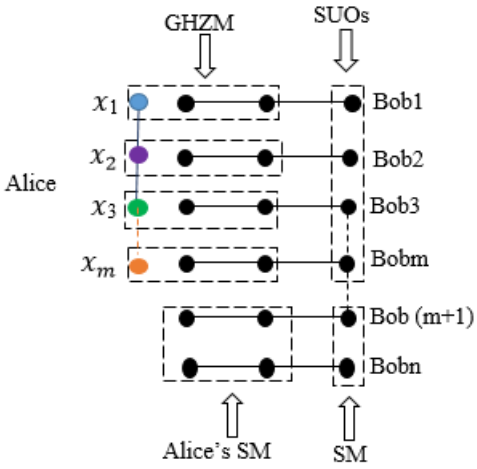

Figure 2. The principles of our proposed QSTS scheme of an arbitrary m-particle state. Alice performs m GHZ state measurements (GHZM) and $2(n-m)$ single particle measurements (SM). Controllers carries out $(n-m)$ single particle measurements and other agents performs single particle unitary operations (SUOs) to recover the unknown state.

Alice then carries out $2(n-m)$ CNOT operations and performs m GHZ state measurements followed by $2(n-m)$ single particle measurements on her particles. 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 [7]. The proportion of the decoy photons is so negligible that the intrinsic efficiency of qubits in our scheme approaches 100% as given by the formula [13];

$$\eta_q \equiv \frac{q_u}{q_t}, \tag{10}$$

where q_u is the number of useful qubits in the QSTS and q_t is the number of transmitted qubits. 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 $q_u = 3n$, $q_s = 3$ and $b_t = 3n$ which gives the total efficiency, η_t, as $1/2n$. This is equivalent to $1/8$ for a five party QSTS. This efficiency greater than that in the QSTS by Deng et al [11, 9] as depicted in Table 1. Though these schemes in reference [11, 9] uses EPR pairs which are easier to prepare practically as compared to GHZ states in our scheme, they involve a lot operations performed by the parties which increases the difficulty of the schemes. For instance, Alice needs to perform 10 joint GHZ states measurements in reference [11] which is practically difficult to implement in the present moment. The scheme by Sheng et al in ref [10] 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 and easier to implement [6]. However, these schemes are asymmetric, therefore only one agent can retrieve the unknown state as compared to our scheme in which any of the agents can act as a receiver. The symmetry created by maximally entangled states allows any of the agents to act as a receiver of the unknown state with the help of other 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[10]	6 GHZ States	3 GHZM, 9 SMs and 3SUOs	15 bits	1/6
Deng et al[11]	8 EPR pairs	10 GHZM, 6 SMs and 2 SUOs	10 bits	1/13
Deng et al[9]	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

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 with 100% probability provided that they act honestly. The security of this scheme against eavesdropping can be accomplished by using the decoy state methods proposed in refs [7]. Our scheme uses less quantum resources as only n-GHZ states are required and has few quantum operations achieving the total efficiency of $\eta_t = 1/2n$. 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 use 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] Sergienko A V 2005 *Quantum communications and cryptography* (CRC Press)
[3] Cerf N J, Leuchs G and Polzik E S 2007 *Quantum information with continuous variables of atoms and light* (Imperial College Press)
[4] Lance A M, Symul T, Bowen W P, Sanders B C and Lam P K 2004 *Physical Review Letters* **92** 177903
[5] Shi R H, Huang L S, Yang W and Zhong H 2011 *Quantum Information Processing* **10** 231–239
[6] Jiang M, Huang X, Zhou L, Zhou Y and Zeng J 2012 *Chinese Science Bulletin* **57** 1089–1094
[7] Xi-Han L, Fu-Guo D and Hong-Yu Z 2007 *Chinese Physics Letters* **24** 1151
[8] Cleve R, Gottesman D and Lo H K 1999 *Physical Review Letters* **83** 648
[9] 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
[10] Sheng Y B, Deng F G and Zhou H Y 2008 *The European Physical Journal D* **48** 279–284
[11] Deng F G, Li X H, Li C Y, Zhou P and Zhou H Y 2006 *Physics Letters A* **354** 190–195
[12] Yuan H, Liu Y M, Zhang W and Zhang Z J 2008 *Journal of Physics B: Atomic, Molecular and Optical Physics* **41** 145506
[13] Cabello A 2000 *Physical Review Letters* **85** 5635