

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: September 11, 2018)

Quantum secret sharing is well known as a method for players to share a classical secret for secret sharing in quantum mechanical ways. Most of the results associated with quantum secret sharing are based on pure multipartite entangled states. In reality, however, it is difficult for players to share a pure entangled state, although they can share a state close to the state. Thus, it is necessary to study how to perform the quantum secret sharing based on a general multipartite state. We here present a quantum secret sharing protocol on an N -qubit state close to a pure N -qubit Greenberger–Horne–Zeiling state. In our protocol, N players use an inequality derived from the Mermin inequality to check secure correlation of classical key bits for secret sharing. We show that if our inequality holds then every legitimate player can have key bits with positive key rate. Therefore, for sufficiently many copies of the state, the players can securely share a classical secret with high probability by means of our protocol.

PACS numbers: 03.67.Dd

I. INTRODUCTION

Secret sharing [1, 2] is a method for splitting a secret so that a sufficient number of shares are needed in order to reconstruct the secret. As a special type of secret sharing, there is a (k, n) threshold secret sharing scheme, in which a dealer allocates a secret into n players so that no group of fewer than k players can restore the secret, but any group of k or more players can.

We note that secret sharing can be regarded as a type of multi-user key agreement, since we can carry out secret sharing by using key bits obtained from the key agreement. Thus, in order to check the security of a given secret sharing protocol, it is sufficient to verify whether the key agreement can be securely performed. We also note that quantum key distribution (QKD) provides us with unconditionally secure communication between two remote players. More precisely, we can accomplish unconditionally secure key agreement by employing quantum mechanics. Hence, it can be an attractive question to ask whether we can quantumly perform unconditionally secure secret sharing. In fact, Hillery, Bužek, Berthiaume [3] proposed the (n, n) threshold quantum secret sharing (QSS) protocol based on the $(n+1)$ -qubit Greenberger–Horne–Zeiling (GHZ) state [4], and hereafter we call this HBB QSS protocol. Since then, a variety of theoretical results related to the HBB QSS protocol have been presented [5–13], and various experiments on QSS have been conducted [14–18].

In the HBB QSS protocol, a dealer can distribute his/her classical secret, and legitimate players can protect the secret from eavesdropping and dishonest players. The HBB QSS protocol is as follows. Suppose that $N \geq 3$ players share the GHZ state, $|\Psi_0^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |2^N - 1\rangle)$, and each player measures his/her own qubit in the X basis or the Y basis. If the number of players measuring their parts in the Y basis is an even number, then they have a perfect correlation of classical bits to accomplish a secret sharing of classical information:

$$m_1 \oplus m_2 \oplus \cdots \oplus m_N = \begin{cases} 0 & \text{if the number of } Y \text{ is } 4t \text{ for some } t \in \mathbb{Z}, \\ 1 & \text{if the number of } Y \text{ is } 4t + 2 \text{ for some } t \in \mathbb{Z}, \end{cases} \quad (1)$$

where m_j is the measurement outcome of the j th player.

On this account, a secure secret sharing can be obtained by sharing the GHZ state $|\Psi_0^+\rangle$. However, it is difficult for N players to share the pure state $|\Psi_0^+\rangle$, although they can share a state close to $|\Psi_0^+\rangle$ by means of distillation schemes [19, 20]. Hence, it can be an important task to find out if there is a secure QSS protocol when N players share a state close to the state $|\Psi_0^+\rangle$.

As a way to address this issue, we propose an $(N-1, N-1)$ threshold QSS protocol on a given N -qubit state close to the GHZ state. In our QSS protocol, N players measure their qubits in the X basis or the Y basis as in the HBB QSS protocol. However, in some states, this method cannot evenly divide a secret. For instance, if Alice, Bob, and Charlie share the state

$$\tilde{\rho}_{ABC} = \frac{9}{10} |\Psi_0^+\rangle \langle \Psi_0^+| + \frac{1}{10} |\Psi_2^+\rangle \langle \Psi_2^+| + \frac{3}{10} (|\Psi_0^+\rangle \langle \Psi_2^+| + |\Psi_2^+\rangle \langle \Psi_0^+|),$$

where $|\Psi_0^+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ and $|\Psi_2^+\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$, and they perform the HBB QSS protocol on the state $\tilde{\rho}_{ABC}$, then the mutual information $I(m_A : m_B) = 0$, and $I(m_A : m_C) \approx 0.14$. In order to enable a dealer to

evenly distribute his/her secret to other players, our QSS protocol includes the step of depolarizing the initial states to a GHZ diagonal state of the form

$$\rho_N = \lambda_0^+ |\Psi_0^+\rangle \langle \Psi_0^+| + \lambda_0^- |\Psi_0^-\rangle \langle \Psi_0^-| + \sum_{j=1}^{2^{N-1}-1} \lambda_j (|\Psi_j^+\rangle \langle \Psi_j^+| + |\Psi_j^-\rangle \langle \Psi_j^-|) \quad (2)$$

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

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

and $\lambda_0^+ + \lambda_0^- + 2 \sum_j \lambda_j = 1$ [21]. In addition, we apply an inequality derived from the Mermin inequality [22, 23] to our QSS protocol to determine whether N players securely achieve perfectly correlated classical bits from measurement outcomes.

We then show the security of our QSS protocol for two cases. The first case is when all players are trusted, and the second case is when there are dishonest players. Especially in the second case, we deal with the situation where each player can only access his/her qubit system, but dishonest players can communicate with eavesdropper Eve who can handle the environment.

We organize our paper as follows. In Sect. II we introduce our $(N-1, N-1)$ threshold QSS protocol and discuss some issues arising from dishonest players for steps. In Sect. III we provide a security proof of our QSS protocol, and, in Sect. IV we give an example that use the Werner state [24]. Finally, we conclude this paper and present some discussion in Sect. V.

II. QUANTUM SECRET SHARING PROTOCOL

We here introduce our QSS protocol. To begin with, let us assume that $N \geq 3$ players, A_1, A_2, \dots, A_N , share sufficiently many identical N -qubit states, and A_1 is a player who wants to distribute his/her secret to the others.

- **Depolarization:** N players depolarize the initial states to a GHZ diagonal state of the form in Eq. (2) by using LOCC until they share $(4 + \varepsilon)n$ depolarized states. They choose ε with high probability there are both more than $2n$ 0's and more than $2n$ 1's in an arbitrary $(4 + \varepsilon)n$ -bit string in which 0 and 1 randomly appear for each bit.
- **Measurement:** Each player A_i randomly measures his/her qubits of the depolarized states in the X basis or the Y basis.
- **Sifting 1:** A_1 randomly chooses $(2 + \varepsilon')n$ strings of N bits. A_1 selects ε' , which is less than ε , in a similar way to ε . In the strings that A_1 chooses, the other players, A_2, \dots, A_N , publicly announce which basis they used with their measurement outcomes. In this process, A_1 does not release measurement information, and for each string, the others present their measurement information in a different order. Then A_1 discards their measurement results if an odd number of players are measured in the Y basis. With high probability, there are at least n strings of N bits. Otherwise, A_1 aborts the protocol.
- **Security check:** A_1 randomly chooses n strings of the sifted measurement results. For $1 \leq i \leq n$ and $1 \leq j \leq N$, let $m_{i,j}$ be the j th bit of the i th string, and let $\mathcal{M}_{i,j}$ be the measurement basis, in which $m_{i,j}$ was obtained in Measurement step. A_1 calculates

$$S_n = \sum_{i=1}^n (-1)^{\frac{k_i}{2}} (-1)^{\oplus_{j=1}^N m_{i,j}},$$

where $k_i = |\{j : \mathcal{M}_{i,j} = Y\}|$. A_1 aborts the protocol if $S_n/n \leq q$, where q is a solution of the equation $(1-q)^2 \log(1-q) + (1+q)^2 \log(1+q) + (1-q^2) \log(1-q^2) = 2$ in $[0.5, 1]$. In fact, $q \approx 0.78$.

- **Sifting 2:** For the remaining strings, N players publicly announce which basis they used. They leave only the results when an even number of players measured in the Y basis, and discard the rest. If the number of the sifted strings is greater than or equal to n , then N players randomly choose n strings among them, and otherwise, they abort the protocol.
- **Post-processing:** N players apply classical error correction and privacy amplification to the remnant [25].

Our QSS protocol can be properly performed if there is no dishonest player. However, there may be dishonest players in secret sharing schemes, so we should take account of the situations that may arise from dishonest players. We here discuss some issues arising from dishonest players for each step in our QSS protocol.

A. Depolarization

We first consider a case that N players share a state close to $|\Psi_0^+\rangle$, but not $|\Psi_0^+\rangle$, and perform the HBB QSS protocol on the state. As mentioned earlier, fewer than $N - 1$ players should have no information about the key in secret sharing. However, this does not generally hold in this case. For example, suppose that Alice, Bob, and Charlie share the state

$$\begin{aligned} \tilde{\rho}_{ABC} = & p|\Psi_0^+\rangle\langle\Psi_0^+| + (1-p)|\Psi_2^+\rangle\langle\Psi_2^+| \\ & + \sqrt{p(1-p)}(|\Psi_0^+\rangle\langle\Psi_2^+| + |\Psi_2^+\rangle\langle\Psi_0^+|), \end{aligned} \quad (3)$$

where $|\Psi_0^+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, $|\Psi_2^+\rangle = \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)$, and $0 \leq p \leq 1$, and they carry out the HBB QSS protocol on the state $\tilde{\rho}_{ABC}$. Then since Bob or Charlie should not know anything about Alice's information with their own information alone in secret sharing schemes, 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. However, in this case, if Alice and Charlie measure their qubits in the same basis, $I(m_A : m_C) = 1 - h\left(\frac{1}{2} + \sqrt{p(1-p)}\right)$, where $h(\cdot)$ is the binary entropy, that is, $h(x) \equiv -x \log x - (1-x) \log(1-x)$, and in another case $I(m_A : m_C) = 0$. Hence, on average,

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

and we can clearly see that if $p \neq 0$ or $p \neq 1$, then the mutual information is not zero.

One way to work out this problem is that N players execute the Depolarization step. We remark that an arbitrary N -qubit state can be depolarized to the GHZ diagonal state of the form in Eq. (2) by means of LOCC, and that if N players share this state and perform the HBB QSS protocol on 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, \dots, j_t ($1 \leq t \leq N-2$). Hence, this step helps them to equally divide the secret.

However, if there are dishonest players, then N players may not be able to share the depolarized state of the form in Eq. (2) after the Depolarization step. We note that all players do not know what the initial state is, so it is difficult for dishonest players to determine whether the state is useful to them. In some cases, dishonest players may be penalized if they do not follow this step. For instance, assume that Bob is an dishonest player in the example in Eq. (3), and that he is able to communicate with Eve who can handle the environment. In this case, the Holevo quantity $\chi(m_A : m_B E)$, which is an upper bound on the Bob and Eve's accessible information, is zero. Hence Bob cannot obtain Alice's information by using his own information even if he can communicate with Eve, but honest Charlie can gain the information.

To sum up, the ignorance of the initial state makes it hard for dishonest players to predict the case that they do not follow the Depolarization step, so it is difficult for them to establish a strategy for getting more information. In addition, if dishonest players do not carry out this step, they can have disadvantages for some situations such as the example above. Dishonest players may be reluctant to encounter such situations. Therefore, we may assume that dishonest players follow this step.

B. Measurement

In Measurement step, N players randomly measure their qubits in the X basis or the Y basis. Then, by using their measurement outcomes, they can determine if they can obtain a secret key. If they pass the Security check step, then they can have a secret key for secret sharing, which will be shown in Sect. III. The problem here is that if there are dishonest players, then they may measure their qubits in other bases, not in the X basis or the Y basis. Dishonest players may not even measure their qubits in this step. However, it is difficult for them to determine whether these methods are meaningful since they have no knowledge of what state they share. Rather, it can be a good choice for them to follow this step. We will discuss this in detail in Sects. II C and II E.

C. Sifting 1

Let us first consider the following example. Suppose that Alice, Bob, and Charlie share sufficiently many identical depolarized states of the form in Eq. (2), and that they randomly measure their qubits in the X basis or the Y basis. Then, as in the HBB QSS protocol, they reveal the basis information and leave only the measurement outcomes which an even number of players measured in the Y basis. If they share some of measurement outcomes, then they can asymptotically estimate the value of $\lambda_0^+ - \lambda_0^-$, which will be shown in Sect. IID. We note that

$$\begin{aligned} |\Psi\rangle_{\text{ABCE}} &= \sqrt{\lambda_0^+} |\Psi_0^+\rangle |e_0^+\rangle + \sqrt{\lambda_0^-} |\Psi_0^-\rangle |e_0^-\rangle \\ &\quad + \sum_{j=1}^3 \sqrt{\lambda_j} (|\Psi_j^+\rangle |e_j^+\rangle + |\Psi_j^-\rangle |e_j^-\rangle) \end{aligned}$$

is a purification of the depolarized state, where $\{|e_0^+\rangle, |e_0^-\rangle, \dots, |e_3^+\rangle, |e_3^-\rangle\}$ is an orthonormal basis in the support of ρ_E . If Eve measures her parts in the basis and Bob communicates with Eve, then Bob and Eve can be perfectly aware of the value of $m_A \oplus m_C$ even if Alice and Charlie do not reveal their measurement outcomes. It means that Bob can estimate the value of $\lambda_0^+ - \lambda_0^-$ without Alice and Charlie, and that if Bob fabricates his measurement outcomes, then Alice and Charlie can make a false judgment even though the state is not close to $|\Psi_0^+\rangle$. This attack is meaningful to dishonest Bob since Eve can measure her system after players decide which measurement outcomes they will use as a secret key. Hence, even if $\lambda_0^+ - \lambda_0^-$ is not close to 1, Bob can manipulate his measurement outcomes so that players can share a key and then can have more dealer's information.

To handle this problem, our QSS protocol includes two Sifting steps. In the Sifting 1 step, A_1 does not announce his/her measurement information, so dishonest players do not know which strings A_1 will discard. This makes it difficult for dishonest players to obtain information about the depolarized state shared by N players, and all they can do is to manipulate the measurement outcomes.

If dishonest players manipulate the measurement outcomes in this step, what is its purpose? Dishonest players may want N players to pass the Security check step even if N players share a state that cannot pass the Security check step. However, it is hard for dishonest players to deceive other players by their intention. In the Sifting 1 step, if dishonest players release their basis information and measurement outcomes before other players, they do not know other player's basis information. Then they should guess which outcomes will satisfy the condition Eq. (1) in order to deceive other players, but it is nearly impossible. The following example helps us to understand this. Let us assume that Alice and Charlie randomly measure their qubits both in the X basis or both in the Y basis on a GHZ diagonal state of the form in Eq. (2) when $N = 3$, and that Bob does not know whether they measured in the X basis or they measured in the Y basis. Then, for any Bob's measurement, the Holevo quantity $\chi(m_A \oplus m_C : m_B E)$ is upper bounded by $\lambda_0^+ + \lambda_0^- + 2\lambda_2$, and so whether or not Bob can deceive other players depends on the shared state. However, since Bob has no knowledge of the shared state, it is impossible to exactly judge whether manipulating his measurement outcomes is useful to him.

In short, since dishonest players do not know which state they share, they cannot always make a correct decision on whether it is useful for them to measure their qubits in other bases or fabricate measurement outcomes in the Sifting 1 step. These methods may rather interfere with key generation, which is not the case that dishonest players want, since their aim is to gain the dealer's information with their own information after sharing a key. Therefore, we may assume that dishonest players follow our QSS protocol up to this step.

D. Security check

The dealer A_1 needs a method to determine whether N players can perform a secure QSS. To this end, we apply the Mermin operator in our QSS protocol because the Mermin operator can be used to check how close the depolarized state is to the $|\Psi_0^+\rangle$. The following propositions explain this.

Proposition 1. *Let*

$$\mathcal{B}_M = \sum (-1)^{\frac{l}{2}} \mathcal{P}_1 \otimes \dots \otimes \mathcal{P}_N$$

be the Mermin operator [22, 23] where $\mathcal{P}_i \in \{X, Y\}$ and the sum is over all operators such that $l \equiv |\{i : \mathcal{P}_i = Y\}|$ is even. Then

$$\lim_{n \rightarrow \infty} \frac{1}{n} S_n = \frac{1}{2^{N-1}} \text{tr}(\rho_N \mathcal{B}_M),$$

where S_n is the value calculated in the Security check step, and ρ_N is the depolarized state of the form in Eq. (2).

Proof. Let $a_i = (-1)^{\frac{k_i}{2}} (-1)^{\oplus_{j=1}^N m_{i,j}}$. Then $S_n = \sum_{i=1}^n a_i$. It can be shown that if the i th chosen string satisfies the condition Eq. (1), then $a_i = 1$ and otherwise, $a_i = -1$, and that

$$\text{Prob}\{a_i = \pm 1\} = \lambda_0^\pm + \sum_{j=1}^{2^{N-1}-1} \lambda_j$$

on the state ρ_N . Since $(+1)\text{Prob}\{a_i = 1\} + (-1)\text{Prob}\{a_i = -1\} = \lambda_0^+ - \lambda_0^-$ and $\lambda_0^+ - \lambda_0^- = \frac{1}{2^{N-1}} \text{tr}(\rho_N \mathcal{B}_M)$, the law of large numbers completes the proof. \square

In addition, since A_1 randomly chooses strings to calculate the value of S_n in the Sifting 1 step, S_n satisfies the following proposition.

Proposition 2. *Let \tilde{S}_n be the value calculated in the same way as S_n , using the sifted measurement outcomes in the Sifting 2 step. Then for any $\delta > 0$, the probability $\text{Prob}\{S_n > (1 - 2\delta)n \text{ and } \tilde{S}_n < (1 - 2\delta - \epsilon)n\}$ is asymptotically less than $\exp(-O(\epsilon^2 n))$.*

Proof. Let ξ and $\tilde{\xi}$ be the number of strings which do not satisfy the condition Eq. (1) among the chosen strings in the Security check step and among the sifted strings in the Sifting 2 step, respectively. Then it follows from the random sampling tests [25] that for $\delta > 0$, the probability $\text{Prob}\{\xi < \delta n \text{ and } \tilde{\xi} > (\delta + \epsilon)n\}$ is asymptotically less than $\exp(-O(\epsilon^2 n))$. Since $S_n = n - 2\xi$ and $\tilde{S}_n = n - 2\tilde{\xi}$, we can obtain $\text{Prob}\{\xi < \delta n \text{ and } \tilde{\xi} > (\delta + \epsilon)n\} = \text{Prob}\{S_n > (1 - 2\delta)n \text{ and } \tilde{S}_n < (1 - 2\delta - \epsilon)n\}$. \square

Proposition 2 means that for sufficiently large n , if $S_n/n > q$ in the Security check step, then $\tilde{S}_n/n > q$ with high probability. Here, q is the value used to determine whether the asymptotic key rate is positive, as we will precisely see in Sect. III. Therefore, after the Security check step, A_1 can decide if N players can have a secret key for secret sharing.

E. Sifting 2

In our QSS protocol, dishonest players may measure the parts not used in the Security check step in the Sifting 2 step, not in Measurement step. Thus they can differently measure their qubits in this step. However, since they do not have any information about the state which N players share, it is hard for them to determine whether this method is helpful to them. Indeed, in some states, it can be beneficial to dishonest players for them to measure in the X basis or the Y basis. For instance, let us assume that Alice, Bob, and Charlie share the depolarized state

$$\bar{\rho}_{ABC} = p |\Psi_0^+\rangle \langle \Psi_0^+| + \frac{1}{2}(1-p) (|\Psi_1^+\rangle \langle \Psi_1^+| + |\Psi_1^-\rangle \langle \Psi_1^-|),$$

where $|\Psi_0^+\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, $|\Psi_1^\pm\rangle = \frac{1}{\sqrt{2}}(|001\rangle \pm |110\rangle)$, and $0 \leq p \leq 1$, and Bob is a dishonest player who measures his qubits in an orthonormal basis $\{\mu|0\rangle + \nu|1\rangle, \nu^*|0\rangle - \mu^*|1\rangle\}$ with $|\mu|^2 + |\nu|^2 = 1$. Then if Alice measures her qubits in the X basis or the Y basis, the Holevo quantity $\chi(m_A : m_B E)$ is written as

$$\begin{aligned} \chi(m_A : m_B E) &= S(\rho_{m_B E}) - \frac{1}{2} (S(\rho_{m_B E|m_A=0}) + S(\rho_{m_B E|m_A=1})) \\ &= H\left(\frac{1}{2}p, \frac{1}{2}p, \frac{1}{2}(1-p)|\mu|^2, \frac{1}{2}(1-p)|\mu|^2, \frac{1}{2}(1-p)|\nu|^2, \frac{1}{2}(1-p)|\nu|^2\right) \\ &\quad - H\left(\frac{1}{4}(1+\sqrt{T}), \frac{1}{4}(1+\sqrt{T}), \frac{1}{4}(1-\sqrt{T}), \frac{1}{4}(1-\sqrt{T})\right) \\ &= -p \log p - (1-p)|\mu|^2 \log(1-p)|\mu|^2 \\ &\quad - (1-p)|\nu|^2 \log(1-p)|\nu|^2 - h\left(\frac{1}{2}(1+\sqrt{T})\right), \end{aligned}$$

where H is the Shannon entropy and $T = 1 - 4(1-p)(p + (1-3p)|\mu|^2|\nu|^2)$, and it can be shown that if Bob measures his qubits in the X basis or the Y basis, then the Holevo quantity $\chi(m_A : m_B E)$ becomes the maximum. For these

reasons, we can assume that dishonest players measure their qubits in the X basis or the Y basis, and in this situation, they have no reason not to measure their qubits in Measurement step.

Dishonest players may not even follow the Sifting 2 step. This can interfere with the generation of correlated key bits, but dishonest players do not get more dealer's information. Hence, if it is not their intent to prevent key generation, they should perform this step well.

F. Post-processing

In order to obtain a secret key in the Post-processing step, all players must cooperate, and dishonest players can disturb this step. However, this behavior does not allow dishonest players to get more information, and they can only prevent key generation. Dishonest players may not want to interfere with sharing a key, so we can expect them to execute this step well.

III. SECURITY PROOF

In this section, we show that players can have a secret key for secret sharing by means of our protocol. For every legitimate player's key bits, it is known that the asymptotic key rate K is lower bounded by the Devetak–Winter key rate K_{DW} [12, 26]. Hence, the security can be verified by examining whether K_{DW} is positive.

There are two cases that we should consider in order to check the security in secret sharing schemes. The first case is that all players are trusted, and in this case, the Devetak–Winter key rate K_{DW} becomes

$$K_{\text{DW}} = I(m_1 : m_2 \oplus \dots \oplus m_N) - \chi(m_1 : E).$$

The other is that dishonest players exist. If A_2, \dots, A_{k+1} ($1 \leq k \leq N-2$) are k dishonest players, then the Devetak–Winter key rate K_{DW} can be written as

$$K_{\text{DW}} = I(m_1 : m_2 \oplus \dots \oplus m_N) - \chi(m_1 : m_2 \dots m_{k+1} E).$$

As mentioned earlier, we assume that dishonest players follow our QSS protocol, and under this assumption, we can calculate the mutual information $I(m_1 : m_2 \oplus \dots \oplus m_N)$.

Lemma 3. *Let m_l ($1 \leq l \leq N$) be the measurement outcomes of l th player in our QSS protocol. Then*

$$I(m_1 : m_2 \oplus \dots \oplus m_N) = 1 - h\left(\frac{1}{2}(1 - (\lambda_0^+ - \lambda_0^-))\right). \quad (4)$$

Proof. Let ρ_N be the depolarized state that N players share in the Depolarization step. Then we obtain

$$\begin{aligned} \rho_{A_1} &= \frac{1}{2} I_{A_1}, \\ \rho_{A_2 \dots A_N} &= \frac{1}{2} (\lambda_0^+ + \lambda_0^-) (|0\rangle\langle 0| + |2^{N-1} - 1\rangle\langle 2^{N-1} - 1|) \\ &\quad + \sum_{j=1}^{2^{N-1}-1} \lambda_j (|j\rangle\langle j| + |2^{N-1} - 1 - j\rangle\langle 2^{N-1} - 1 - j|). \end{aligned}$$

Thus

$$\begin{aligned} H(m_1) &= H(m_2 \oplus \dots \oplus m_N) = h\left(\frac{1}{2}\right), \\ H(m_1, m_2 \oplus \dots \oplus m_N) &= H\left(\frac{1}{2}\tilde{p}, \frac{1}{2}\tilde{p}, \frac{1}{2}(1 - \tilde{p}), \frac{1}{2}(1 - \tilde{p})\right), \end{aligned}$$

where H is the Shannon entropy and $\tilde{p} = \lambda_0^+ + \sum_{j=1}^{2^{N-1}-1} \lambda_j$. Hence,

$$\begin{aligned} I(m_1 : m_2 \oplus \dots \oplus m_N) &= H(m_1) + H(m_2 \oplus \dots \oplus m_N) - H(m_1, m_2 \oplus \dots \oplus m_N) \\ &= 1 - h\left(\frac{1}{2}(1 - (\lambda_0^+ - \lambda_0^-))\right). \end{aligned}$$

□

A. Case 1: all players are trusted

We here consider the case that all players are trusted. In order to calculate the Holevo quantity $\chi(m_1 : E)$, we first think about the purification of ρ_N :

$$\begin{aligned} |\Psi\rangle_{A_1 A_2 \dots A_N E} &= \sqrt{\lambda_0^+} |\Psi_0^+\rangle |e_0^+\rangle + \sqrt{\lambda_0^-} |\Psi_0^-\rangle |e_0^-\rangle \\ &\quad + \sum_{j=1}^{2^{N-1}-1} \sqrt{\lambda_j} (|\Psi_j^+\rangle |e_j^+\rangle + |\Psi_j^-\rangle |e_j^-\rangle), \end{aligned}$$

where $\langle e_i^a | e_j^b \rangle = \delta_{ij} \delta_{ab}$. Calculating ρ_E and $\rho_{A_1 E}$, we have

$$\begin{aligned} \chi(m_1 : E) &= S(\rho_E) - \frac{1}{2} (S(\rho_{E|m_1=0}) + S(\rho_{E|m_1=1})) \\ &= -\lambda_0^+ \log \lambda_0^+ - \lambda_0^- \log \lambda_0^- - 2 \sum_{i=1}^{2^{N-1}-1} \lambda_i \log \lambda_i \\ &\quad + (\lambda_0^+ + \lambda_{2^{N-1}-1}) \log(\lambda_0^+ + \lambda_{2^{N-1}-1}) \\ &\quad + (\lambda_0^- + \lambda_{2^{N-1}-1}) \log(\lambda_0^- + \lambda_{2^{N-1}-1}) \\ &\quad + 2 \sum_{i=1}^{2^{N-2}-1} (\lambda_i + \lambda_{t_i}) \log(\lambda_i + \lambda_{t_i}), \end{aligned} \tag{5}$$

where $t_i = 2^{N-1} - 1 - i$. Since N players do not estimate the values of λ_0^+ , λ_0^- , and λ_j ($1 \leq j \leq 2^{N-1} - 1$) in our QSS protocol, they cannot calculate the Holevo quantity $\chi(m_1 : E)$ in Eq. (5). We hence find an upper bound of the Holevo quantity $\chi(m_1 : E)$, which can be calculated by $\lambda_0^+ - \lambda_0^-$.

Lemma 4. Let $p \equiv \lambda_0^+ - \lambda_0^-$ and $\chi(m_1 : E)$ be the Holevo quantity in Eq. (5). If $p > q$ then

$$\chi(m_1 : E) \leq -\alpha^2 \log \alpha^2 - \beta^2 \log \beta^2 - 2\alpha\beta \log \alpha\beta - h(\alpha), \tag{6}$$

where $\alpha = \frac{1}{2}(1-p)$ and $\beta = \frac{1}{2}(1+p)$.

Proof. By concavity of $f(x) \equiv -x \log x$,

$$-\lambda_i \log \lambda_i - \lambda_{t_i} \log \lambda_{t_i} + (\lambda_i + \lambda_{t_i}) \log(\lambda_i + \lambda_{t_i}) \leq \lambda_i + \lambda_{t_i}$$

for $1 \leq i \leq 2^{N-2} - 1$. Thus the Holevo quantity $\chi(m_1 : E)$ is upper bounded by

$$\begin{aligned} &-\lambda_0^+ \log \lambda_0^+ - \lambda_0^- \log \lambda_0^- - 2\lambda_{2^{N-1}-1} \log \lambda_{2^{N-1}-1} \\ &\quad + (\lambda_0^+ + \lambda_{2^{N-1}-1}) \log(\lambda_0^+ + \lambda_{2^{N-1}-1}) + (\lambda_0^- + \lambda_{2^{N-1}-1}) \log(\lambda_0^- + \lambda_{2^{N-1}-1}) \\ &\quad + 1 - (\lambda_0^+ + \lambda_0^- + 2\lambda_{2^{N-1}-1}). \end{aligned}$$

Let $C \equiv \{(x, y) : x \geq 0, y \geq 0, x + y \leq \frac{1}{2}(1-p)\}$. Define $\tau(x, y)$ on C by

$$\begin{aligned} \tau(x, y) &\equiv -(p+x) \log(p+x) - x \log x - 2y \log y \\ &\quad + (p+x+y) \log(p+x+y) + (x+y) \log(x+y) \\ &\quad + (1-p) - 2(x+y). \end{aligned}$$

Then τ is continuous on the compact set C and hence τ has a maximum value in C . Since

$$\begin{aligned} \frac{\partial}{\partial x} \tau(x, y) &= \log \frac{(x+y)(p+x+y)}{4x(p+x)} \\ \frac{\partial}{\partial y} \tau(x, y) &= \log \frac{(x+y)(p+x+y)}{4y^2}, \end{aligned}$$

there is no critical point in the interior of C , and hence τ has the maximum on the boundary of C . From simple calculations, we can see that if $p > q$ then $\tau(x, y)$ has its maximum value

$$-\alpha^2 \log \alpha^2 - \beta^2 \log \beta^2 - 2\alpha\beta \log \alpha\beta - h(\alpha)$$

at $(\alpha^2, -\alpha^2 + \alpha)$ on the boundary of C . Therefore, if $p > q$ then

$$\chi(m_1 : E) \leq -\alpha^2 \log \alpha^2 - \beta^2 \log \beta^2 - 2\alpha\beta \log \alpha\beta - h(\alpha).$$

□

Combining Eqs. (4) and (6), if $p > q$ then we obtain a lower bound of K_{DW} :

$$K_{\text{DW}} \geq 1 + \alpha^2 \log \alpha^2 + \beta^2 \log \beta^2 + 2\alpha\beta \log \alpha\beta. \quad (7)$$

Let $\tilde{\tau}(p) \equiv 1 + \alpha^2 \log \alpha^2 + \beta^2 \log \beta^2 + 2\alpha\beta \log \alpha\beta$ be the right-hand side in Eq. (7). Then $\tilde{\tau}$ is a strictly increasing function on $[0.5, 1]$ and $\tilde{\tau}(q) = 0$. Thus $K_{\text{DW}} \geq \tilde{\tau}(p) > \tilde{\tau}(q) = 0$ if $p > q$.

We note that Proposition 1 means $p \approx S_n/n$ for sufficiently large n . In addition, Proposition 2 implies that for sufficiently large n , if $S_n/n > q$ then $\tilde{S}_n/n > q$ with high probability. Therefore, in this case, if N players pass the Security check step, they can have a secret key for secret sharing with positive key rate in asymptotic case by means of our QSS protocol.

B. Case 2: there are dishonest players

In this subsection, the case that there are dishonest players is taken into consideration. As in Sect. III A, we find an upper bound of $\chi(m_1 : m_2 \cdots m_{k+1} E)$, which can be represented by $\lambda_0^+ - \lambda_0^-$.

Lemma 5. *Let $p \equiv \lambda_0^+ - \lambda_0^-$. If $p > q$ then*

$$\chi(m_1 : m_2 \cdots m_{k+1} E) \leq -\alpha^2 \log \alpha^2 - \beta^2 \log \beta^2 - 2\alpha\beta \log \alpha\beta - h(\alpha),$$

where $\alpha = \frac{1}{2}(1 - p)$ and $\beta = \frac{1}{2}(1 + p)$.

Proof. For ease of calculation, we rewrite $|\Psi_j^\pm\rangle = \frac{1}{\sqrt{2}}(|j\rangle \pm |2^N - 1 - j\rangle)$ as

$$|\Psi_{t,s}^\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle|t\rangle|s\rangle \pm |1\rangle|2^k - 1 - t\rangle|2^{N-k-1} - 1 - s\rangle),$$

where $0 \leq t \leq 2^k - 1$, $0 \leq s \leq 2^{N-k-1} - 1$. Then ρ_N becomes

$$\begin{aligned} \rho_N &= \lambda_{0,0}^+ |\Psi_{0,0}^+\rangle \langle \Psi_{0,0}^+| + \lambda_{0,0}^- |\Psi_{0,0}^-\rangle \langle \Psi_{0,0}^-| \\ &+ \sum_{(t,s) \neq (0,0)} \lambda_{t,s} (|\Psi_{t,s}^+\rangle \langle \Psi_{t,s}^+| + |\Psi_{t,s}^-\rangle \langle \Psi_{t,s}^-|), \end{aligned}$$

where $\lambda_{0,0}^+ = \lambda_0^+$, $\lambda_{0,0}^- = \lambda_0^-$ and $\lambda_{t,s} = \langle \Psi_{t,s}^+ | \rho_N | \Psi_{t,s}^+ \rangle = \langle \Psi_{t,s}^- | \rho_N | \Psi_{t,s}^- \rangle$ for $(t,s) \neq (0,0)$. Thus the purification of ρ_N can be written as

$$\begin{aligned} |\Psi\rangle_{A_1 A_2 \cdots A_N E} &= \sqrt{\lambda_{0,0}^+} |\Psi_{0,0}^+\rangle |e_{0,0}^+\rangle + \sqrt{\lambda_{0,0}^-} |\Psi_{0,0}^-\rangle |e_{0,0}^-\rangle \\ &+ \sum_{(t,s) \neq (0,0)} \sqrt{\lambda_{t,s}} (|\Psi_{t,s}^+\rangle |e_{t,s}^+\rangle + |\Psi_{t,s}^-\rangle |e_{t,s}^-\rangle), \end{aligned}$$

where $\langle e_{i,x}^a | e_{j,y}^b \rangle = \delta_{ij} \delta_{xy} \delta_{ab}$. From tedious but straightforward calculations, $\chi(m_1 : m_2 \cdots m_{k+1} E)$ becomes

$$\begin{aligned} \chi(m_1 : m_2 \cdots m_{k+1} E) &= -\zeta^+(0) \log \zeta^+(0) - \zeta^-(0) \log \zeta^-(0) \\ &- 2 \sum_{s=1}^{2^{N-k-1}-1} \zeta(s) \log \zeta(s) \\ &+ (\zeta^+(0) + \zeta(2^{N-k-1} - 1)) \log(\zeta^+(0) + \zeta(2^{N-k-1} - 1)) \\ &+ (\zeta^-(0) + \zeta(2^{N-k-1} - 1)) \log(\zeta^-(0) + \zeta(2^{N-k-1} - 1)) \\ &+ 2 \sum_{s=1}^{2^{N-k-2}-1} ((\zeta(s) + \zeta(2^{N-k-1} - 1 - s)) \\ &\cdot \log(\zeta(s) + \zeta(2^{N-k-1} - 1 - s))), \end{aligned}$$

where $\zeta^\pm(0) \equiv \lambda_{0,0}^\pm + \sum_{t=1}^{2^k-1} \lambda_{t,0}$ and $\zeta(s) \equiv \sum_{t=0}^{2^k-1} \lambda_{t,s}$ for $1 \leq s \leq 2^{N-k-1} - 1$. Hence, by concavity of $f(x) \equiv -x \log x$, we can have

$$\begin{aligned} \chi(m_1 : m_2 \cdots m_{k+1} E) \leq & -\zeta^+(0) \log \zeta^+(0) - \zeta^-(0) \log \zeta^-(0) \\ & - 2\zeta(2^{N-k-1} - 1) \log \zeta(2^{N-k-1} - 1) \\ & + (\zeta^+(0) + \zeta(2^{N-k-1} - 1)) \log(\zeta^+(0) + \zeta(2^{N-k-1} - 1)) \\ & + (\zeta^-(0) + \zeta(2^{N-k-1} - 1)) \log(\zeta^-(0) + \zeta(2^{N-k-1} - 1)) \\ & + 1 - (\zeta^+(0) + \zeta^-(0) + 2\zeta(2^{N-k-1} - 1)). \end{aligned}$$

By applying similar logic in Lemma 4, if $p > q$ then we can obtain

$$\chi(m_1 : m_2 \cdots m_{k+1} E) \leq -\alpha^2 \log \alpha^2 - \beta^2 \log \beta^2 - 2\alpha\beta \log \alpha\beta - h(\alpha).$$

□

From Lemmas 3 and 5, if $p > q$ then we can have

$$K_{\text{DW}} \geq 1 + \alpha^2 \log \alpha^2 + \beta^2 \log \beta^2 + 2\alpha\beta \log \alpha\beta. \quad (8)$$

By the same reason as in Sect. III A, it can be shown that N players can gain a secret key for secret sharing by means of our protocol if they pass the Security check step, even if there are dishonest players.

In both cases, violation of our inequality implies that a secret key for secret sharing can be obtained for sufficiently large n with high probability. One note here is that the lower bound of K_{DW} does not depend on the number of trusted players and the number of dishonest players. Therefore, if there is at least one trusted player except for dealer, then the dealer and the trusted players can obtain a secret key by using our QSS protocol in asymptotic case.

IV. EXAMPLE: THE WERNER STATE

Suppose that the depolarized state is the Werner state [24]

$$\hat{\rho}_{A_1 A_2 \cdots A_N} = p |\Psi_0^+\rangle \langle \Psi_0^+| + \frac{(1-p)}{2^N} I_{A_1 A_2 \cdots A_N}.$$

Then the Holevo quantity χ can be represented by p and the number of trusted players, and so the Devetak–Winter key rate K_{DW} becomes

$$\begin{aligned} K_{\text{DW}} = & 1 - h\left(\frac{1-p}{2}\right) - h(T_m) - (1 - T_m) \log(2^m - 1) \\ & + h(T_{m-1}) + (1 - T_{m-1}) \log(2^{m-1} - 1), \end{aligned} \quad (9)$$

where $T_j = (1 + (2^j - 1)p)/2^j$ and m is the number of trusted players ($2 \leq m \leq N$). Hence, K_{DW} depends on the number of trusted players, and we can see that the key rate is a strictly increasing function for m .

As seen in FIG. 1, the Devetak–Winter key rates in this example are all greater than the lower bound calculated in Sect. III. Therefore, in this example, we can easily see that if N players pass the Security check step, they can have a secret key for secret sharing by using our QSS protocol.

V. CONCLUSION

We have introduced an $(N-1, N-1)$ threshold QSS protocol on a state close to the N -qubit GHZ state. The inequality used in our QSS protocol is derived from the Mermin inequality, and by using our inequality, N players in the protocol can check whether distributed key bits have secure correlation for secret sharing. We have found lower bound on its asymptotic key rate and have shown that our QSS protocol is secure in asymptotic case by employing the lower bound.

In a device-independent scenario for QKD, to verify the security of a QKD protocol, two remote players compute the average with respect to the Bell operator by using their local measurement outcomes only. In our protocol, N players can calculate the value of S_n by using their local measurement outcomes only, and can check whether the value of S_n satisfies the inequality derived from the Mermin inequality. Furthermore, it can be shown that if ρ_N is the depolarized

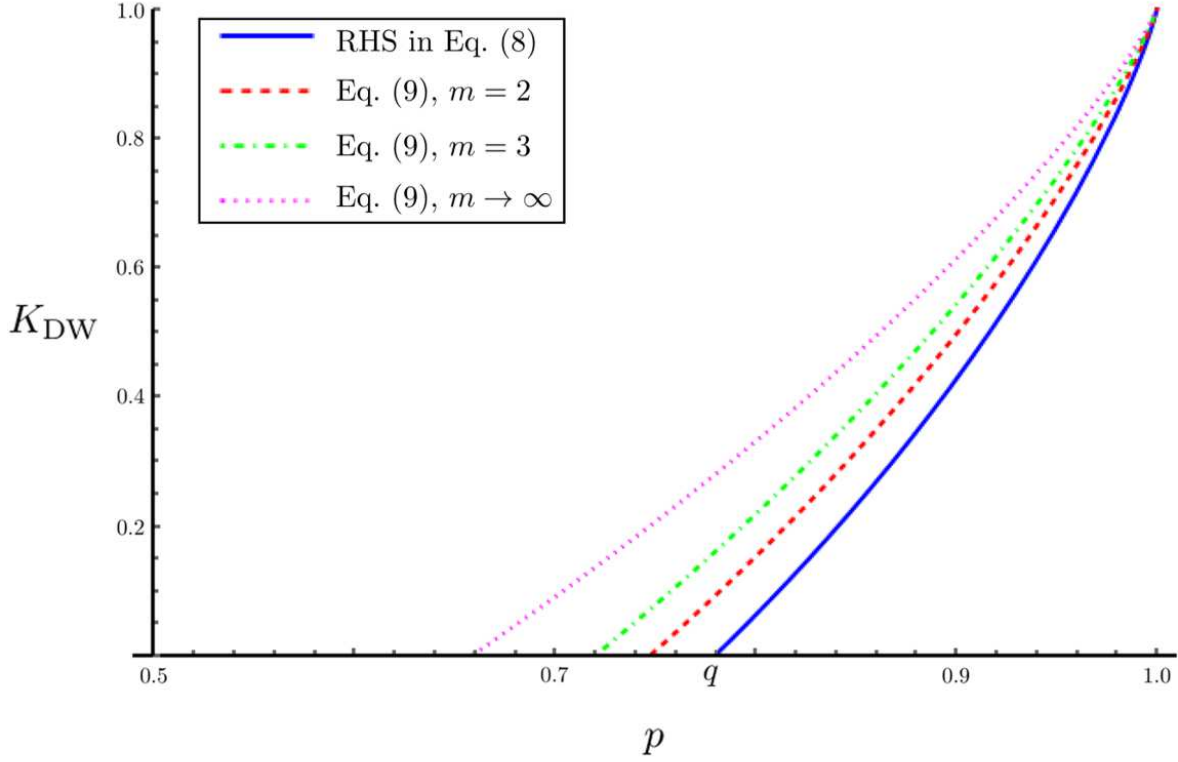


FIG. 1: Our lower bound of the asymptotic key rate (solid line): The lower bound is not dependent on the number of trusted players, so the dealer only checks that the estimated value of p is larger than the constant q in the Security check step of our protocol to confirm that secret sharing can be securely performed. The dashed line and the dash-dotted line represent the Devetak–Winter key rate in Eq. (9) when m , the number of trusted players, is 2 and 3, respectively, if N players share the Werner state. In this example, if the dealer knows m , he/she can properly adjust the value q in our protocol according to m . The dotted line indicates Eq. (9) when m goes to infinity. This implies that there is a limit on the value of p for performing our secure QSS, even though m is large enough.

state of ρ in our protocol then $\Delta \equiv \text{tr}(\rho_N(|\Psi_0^+\rangle\langle\Psi_0^+| - |\Psi_0^-\rangle\langle\Psi_0^-|)) = \text{tr}(\rho(|\Psi_0^+\rangle\langle\Psi_0^+| - |\Psi_0^-\rangle\langle\Psi_0^-|))$, which are the averages with respect to the Mermin operator and $\Delta \approx S_n$ for sufficiently large n . Therefore, for arbitrary N -qubit state ρ , we could obtain a device-independent QSS protocol from our QSS protocol. In addition, since an important theorem related to the device-independent QKD [27], called the entropy accumulation theorem [28], was recently introduced, it can be an interesting topic to find how to apply the theorem to our QSS protocol in order to obtain a device-independent QSS protocol.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (NRF-2016R1A2B4014928).

-
- [1] G. R. Blakley, Proc. Natl. Comput. 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] A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
 - [6] D. Gottesman, Phys. Rev. A **61**, 042311 (2000).

- [7] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, Phys. Rev. A **69**, 052307 (2004).
- [8] Z. jun Zhang and Z. xiao Man, Phys. Rev. A **72**, 022303 (2005).
- [9] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, Phys. Rev. A **76**, 062324 (2007).
- [10] S. Schauer, M. Huber, and B. C. Hiesmayr, Phys. Rev. A **82**, 062311 (2010).
- [11] A. Marin and D. Markham, Phys. Rev. A **88**, 042332 (2013).
- [12] I. Kogias, Y. Xiang, Q. He, and G. Adesso, Phys. Rev. A **95**, 012315 (2017).
- [13] C.-Y. Wei, X.-Q. Cai, B. Liu, T.-Y. Wang, and F. Gao, IEEE Trans. Comput. **67**, 2 (2018).
- [14] W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
- [15] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
- [16] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Phys. Rev. Lett. **95**, 200502 (2005).
- [17] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Phys. Rev. Lett. **98**, 020503 (2007).
- [18] B. A. Bell, D. Markham, D. A. Herrera-Mart, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, Nat. Commun. **5**, 5480 (2014).
- [19] K. Chen and H.-K. Lo, Q. Inf. Comput. **7**, 689 (2007).
- [20] S. Lee and J. Park, Phys. Lett. A **372**, 3157 (2008).
- [21] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).
- [22] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
- [23] A. V. Belinski and D. N. Klyshko, Phys. Usp. **36**, 653 (1993).
- [24] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
- [25] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University, Cambridge, 2000).
- [26] I. Devetak and A. Winter, Proc. R. Soc. A **461**, 207 (2005).
- [27] R. Arnon-Friedman, R. Renner, and T. Vidick, arXiv:1607.01797.
- [28] F. Dupuis, O. Fawzi, and R. Renner, arXiv:1607.01796.