Quantum secret sharing and Mermin operator

Minjin Choi, Yonghae Lee, and Soojoon Lee
Department of Mathematics and Research Institute for Basic Sciences,
Kyung Hee University, Seoul 02447, Korea

(Dated: July 10, 2017)

We present a quantum secret sharing protocol on a given state close to the Greenberger-Horne-Zeilinger state, and use an inequality derived from the Mermin inequality to determine whether players in our protocol securely achieve perfectly correlated classical bits. Therefore, we show that if our inequality holds then the players can securely share a classical secret by our protocol.

Quantum information theory provides us with unconditionally secure communication between two remote parties. However, there are many communication protocols for three or more parties. So, it can be an interesting question to ask whether quantum information theory can make communication for three or more parties such as secret sharing [1, 2] unconditionally secure.

In order to find an unconditionally secure quantum secret sharing (QSS) protocol, we begin with the original QSS protocol proposed by Hillery, Bužek and Berthiaume [3], in which they have dealt with the N-qubit Greenberger-Horne-Zeilinger (GHZ) state [4] $|\Psi_0^+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |2^N - 1\rangle\right)$, and each player measures $|\Psi_0^+\rangle$ in the X basis or the Y basis. If an even number of players measure the state in the Y basis, then they can have a perfect correlation of classical bits to perform secret sharing of classical information. However, since it is difficult for N players to share the state $|\Psi_0^+\rangle$, we need to find out if there is a QSS protocol for N players even though they share a state close to $|\Psi_0^+\rangle$.

Let us suppose that Alice, Bob, and Charlie share a three-qubit state which is close to $|\Psi_0^+\rangle$, and they perform the original QSS protocol on the three-qubit state. Then since Bob or Charlie should not know anything about Alice's information with their own information alone in QSS, the mutual information $I(m_A : m_B)$ and $I(m_A : m_C)$ must be zero, where m_A, m_B, and m_C are the measurement outcomes of Alice, Bob, and Charlie, respectively. But, this does not hold in general. For example,

$$\begin{aligned}\rho_{ABC} \;=\; & p\,|\Psi_0^+\rangle\langle\Psi_0^+| + (1-p)\,|\Psi_1^+\rangle\langle\Psi_1^+| \\ & + \sqrt{p(1-p)}\left(|\Psi_0^+\rangle\langle\Psi_1^+| + |\Psi_1^+\rangle\langle\Psi_0^+|\right), \end{aligned} \tag{1}$$

where $|\Psi_1^+\rangle = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)$. In this case,

$$I(m_A : m_B) = \frac{1}{2} - \frac{1}{2}h\left(\frac{1}{2} + \sqrt{p(1-p)}\right), \tag{2}$$

where $h(\cdot)$ is the binary entropy. Thus we can clearly see that if $p \neq 1$, then the mutual information is not zero.

We note that an arbitrary N-qubit state can be depolarized to the GHZ diagonal state of the form

$$\begin{aligned}\rho_N \;=\; & \lambda_0^+ |\Psi_0^+\rangle\langle\Psi_0^+| + \lambda_0^- |\Psi_0^-\rangle\langle\Psi_0^-| \\ & + \sum_{j=1}^{2^{N-1}-1} \lambda_j \left(|\Psi_j^+\rangle\langle\Psi_j^+| + |\Psi_j^-\rangle\langle\Psi_j^-|\right)\end{aligned} \tag{3}$$

by means of local operations and classical communication (LOCC) [5], where

$$|\Psi_j^\pm\rangle = \frac{1}{\sqrt{2}}\left(|j\rangle \pm |2^N - 1 - j\rangle\right) \tag{4}$$

and $\lambda_0^+ + \lambda_0^- + 2\sum_j \lambda_j = 1$, and that if N players share this state, then they obtain $I(m_i : m_{j_1} \oplus m_{j_2} \oplus \cdots \oplus m_{j_t}) = 0$ for distinct i, j_1, $\cdots$, j_t $(1 \leq t \leq N-2)$, where m_k is the measurement outcome of the kth player. In this paper, we hence suggest that N players change a given state to the GHZ diagonal state in Eq. (3) by using LOCC, and then perform the original QSS protocol on the state.

In addition, we need another process to determine if N players securely achieve perfectly correlated classical bits from measurement outcomes in QSS on the state in Eq. (3). As a tool of such a process, we use an inequality derived from the Mermin inequality [6]. Since N players can estimate all values in our inequality from randomly chosen outcomes of local measurements in QSS, we can show that if our inequality is satisfied then N players can securely carry out QSS.

We now introduce our QSS protocol. To begin with, let us assume that N players share sufficiently many copies of an N-qubit state.

- **Depolarization:** $N \geq 3$ players, A_1, A_2, $\cdots$, A_N, depolarize each of the initial states to the state of the form in Eq. (3) by LOCC.

- **Measurement:** Each player A_i measures his/her particles of the depolarized states in the X or Y basis. Then they publicly announce on which basis they used.

- **Sifting:** A_1, A_2, $\cdots$, A_N discard their measurement results if an odd number of players measured in the Y basis.

- **Security check:** N players randomly choose half of the sifted measurement results. For each of randomly chosen ones, let a_i and b_i be the ith player's measurement outcome, in the cases that the number of players who measured in the Y basis is a multiple of four and is congruent to two modulo four, respectively. Players calculate the averages $\bar{A}$ and $\bar{B}$ of $(-1)^{\sum_i a_i}$ and $(-1)^{\sum_i b_i}$ over the randomly chosen measurement results, respectively. The protocol aborts if $\bar{A} - \bar{B} \leq q$, where $q \in [0.5, 1]$ is the unique solution of the equation $h\left(\frac{1}{2}(1-q)\right) - h(q) = 1$. In fact, $q \approx 0.84865$.

- **Post-processing:** N players securely share perfectly correlated classical bits by applying classical error correction and privacy amplification.

Lemma 1. *If $\bar{A} - \bar{B} > q$, then each legitimate player in our QSS protocol has a strictly positive asymptotic key rate with high probability.*

By Lemma 1, we can conclude that it is possible to achieve secure QSS by exploiting our protocol.

---

[1] G. R. Blakley, Proc. of the National Computer Conf. **48**, 313 (1979).

[2] A. Shamir, Commun. ACM **22**, 612 (1979).

[3] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).

[4] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Bell's Theorem, Quantum Theory, and Conceptions of the Universe ed M Kafatos (Dordrecht: Kluwer) p. 69 (1989).

[5] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).

[6] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).

[7] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).

[8] I. Kogias, Y. Xiang, Q. He, and G. Adesso, Phys. Rev. A **95**, 012315 (2017).

[9] A. S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973).