Multiparty quantum data hiding with enhanced security and remote deletion

Xingyao Wu\(^1\) and Jianxin Chen\(^1\)

\(^1\)Joint Center for Quantum Information and Computer Science, University of Maryland, College Park, MD 20742, US

(Dated: April 6, 2018)

One of the applications of quantum technology is to use quantum states and measurements to communicate which offers more reliable security promises. Quantum data hiding, which gives the source party the ability of sharing data among multiple receivers and revealing it at a later time depending on his/her will, is one of the promising information sharing schemes which may address practical security issues. In this work, we propose a novel quantum data hiding protocol. By concatenating different subprotocols which apply to rather symmetric hiding scenarios, we cover a variety of more general hiding scenarios. We provide the general requirements for constructing such protocols and give explicit examples of encoding states for five parties. We also proved the security of the protocol in sense that the achievable information by unauthorized operations asymptotically goes to zero. In addition, due to the capability of the sender to manipulate his/her subsystem, the sender is able to abort the protocol remotely at any time before he/she reveals the information.

I. INTRODUCTION

Information security in the era of quantum information science has changed dramatically [1–3]. With subfields like quantum cryptography [4, 5], quantum teleportation [6–8], quantum network [9], error correction codes [10, 11] etc., protocols for secure classical and quantum information sharing have been developed and, in some cases, implemented. While in the domain of classical steganography, applications have been made widely in covert message sharing [12] and copyright protection [13], one also seeks to bridge these information sharing schemes with quantum information since classical protocols are generally fragile in the sense that they depend on how well the senders keep the decoding strings and the existence of eavesdroppers would potentially undermine the security. Depending on whether the participants are allowed to have quantum communication, protocols are divided into two subcategories, namely quantum secret sharing (QSS) [14, 15] where only local operations and classical communication (LOCC) are allowed and quantum data hiding (QDH) [16, 17] where quantum communication is allowed in certain ways. Experiments have also demonstrated the possibility of sharing secrets quantum systems [15].

In this work, we will be focusing on the part of quantum data hiding applied to multiple parties, i.e., more than two. Different from quantum secret sharing, the receivers in a quantum data hiding protocol are normally assumed to be individually malevolent which means they would do anything they could to decrypt the hidden information before the sender gives them the permission. Previous studies have been made with such two parties [16]. In that work, by utilizing the fact that the four Bell states cannot be distinguished by only LOCC, a classical information bit is securely encrypted in the parity of the number of the singlet states in a series of prepared Bell states. To later reveal the information, the two parties are given access to a shared quantum communication channel which enables them to distinguish the four Bell states easily.

Hiding information among multiple parties with quantum states has also been discussed in [18, 19]. However, these schemes will either require the allowed measurements to be in special forms or have very specific hiding structure considered. More general multipartite cases have been studied in [20], but no example of the encoding states was given and the protocol success probabilistically. On the contrary, in this work, we will present a new multipartite quantum data hiding protocol which is equipped with new features mostly concerned with improvements of security compared to previous protocols [18, 19], but also provides more straightforward measurements.

The security of all the previous quantum data hiding protocols rely on the ability of the receivers to access certain quantum channels. The receivers are able to perform quantum nonlocal operations to reveal the hidden information given the authorization of the sender. We show that this may not be the safest option when hiding quantum data. Instead of relying on the authorization of the sender for the security, the protocol in this work enables the sender to hide the information bits securely even though the receivers maliciously get unauthorized access to quantum channel.

II. THE PROTOCOL

In a multipartite hiding scheme, comparing with the bipartite case, one important aspect we need to consider is how the receivers are collaborating with each other, specifically the grouping style of the receivers under which the information is hidden or revealed. For instance, given a set of receivers \(\{A,B,C,D\}\), a partition of \(\{\{A,B,C\}, \{D\}\}\), where within the subgroups of \(\{A,B,C\}\) or \(\{D\}\) quantum communication is allowed and only classical communication between these two groups is allowed, will have different requirements on the proto-
col compared to a partition of \( \{ \{A, B\}, \{C, D\} \} \). Thus, while considering the hiding protocol under the multipartite case, one also needs to take the hiding structure into account.

In a general setting, suppose a sender, denoted by \( S \), wants to share some bits of classical information to a group of receivers, denoted by \( R \). In the protocol, the sender wants to achieve the hiding and revealing of the bits only by modification (locally) on his/her part of the shared quantum state, while on the other hand, the receivers try their best to decrypt the hidden bits even though the sender has not given permission yet.

Let us use the quantum state \( |\psi^b\rangle \) to represent the hidden bits \( b \in \{0, 1, ..., m - 1\} \) which the sender want to share with the receivers. Unlike some typical protocols of data hiding proposed before \([16–18, 20]\), the sender \( S \) here will still keep part of the system rather than sending states completely to the receivers. It will be shown later in section IV and V that such treatment will actually improve the security in the hiding stage and also give the sender the flexibility to abort the protocol locally. The state on the receivers' side before the sender reveals or aborts will be

\[
\rho_{R_1,R_2,...}^b = \text{Tr}_S[|\psi^b\rangle_S\rho_{S,R_1,R_2,...}],
\]

where \( R_i \) is the \( i \)th receiver.

In the hiding stage, the receivers are not able to guess the correct secret \( b \). The sender can also specify how the receivers may collaborate with each other. For a partition \( P = \{P_1, P_2, ...\} \), where \( P_j \) is the \( j \)th subgroup of the receivers among the set of the receivers \( R \), the sender will impose the restriction that only classical communication could be made across \( P_j \)'s and quantum communication could be made inside each group \( P_j \). The easiest way to realize these constraints is to make all the reduced states of the receivers to be the same, which is

\[
\rho_{R_1,R_2,...}^b = \rho_{R_1,R_2,...}^{b'},
\]

(for \( b \neq b' \)).

This will guarantee that no matter what operation was made inside the group \( P_j \) and classical communication among \( P_j \)'s, the receivers cannot differentiate the encoding states for different \( b \). We will show later in section IV that the security in this hiding stage is unconditionally secure.

The next stage is to reveal the secret. Since the sender still has part of the quantum state, he/she could manipulate the state in a way that will make the receivers able to recover the secret. This is done by making a local measurement on the sender's side. Suppose the positive-operator valued measure (POVM) elements corresponding to the sender's measurement are \( \{M_t\}_t \), the state on the receivers' side after \( S \) made the measurement with outcome \( t = 0, ..., m - 1 \) will be

\[
\sigma_t^b = \frac{\text{Tr}_S[M_t|\psi^b\rangle \langle \psi^b| M_t^t]}{\text{Tr}[M_t|\psi^b\rangle \langle \psi^b| M_t^t]}.
\]

The sender will then inform the receivers classically with the outcome of the measurement, namely \( t \). In this protocol, the sender would like the receivers in each partition \( P_j \) to collaborate nonlocally and receivers among different subgroups collaborate classically to recover the hidden information. To ensure this, we need to choose the encoding states carefully such that they satisfy these requirements. This simply means the states

\[
\text{Tr}_{\cup_{k\neq j} P_k} [\sigma_t^b],
\]

with fixed \( t \) are LOCC indistinguishable. To achieve this goal, we propose the following subprotocol.

**Subprotocol. Suppose there are a set of multipartite states \( \{|\phi_i\rangle\} \), where \(|i| \geq m \), they satisfy a subprotocol if they cannot be perfectly distinguished by LOCC.**

The set of states \( \{|\phi_i\rangle\} \) can also be divided into \( m \) subsets and the states \( \rho_i \) \( (i = 0, ..., m - 1) \), where each of them is the uniform mixture of the states in each subset, also cannot be perfectly distinguished by LOCC.

With the subprotocol defined above, for each subgroup \( P_j \), we can conveniently assign the state in (4) to one of the uniform mixture \( \rho_{b_j} \). Thus, in a subprotocol, the members in the subgroup \( P_j \) are attempting to recover the information \( b_j \) with the allowed measurements. As stated already, only nonlocal measurement will enable each group \( P_j \) to perfectly distinguish the information \( b_j \).

In order to force the receivers among different subgroup \( P_j \) to make classical communication to retrieve the hidden bits, the hidden bits \( b \) could take the form

\[
b = t \oplus b_1 \oplus b_2 \oplus ... \oplus b_n \pmod{m},
\]

where \( n \) is the total number of the subgroups and \( t \) is the outcome of the POVM measurement made by the sender. In each round of the hiding protocol, the sender can decide a series \( \{b_1, b_2, ..., b_n\} \) which encode the hidden bits \( b \), and prepare the encoding state \( |\psi^b\rangle \) with the right subprotocol states \( \rho_{b_j} \). We will give examples of how to construct the subprotocol later in section III.

We have described above the protocol of hiding and revealing classical bits using quantum states. We will also discuss the security in the section IV.

### III. A CASE STUDY: HIDING WITH \( \{\{A, B\}, \{C, D, E\}\} \)

In this section, we will show how could we construct the quantum data hiding protocol as we described above for a specific scenario, which has the receiver partition \( \{\{A, B\}, \{C, D, E\}\} \). Our protocol states that in the hiding stage, even though all the five members \( \{A, B, C, D, E\} \) can make global quantum measurement, they still cannot recover the hidden bit (we will restrict to bit here and the generalization to multiple bits will be discussed at the end of the section). In the revealing stage, on the contrary, the sender will require the
members in each subgroup to collaborate nonlocally to recover the hidden bit. Different stages of the protocol are depicted in Fig. 1.

We will first describe how we choose the states of the subprotocol for the subgroup. Depending on the number of parties in each subgroup, we may have different subprotocols. For the convenience of experimental realization, we prefer that all the receivers will be given a qubit. We will show that, with this restriction, the subprotocol will be of different types for the first and second subgroups. The one we would like to adopt here for the first subgroup \{A, B\} is the four Bell states protocol [16, 17]. Literally speaking, the four Bell states defined as $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, cannot be perfectly distinguished with an infinite number of LOCC "rounds"[17]. Thus, the subprotocol states $\rho_{b_1}$ will be

$$
\rho_{b_1} = \begin{cases} 
\frac{1}{2}(|\Psi^-\rangle \langle \Psi^-| + |\Phi^+\rangle \langle \Phi^+|), & \text{if } b_1 = 0. \\
\frac{1}{2}(|\Psi^+\rangle \langle \Psi^+| + |\Phi^-\rangle \langle \Phi^-|), & \text{if } b_1 = 1.
\end{cases}
$$

On the other hand, for the second group \{C, D, E\}, we will choose the unextendible product bases (UPB) [19, 21] for the subprotocol states. It has been shown in [22] that any set of states make up an UPB are LOCC indistinguishable. Actually, for a subprotocol of more than two parties, we can always define a UPB which involves only qubits and is LOCC indistinguishable [23, 24] and thus could be used for the construction of the subprotocol. A neat and simple example of UPB states with three qubits are

$$\{ |000\rangle, |1\bar{e}\rangle, |e1\bar{e}\rangle, |\bar{e}e1\rangle \},$$

where \{ |e\rangle, |\bar{e}\rangle \}$ \in \mathbb{C}^2$ and the two states are orthogonal to each other but different than \{ |0\rangle, |1\rangle \} [23]. The subprotocol states $\rho_{b_2}$ can now be defined as

$$
\rho_{b_2} = \begin{cases} 
\frac{1}{2}(|000\rangle \langle 000| + |1\bar{e}\rangle \langle 1\bar{e}|), & \text{if } b_2 = 0. \\
\frac{1}{2}(|e1\bar{e}\rangle \langle e1\bar{e}| + |\bar{e}e1\rangle \langle \bar{e}e1|), & \text{if } b_2 = 1.
\end{cases}
$$

With the two subprotocol states ready, we can now write down the form of the encoding states $|\psi^0\rangle$. The state $|\psi^0\rangle$ will be chosen randomly from one of the following states

$$
|\psi^0\rangle = \begin{cases} 
|0\rangle_S |0^{*}\rangle_{AB} |0^\#\rangle_{CDE} + |1\rangle_S |0^{*}\rangle_{AB} |1^\#\rangle_{CDE}, & \\
|0\rangle_S |1^{*}\rangle_{AB} |1^\#\rangle_{CDE} + |1\rangle_S |1^{*}\rangle_{AB} |0^\#\rangle_{CDE},
\end{cases}
$$

where the register of the receivers are labelled by $b_1^*$ and $b_2^*$, and $|0^*\rangle \in \{|\Psi^-\rangle, |\Phi^+\rangle\}$, $|1^*\rangle \in \{|\Psi^+\rangle, |\Phi^-\rangle\}$, $|0^\#\rangle \in \{|000\rangle, |1\bar{e}\rangle\}$ and $|1^\#\rangle \in \{|e1\bar{e}\rangle, |\bar{e}e1\rangle\}$, and moreover, they are all chosen randomly from each set.

Similarly, the state $|\psi^1\rangle$ will be chosen randomly from one of the following states

$$
|\psi^1\rangle = \begin{cases} 
|0\rangle_S |1^{*}\rangle_{AB} |1^\#\rangle_{CDE} + |1\rangle_S |0^{*}\rangle_{AB} |0^\#\rangle_{CDE}, & \\
|0\rangle_S |0^{*}\rangle_{AB} |0^\#\rangle_{CDE} + |1\rangle_S |1^{*}\rangle_{AB} |1^\#\rangle_{CDE},
\end{cases}
$$

where $|b_1^*\rangle$ and $|b_2^*\rangle$ are chosen similarly as that for $|\psi^0\rangle$.

With the states defined above, it can be checked that they satisfy all the requirements we set for a quantum data hiding protocol described in section II, and the corresponding measurement $\{M_i\}$ of the sender will be the projective measurement in the computational basis.

Regarding hiding multiple bits, it has been shown in [16, 17] that the sender can simply encode the bits into multiple parallel blocks of the above protocol. On the other hand, as the formalism of our protocol does not rely on the unique properties of the maximally entangled states as in [16, 17], we do not have to restrict ourselves to qubits case and can go further into the qudit case for each of the parties. Since the UPB states are also available in higher dimensions [25, 26], to find proper states for the multiple bits is not a difficult task.

IV. UPPER BOUND OF THE ATTAINABLE INFORMATION

As suggested by the name of quantum data hiding, the main purpose of the protocol is that the sender can hide data among the receivers and then reveal the data only if the receivers later perform authorized operations. The security issue arises in two main aspects, namely,
how well the protocol can hide the information bits and how much can the sender assure that the receivers are performing authorized operations.

We will first discuss the first aspect which is how well the protocol can hide the bits in the hiding stage. Since we assume the receivers to be malevolent, without loss of generality, we can assume the measurement made by the receivers to be a POVM \( \{N_k\} \). The probability of the receivers to guess the bits as \( i \) given the encoding states as \( |\psi^b_i\rangle \) will be

\[
p(b|k) = \text{Tr} \left[ N_k \text{Tr}_S[|\psi^b_i\rangle_S R_1 ...] N_k^\dagger \right].
\] (11)

With the promise of (2) by the protocol, we know that \( \text{Tr}_S[|\psi^b_i\rangle_S R_1 ...] \) is the same for all the values of \( b \). Thus the above probability will be

\[
p(b|k) = \frac{1}{m}.
\] (12)

Hence, in the hiding stage, the attainable information by performing the POVM \( \{N_k\} \) will be the mutual information

\[
I(B : K) = \log_2 m - \sum_k p(k) H(B|K = k)
\] (13)

\[
= \log_2 m - m \times \frac{1}{m} \times \sum_b p(b|k) \log_2 p(b|k)
\]

\[
= 0,
\]

where \( B \) and \( K \) corresponds to the events represented by the random variable \( b \) and \( k \). We have shown that the information attainable by the receivers is zero in the hiding stage. It should be stressed here that this is quite special compared to previous QDH protocols [16, 18–20], since the attainable information there are all at a finite amount in the hiding stage.

Now, we turn to the discussion about how much can the sender assure that the receivers are performing authorized operations. The idea is the same, which is to show how much information the receivers can attain by unauthorized operations, which will be LOCC operations in this case. Since the two subgroups are only allowed to have classical channel, we can assume the POVM elements for each of the group to be \( \{P_i\}, \{Q_i\} \) and etc. To bound the attainable information Specifically, we want to bound the mutual information

\[
I(B; P, Q, ...) = H(B) - H(B|P, Q, ...)
\]

\[
\leq H(B_1) - H(B_1|P) + H(B_2) - H(B_2|Q) + ... = I(B_1; P) + I(B_2; Q) + ...
\] (14)

The above equation simply tell us that the attainable information about \( b \) is bounded by the sum of the attainable information of the subprotocols. Thus, one only needs to bound the attainable information of each subprotocol. For a good protocol, one always wants to bound this attainable information to zero. Here, we will use the example in section III to show how this is achieved.

In the case of hiding a bit, it involves a two outcome measurement for the subprotocol. Let us take the first subgroup \( \{A, B\} \) as an example. It is shown in [17] that if \( |p(b_1 = 0|0) + p(b_1 = 0|1) - 1| \leq \delta \), the mutual information between \( B_1 \) and \( P \) will be bounded by

\[
I(B_1; P) \leq \delta H(B_1).
\] (15)

Since the two states in the subprotocol is not perfectly distinguishable by LOCC,

\[
|p(b_1 = 0|0) + p(b_1 = 0|1) - 1| < 1.
\] (16)

However, even if the value on the left hand side is smaller than one, it is definitely not going to bound the mutual information to be close to zero. To solve this problem, we consider the case where the subprotocol is composed with \( n \) parallel original subprotocols and the answering bit \( b_1 \) is decided by the sum of the answering bit of each parallel session (modulo 2). In this case, suppose \( p(0|0) + p(0|1) = 1 + p \) for the original subprotocol,

\[
p^{(n)}(0|0) + p^{(n)}(0|1) \leq 2 \sum_{i \text{ even}} (1 + p)^{n-i} p^i {n\choose i} = 1 + p^n.
\] (17)

Since \( p \leq 1 \) for all the subprotocols we chose, it will suffice to bound the attainable information to a desired small amount with large \( n \). Thus, with enough resources, the sender can always make sure that the receivers may not recover the hidden bits with LOCC, which is not the authorized operation.

V. BURN THE MESSAGE

When hiding data in the real world, even though the sender could make his/her best to keep his/her subsystem in the safest place, it is still possible that the eavesdropper could make his/her way somehow to access it and use it for some malicious purposes. A simple example is that he/she could use it to send fake information to the receivers which is not what the sender wished them to see. The good thing of our protocol is that we allow the sender to abort the protocol at any time before the information was revealed. Let us say there is another POVM \( \{K_i\} \) on the sender’s side. Mathematically speaking, we require that the states in the protocol after the measurement will be indistinguishable for all \( b \),

\[
\frac{\text{Tr}_S[K_i |\psi^b_i\rangle \langle \psi^b_i | K_i^\dagger]}{\text{Tr}[K_i |\psi^b_i\rangle \langle \psi^b_i | K_i^\dagger]} = e^{i\theta_{b'}} \frac{\text{Tr}_S[K_i |\psi^{b'}_i\rangle \langle \psi^{b'}_i | K_i^\dagger]}{\text{Tr}[K_i |\psi^{b'}_i\rangle \langle \psi^{b'}_i | K_i^\dagger]},
\] (18)

for \( b \neq b' \) up to a global phase \( e^{i\theta_{b'}} \).

This means, immediately after \( S \) made the measurement, the quantum state shared by all the parties is erased to a state which cannot be used for information sharing anymore. With the example in section III, the corresponding measurement of the sender will just be the measurement \( \{|+\rangle \langle +|, |-\rangle \langle -|\} \).
VI. CONCLUSION

In this work, we presented a novel quantum data hiding protocol. The protocol extends the application scenario to arbitrary multipartite settings. We give the general requirements that the encoding states need to satisfy and illustrate how one could construct such a protocol with a specific example, which involves five parties. Since the states in the example are all pure qubit states, it is reasonable to say that the protocol is realizable with current experimental capabilities. In addition, due to the special construction of the encoding states, we proved that the protocol is promised to be unconditionally safe in the hiding stage, which is not the case for all previous protocols, and the sender can reduce the possibility of the receivers being cheating asymptotically to zero. Moreover, in section V, we show that it is possible for the sender to abort the data hiding protocol anytime before sending out the revealing permission.

As for the outlook for future study, even though the case for higher dimensional system is promised to be existing, we still need to find an explicit construction. Moreover, while we are parallelizing the subprotocol in section III to make the attainable information asymptotic zero, we assumed that the decoding strategy for the receivers cannot be better than measuring each block separately and then combine the results. Even though this is also assumed in previous works [17], we still look forward to a proof without such assumption.

ACKNOWLEDGEMENT

We acknowledge Eric Chitambar, Houghao Fu, Minh Tran and Alexey Gorshkov for helpful discussions. This work was supported by the ARL funded CDQI at the University of Maryland.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Đušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. 81, 1301 (2009).
[2] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. 98, 230501 (2007).
[3] D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, in International Symposium on Information Theory, 2004: ISIT 2004. Proceedings. (2004) pp. 136–.
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
[5] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. 70, 1895 (1993).
[7] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature 390, 575 (1997).
[8] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, et al., arXiv preprint arXiv:1707.00934 (2017).
[9] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, Physical Review Letters 78, 3221 (1997).
[10] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Physical Review A 54, 3824 (1996).
[11] D. G. Cory, M. Price, W. Maas, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. Somaroo, Physical Review Letters 81, 2152 (1998).
[12] K. Bailey and K. Curran, Multimedia Tools and Applications 30, 55 (2006).
[13] E. I. Lin, A. M. Eskicioglu, R. L. Lagendijk, and E. J. Delp, Proceedings of the IEEE 93, 171 (2005).
[14] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A 59, 1829 (1999).
[15] L. Xiao, G. Lu Long, F.-G. Deng, and J.-W. Pan, Phys. Rev. A 69, 052307 (2004).
[16] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. 86, 5807 (2001).
[17] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, IEEE Transactions on Information Theory 48, 580 (2002).
[18] T. Eggeling and R. F. Werner, Phys. Rev. Lett. 89, 097905 (2002).
[19] D. P. DiVincenzo, P. Hayden, and B. M. Terhal, Foundations of Physics 33, 1629 (2003).
[20] P. Hayden, D. Leung, and G. Smith, Phys. Rev. A 71, 062339 (2005).
[21] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, Phys. Rev. A 59, 1070 (1999).
[22] S. De Rinaldis, Phys. Rev. A 70, 022309 (2004).
[23] R. Augusiak, T. Fritz, M. Kotowski, M. Kotowski, M. Pawłowski, M. Lewenstein, and A. Acín, Phys. Rev. A 85, 042113 (2012).
[24] N. Johnston, in 8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013), Leibniz International Proceedings in Informatics (LIPIcs), Vol. 22, edited by S. Severini and F. Brandao (Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 2013) pp. 93–105.
[25] Y.-L. Wang, M.-S. Li, Z.-J. Zheng, and S.-M. Fei, Phys. Rev. A 92, 032313 (2015).
[26] X. Zhang, X. Tan, J. Weng, and Y. Li, Scientific reports 6, 28864 (2016).