Tighter generalized entropic uncertainty relations in multipartite systems

Lin Wu, Liu Ye, and Dong Wang [*]
School of Physics & Optoelectronic Engineering, Anhui University, Hefei 230601, People's Republic of China

(Received 18 April 2022; revised 29 September 2022; accepted 19 December 2022; published 28 December 2022)

The uncertainty principle, which demonstrates the intrinsic uncertainty of nature from an information-theory perspective, is at the heart of quantum information theory. In the realm of quantum information theory, Shannon entropy is used to depict the uncertainty relation in general. A tighter lower bound for uncertainty relations facilitates more accurate predictions of measurement outcomes and more robust quantum information processing. Interestingly, the tripartite entropic uncertainty relation (EUR) can be further optimized. Renes *et al.* proposed a tripartite EUR [J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009)], and subsequently, Ming *et al.* strengthened its lower bound in [F. Ming, D. Wang, X.-G. Fan, W.-N. Shi, L. Ye, and J.-L. Chen, Phys. Rev. A **102**, 012206 (2020)]. Specifically, we derive a tighter lower bound of the tripartite EUR using the Holevo quantity. Furthermore, we generalize the tripartite EUR, that is, the generalized entropic uncertainty relation for multiple measurements in multipartite systems. As illustrations, we provide several typical examples to show that our bound is tight and outperforms the previous bound. Furthermore, our findings pave the way for using the tighter bound for the quantum secret key rate in quantum key distribution protocols and are essential for quantum precision measurements in the framework of genuine multipartite systems. By providing a close peek at the nature of uncertainty, our results may find broad applications in the security analysis of quantum cryptography.

DOI: 10.1103/PhysRevA.106.062219

I. INTRODUCTION

The uncertainty principle proposed by Heisenberg in 1927 [1] is significant in quantum information theory, which distinguishes quantum physics from classical physics. The uncertainty principle bounds the product (or sum) of two or more uncertainties, each associated with a different observable [2]. Kennard [3] improved the position-momentum uncertainty relation and Robertson [4] derived a generalized uncertainty relation for two arbitrarily incompatible observables $\hat{Q}$ and $\hat{R}$, described as

$$\Delta\hat{Q}\Delta\hat{R} \geqslant \tfrac{1}{2}|\langle[\hat{Q},\hat{R}]\rangle|. \tag{1}$$

Robertson's relation, which provides a lower bound of the standard deviation, is the most widely used formula for the uncertainty principle. However, the bound depends on the state of system. This result well be trivial if the system is prepared in an observable's eigenstate. With the development of quantum information theory, Shannon entropy was introduced as an effective measure of uncertainty [5]. Pioneeringly, Białynicki-Birula and Mycielski [6] proposed novel entropy-based Heisenberg uncertainty relations for position and momenta. Subsequently, Deutsch presented the entropic uncertainty relation (EUR) for two arbitrarily incompatible observables [7]. Later, Kraus [8], Maassen, and Uffink [9] optimized Deutsch's result into

$$H(\hat{Q}) + H(\hat{R}) \geqslant -\log_2 c(\hat{Q},\hat{R}) \equiv q_{MU}, \tag{2}$$

where $H(\hat{Q}) = -\sum_i p_i \log_2 p_i$ represents Shannon entropy and $p_i = \langle\mu_i|\hat{\rho}|\mu_i\rangle$. The quantity $c(\hat{Q},\hat{R}) \equiv \max_{j,k}|\langle\mu_j|\nu_k\rangle|^2$ denotes maximal overlap, where $|\mu_j\rangle$ and $|\nu_k\rangle$ denote the eigenvectors of observables $\hat{Q}$ and $\hat{R}$, respectively. The bound q_{MU} is determined only by the incompatibility of the observables, which is state independent.

Renes *et al.* [10] and Berta *et al.* [11] proposed the following quantum-memory-assisted entropic uncertainty relation (QMA-EUR) for when the measured particle is correlated to another particle:

$$S(\hat{Q}|B) + S(\hat{R}|B) \geqslant S(A|B) - \log_2 c(\hat{Q},\hat{R}), \tag{3}$$

with an arbitrary bipartite system AB, where $S(\hat{R}|B) = S(\hat{\rho}_{\hat{R}B}) - S(\hat{\rho}_B)$ denotes the conditional von Neumann entropy [12] of the postmeasurement states after measuring $\hat{R}$ on A using $\hat{\rho}_{\hat{R}B} = \sum_i (|\nu_i\rangle_A\langle\nu_i| \otimes \mathbb{I}_B)\hat{\rho}_{AB}(|\nu_i\rangle_A\langle\nu_i| \otimes \mathbb{I}_B)$. $\mathbb{I}_B$ is an identical operator in the Hilbert space of B. $S(A|B) = S(\hat{\rho}_{AB}) - S(\hat{\rho}_B)$ denotes the conditional von Neumann entropy of the systemic density operator $\hat{\rho}_{AB}$. Following this inequality, several interesting conclusions can be: (i) Equation (2) can be obtained from Eq. (3) when A is disentangled from B. (ii) When the conditional von Neumann entropy $S(A|B)$ is negative, the measured particle A and memory particle B are entangled, which reduces the measurement uncertainty. In particular, Alice's measured outcomes can be perfectly predicted by Bob using $S(A|B) = -\log_2 d$ (d is the dimension of the measured particle) when A and B are maximally entangled. (iii) If the quantum memory is absent, Eq. (3) simplifies $H(\hat{Q}) + H(\hat{R}) \geqslant -\log_2 c(\hat{Q},\hat{R}) + S(A)$, which yields a tighter lower bound compared with Maassen and Uffink's result (2) owing to $S(A) \geqslant 0$.

The EUR, although initially developed to improve the predictive accuracy of the quantum uncertainty principle, is also a pillar for quantum information processing, including entan-

[*] dwang@ahu.edu.cn

glement witnesses [11], quantum teleportation [13], quantum randomness [14], QKD [15], quantum metrology [16,17], quantum steering [18–20], and so forth [21–24]. In addition, many promising improvements for QMA-EUR have been made [25–42]. Specifically, Pramanik *et al.* [28] presented a new form of uncertainty relation using extractable classical information. By considering the second-largest value of the overlap $c(\hat{Q}, \hat{R})$, Coles and Piani [32] presented another tight uncertainty relation. In 2015, Liu *et al.* [37] presented an uncertainty relation for multiobservable scenarios. In 2016, Adabi *et al.* [38] optimized the lower bound by adding mutual information, and the Holevo quantity was expressed as

$$S(\hat{Q}|B) + S(\hat{R}|B) \geqslant q_{MU} + S(A|B) + \max\{0, \Lambda\}, \quad (4)$$

where

$$\Lambda = \mathcal{I}(A:B) - [\mathcal{I}(\hat{Q}:B) + \mathcal{I}(\hat{R}:B)], \quad (5)$$

here $\mathcal{I}(A:B) = S(\hat{\rho}_A) + S(\hat{\rho}_B) - S(\hat{\rho}_{AB})$ is the mutual information and $\mathcal{I}(\hat{Q}:B) = S(\hat{\rho}_B) - \sum_i p_i S(\hat{\rho}_{B|i})$ denotes the Holevo quantity. Additionally, $p_i = \mathrm{Tr}_{AB}(\Pi_i^A \hat{\rho}^{AB} \Pi_i^A)$ is the probability of obtaining the ith measurement outcome by measuring $\hat{Q}$ on A. Xie *et al.* [41] improved the lower bound of the entropic uncertainty relation for multiple measurements in bipartite systems [37]. To date, several novel experiments have been conducted to demonstrate various uncertainty relations [43–51].

For tripartite cases, Renes and Boileau [10] originally proposed an uncertainty relation only for observables related by a Fourier transform. Later, the general case was proven by Berta *et al.* [11]

$$S(\hat{Q}|B) + S(\hat{R}|C) \geqslant q_{MU}. \quad (6)$$

Essentially, this inequality implies a tradeoff between complementarity measurements, which can be interpreted using the monogamy game. Assume that the tripartite A, B, and C are available to three participants, Alice, Bob, and Charlie, respectively, who share a quantum state $\hat{\rho}_{ABC}$. Alice randomly measures one of the two observables ($\hat{Q}$ and $\hat{R}$) and obtains κ. She then informs Bob and Charlie of her choice of measurement. Finally, the game can only be won if both successfully predict the outcome κ. The lower bound q_{MU} is only relevant to the complementarity of the observables and is state independent. The pursuit of a tighter bound is fundamental for realistic quantum information processing. Motivated by this, some efforts have been made [52,53] to improve the tripartite QMA-EURs. Recently, Ming *et al.* [52] presented a new tripartite QMA-EUR by considering mutual information and the Holevo quantity as

$$S(\hat{Q}|B) + S(\hat{R}|C) \geqslant q_{MU} + \max\{0, \Delta\}, \quad (7)$$

with $\Delta = 2S(A) + q_{MU} - \mathcal{I}(A:B) - \mathcal{I}(A:C) + \mathcal{I}(\hat{R}:B) + \mathcal{I}(\hat{Q}:C) - H(\hat{Q}) - H(\hat{R})$, which provides a tighter lower bound than that found in Ref. [10].

The relations mentioned above are only applicable to two- or three-particle systems. Genuine quantum information processing is not only required to estimate the measurement uncertainty of two observables in bipartite or tripartite systems, but also for multiple measurements in correlated many-body systems. Finding a generalized communication bound that suits arbitrary multiple nodes is at the heart of constructing a quantum network. In particular, as a critical application in the security analysis of QKD, EURs not only require simple two- or three-particle systems but also require more generalized many-body systems. Considering this, we focus on suggesting a stronger tripartite QMA-EUR, which perfectly captures the characteristics of measurement uncertainty for some canonical states ρ_{ABC}. Furthermore, we derived a generalized QMA-EUR for multiple measurements within multipartite systems.

The remainder of this paper is organized as follows. In Sec. II, a lower bound of the tripartite QMA-EUR is derived by considering the Holevo quantity. We generalize this to the case of arbitrary multiobservables in multipartite systems. In Sec. III, we take several examples (the GHZ-type, Werner-type, symmetric family of mixed four-qubit, and random four-qubit states) to support our findings. In Sec. IV, the application of our proposed generalized QMA-EUR on the quantum secret key rate is discussed. Finally, we provide a concise conclusion.

II. TIGHTER TRIPARTITE EUR AND GENERALIZED EUR

We propose a tighter tripartite QMA-EUR based on Adabi *et al.*'s bipartite EUR in Eq. (4) and Renes-Boileau's EUR in Eq. (6).

Theorem 1. By considering the Holevo quantity, the improved tripartite QMA-EUR can be expressed as

$$S(\hat{Q}|B) + S(\hat{R}|C) \geqslant q_{MU} + \max\{0, \delta\} \quad (8)$$

for any tripartite state $\hat{\rho}_{ABC}$ with

$$\delta = q_{MU} + 2S(A) - \mathcal{I}(\hat{Q}:B) - \mathcal{I}(\hat{R}:C) - H(\hat{Q}) - H(\hat{R}), \quad (9)$$

which outperforms the previous bounds in Eqs. (6) and (7).

Proof. Considering the QMA-EUR in Eq. (4), the following equation is satisfied:

$$S(\hat{Q}|B) + S(\hat{R}|B) \geqslant q_{MU} + S(A|B) + \mathcal{I}(A:B) - \mathcal{I}(\hat{Q}:B) - \mathcal{I}(\hat{R}:B), \quad (10)$$

$$S(\hat{Q}|C) + S(\hat{R}|C) \geqslant q_{MU} + S(A|C) + \mathcal{I}(A:C) - \mathcal{I}(\hat{Q}:C) - \mathcal{I}(\hat{R}:C), \quad (11)$$

for a tripartite system $\hat{\rho}_{ABC}$. By combining Eqs. (10) and (11), the following inequality is obtained:

$$\begin{aligned} S(\hat{Q}|B) + S(\hat{R}|C) \geqslant\ & 2q_{MU} + S(A|B) + S(A|C) \\ & + \mathcal{I}(A:B) + \mathcal{I}(A:C) \\ & - \mathcal{I}(\hat{Q}:B) - \mathcal{I}(\hat{Q}:C) \\ & - \mathcal{I}(\hat{R}:B) - \mathcal{I}(\hat{R}:C) \\ & - S(\hat{Q}|C) - S(\hat{R}|B). \end{aligned} \quad (12)$$

By substituting $S(A) = S(A|B) + \mathcal{I}(A:B) = S(A|C) + \mathcal{I}(A:C)$, $H(\hat{Q}) = S(\hat{Q}|C) + \mathcal{I}(\hat{Q}:C)$ and $H(\hat{R}) = S(\hat{R}|B) + \mathcal{I}(\hat{R}:B)$ into on the right-hand side of the inequality above, we obtain

$$S(\hat{Q}|B)+S(\hat{R}|C)\geqslant 2q_{MU}+2S(A)-\mathcal{I}(\hat{Q}:B)-\mathcal{I}(\hat{R}:C)-H(\hat{Q})-H(\hat{R}). \tag{13}$$

Resorting to Eqs. (6) and (13), we can derive the desired results in Eqs. (8) by considering optimization over the two bounds.

Incidentally, we note that Dolatkhah *et al.* [53] proposed another lower bound of the tripartite QMA-EUR by adding mutual information and the Holevo quantity beyond Ming *et al.*'s result [52], expressed as

$$S(\hat{Q}|B)+S(\hat{R}|C)\geqslant q_{MU}+\frac{S(A|B)+S(A|C)}{2}+\max\{0,\delta'\}, \tag{14}$$

with $\delta'=\frac{\mathcal{I}(A:B)+\mathcal{I}(A:C)}{2}-[\mathcal{I}(\hat{Q}:B)+\mathcal{I}(\hat{R}:C)]$. Remarkably, it is found that the result in Eq. (14) is incorrect. It is verified that the derivation is illogical and the lower bound $q_{MU}+\frac{S(A|B)+S(A|C)}{2}$ exceeds the uncertainty quantity [that is, $S(\hat{Q}|B)+S(\hat{R}|C)$] in some cases when $\delta'<0$ hold, which violates the result of Eq. (14).

Theorem 2. The generalized entropic uncertainty relation for multiobservable measurements in the context of a multipartite system can be written as

$$\sum_{i=1}^{n}S(\hat{\mathcal{O}}_i|B_i)\geqslant-\frac{\sum_{i\neq j,i=1}^{n}\log_2 c(\hat{\mathcal{O}}_i,\hat{\mathcal{O}}_j)}{n-1}+\max\{0,\delta_n\}, \tag{15}$$

with

$$\delta_n=-\frac{\sum_{i\neq j,i=1}^{n}\log_2 c(\hat{\mathcal{O}}_i,\hat{\mathcal{O}}_j)}{n-1}+nS(A)-\sum_{i=1}^{n}H(\hat{\mathcal{O}}_i)-\sum_{i=1}^{n}\mathcal{I}(\hat{\mathcal{O}}_i:B_i), \tag{16}$$

where $\hat{\mathcal{O}}_i$ denotes the ith measurement on subsystem A and B_i represents the ith quantum memory in the multipartite system.

Proof. Compared to the tripartite EUR in Eq. (13), we can write $n(n-1)/2$ inequalities for n-observable measurements in $(n+1)$-party system $\hat{\rho}_{AB_1B_2B_3B_4\ldots B_n}$ as

$$\begin{aligned}
&S(\hat{\mathcal{O}}_1|B_1)+S(\hat{\mathcal{O}}_2|B_2)\geqslant-2\log_2 c(\hat{\mathcal{O}}_1,\hat{\mathcal{O}}_2)+2S(A)-H(\hat{\mathcal{O}}_1)-H(\hat{\mathcal{O}}_2)-\mathcal{I}(\hat{\mathcal{O}}_1:B_1)-\mathcal{I}(\hat{\mathcal{O}}_2:B_2),\\
&S(\hat{\mathcal{O}}_1|B_1)+S(\hat{\mathcal{O}}_3|B_3)\geqslant-2\log_2 c(\hat{\mathcal{O}}_1,\hat{\mathcal{O}}_3)+2S(A)-H(\hat{\mathcal{O}}_1)-H(\hat{\mathcal{O}}_3)-\mathcal{I}(\hat{\mathcal{O}}_1:B_1)-\mathcal{I}(\hat{\mathcal{O}}_3:B_3),\\
&S(\hat{\mathcal{O}}_1|B_1)+S(\hat{\mathcal{O}}_4|B_4)\geqslant-2\log_2 c(\hat{\mathcal{O}}_1,\hat{\mathcal{O}}_4)+2S(A)-H(\hat{\mathcal{O}}_1)-H(\hat{\mathcal{O}}_4)-\mathcal{I}(\hat{\mathcal{O}}_1:B_1)-\mathcal{I}(\hat{\mathcal{O}}_4:B_4),\\
&\qquad\vdots\\
&S(\hat{\mathcal{O}}_2|B_2)+S(\hat{\mathcal{O}}_3|B_3)\geqslant-2\log_2 c(\hat{\mathcal{O}}_2,\hat{\mathcal{O}}_3)+2S(A)-H(\hat{\mathcal{O}}_2)-H(\hat{\mathcal{O}}_3)-\mathcal{I}(\hat{\mathcal{O}}_2:B_2)-\mathcal{I}(\hat{\mathcal{O}}_3:B_3),\\
&S(\hat{\mathcal{O}}_2|B_2)+S(\hat{\mathcal{O}}_4|B_4)\geqslant-2\log_2 c(\hat{\mathcal{O}}_2,\hat{\mathcal{O}}_4)+2S(A)-H(\hat{\mathcal{O}}_2)-H(\hat{\mathcal{O}}_4)-\mathcal{I}(\hat{\mathcal{O}}_2:B_2)-\mathcal{I}(\hat{\mathcal{O}}_4:B_4),\\
&\qquad\vdots\\
&S(\hat{\mathcal{O}}_{n-1}|B_{n-1})+S(\hat{\mathcal{O}}_n|B_n)\geqslant-2\log_2 c(\hat{\mathcal{O}}_{n-1},\hat{\mathcal{O}}_n)+2S(A)-H(\hat{\mathcal{O}}_{n-1})-H(\hat{\mathcal{O}}_n)-\mathcal{I}(\hat{\mathcal{O}}_{n-1}:B_{n-1})-\mathcal{I}(\hat{\mathcal{O}}_n:B_n).
\end{aligned}$$

Next, the above $n(n-1)/2$ inequalities are summed and divided on both sides of the summation inequality by $(n-1)$. Consequently, we obtain

$$\sum_{i=1}^{n}S(\hat{\mathcal{O}}_i|B_i)\geqslant-2\frac{\sum_{i\neq j,i=1}^{n}\log_2 c(\hat{\mathcal{O}}_i,\hat{\mathcal{O}}_j)}{n-1}+nS(A)-\sum_{i=1}^{n}H(\hat{\mathcal{O}}_i)-\sum_{i=1}^{n}\mathcal{I}(\hat{\mathcal{O}}_i:B_i). \tag{17}$$

Similarly, to compare our bound with Renes-Boileau's result, we generalize the previous tripartite QMA-EURs in Eq. (6) into a general case of n-observable measurements in the $(n+1)$-party system $\hat{\rho}_{AB_1B_2B_3B_4\ldots B_n}$ and deduce the following inequality:

$$\sum_{i=1}^{n}S(\hat{\mathcal{O}}_i|B_i)\geqslant-\frac{\sum_{i\neq j,i=1}^{n}\log_2 c(\hat{\mathcal{O}}_i,\hat{\mathcal{O}}_j)}{n-1}. \tag{18}$$

Combining the two derivations in Eqs. (17) and (18), the desired generalized EUR for multiobservables in multipartite systems can be obtained as Eq. (15) by considering the optimization.

In addition, to compare our results with those of Ming *et al.*, we derive the tripartite EUR proposed by Ming *et al.* for multimeasurements in multipartite systems

$$\sum_{i=1}^{n}S(\hat{\mathcal{O}}_i|B_i)\geqslant-\frac{\sum_{i\neq j,i=1}^{n}\log_2 c(\hat{\mathcal{O}}_i,\hat{\mathcal{O}}_j)}{n-1}+\max\{0,\Delta_n\}, \tag{19}$$

where $\Delta_n=-\frac{\sum_{i\neq j,i=1}^{n}\log_2 c(\hat{\mathcal{O}}_i,\hat{\mathcal{O}}_j)}{n-1}+nS(A)-\sum_{i=1}^{n}\mathcal{I}(A:B_i)-\sum_{i=1}^{n}H(\hat{\mathcal{O}}_i)+\frac{\sum_{i\neq j,i=1,j=1}^{n}\mathcal{I}(\hat{\mathcal{O}}_i:B_j)}{n-1}$.

III. TYPICAL EXAMPLES

It is well known that mutually unbiased observables are crucial in quantum information theory. For mutually unbiased bases (MUBs), $\{|\psi_a\rangle\}_{a=1,2,\ldots,d}$ and $\{|\phi_b\rangle\}_{b=1,2,\ldots,d}$, $|\langle\psi_a|\phi_b\rangle|^2=1/d$ holds, $\forall$ a and b. The mutually unbiased observables are observables whose eigenbases are MUBs. In two-dimensional space, the Pauli measurements $\hat{\sigma}_1, \hat{\sigma}_2, \hat{\sigma}_3$ are known as typical MUBs. Here, we consider spin-1/2 Pauli matrices as the measured observables in various quadripartite systems $\hat{\rho}_{ABCD}$. Thus, $c(\hat{O}_i, \hat{O}_j) = 1/2 \ (i \neq j)$, which leads to $-\log_2 c(\hat{O}_i, \hat{O}_j) = 1$. Furthermore, we generalize Renes-Boileau's and Ming *et al.*'s relations in Eqs. (18) and (19) to the quadripartite framework to demonstrate that our lower bound is tighter than the previous ones. The generalized Renes-Boileau relation can be written as

$$S(\hat{Q}|B) + S(\hat{R}|C) + S(\hat{T}|D) \geqslant \mathcal{Q}_{MU} := B_{RB} \tag{20}$$

in a quadripartite system, where

$$\mathcal{Q}_{MU} = \frac{q_{MU1} + q_{MU2} + q_{MU3}}{2}. \tag{21}$$

However, the relation of Ming *et al.* can be generalized to the quadripartite system version

$$S(\hat{Q}|B) + S(\hat{R}|C) + S(\hat{T}|D) \geqslant \mathcal{Q}_{MU} + \max\{0, \Delta_3\} := B_M, \tag{22}$$

where

$$\begin{aligned}\Delta_3 = {} & \mathcal{Q}_{MU} + 3S(A) - H(\hat{Q}) - H(\hat{R}) - H(\hat{T}) \\ & - [\mathcal{I}(A, B) + \mathcal{I}(A, C) + \mathcal{I}(A, D)] \\ & + \frac{\mathcal{I}(\hat{Q}, C) + \mathcal{I}(\hat{Q}, D) + \mathcal{I}(\hat{R}, B)}{2} \\ & + \frac{\mathcal{I}(\hat{R}, D) + \mathcal{I}(\hat{T}, B) + \mathcal{I}(\hat{T}, C)}{2}.\end{aligned} \tag{23}$$

In the following, we can use the result from Eq. (15) for three measurements and obtain a tighter bound

$$S(\hat{Q}|B) + S(\hat{R}|C) + S(\hat{T}|D) \geqslant \mathcal{Q}_{MU} + \max\{0, \delta_3\} := B_O, \tag{24}$$

with

$$\begin{aligned}\delta_3 = {} & \mathcal{Q}_{MU} + 3S(A) - H(\hat{Q}) - H(\hat{R}) - H(\hat{T}) \\ & - [\mathcal{I}(\hat{Q} : B) + \mathcal{I}(\hat{R} : C) + \mathcal{I}(\hat{T} : D)].\end{aligned} \tag{25}$$

To verify our findings, we now compare our proposed bound with the results of Renes-Boileau and Ming *et al.* in different four-qubit state scenarios.

A. GHZ-type states

First, we consider a generalized pure four-qubit Greenberg (Horne) Zeilinger state, expressed as

$$|\Psi\rangle_{ABCD}^{\mathrm{GHZ}} = \sin\alpha|0000\rangle + \cos\alpha|1111\rangle, \tag{26}$$

with the state parameter $\alpha \in [0, 2\pi)$. To compare our result with the previous one, we draw different lower bounds versus α in the four-qubit GHZ state, as shown in Fig. 1. In this case, the bounds of Renes-Boileau and Ming *et al.* are equal to 3/2 and our lower bound is stronger than the previous ones, as displayed in the figure.

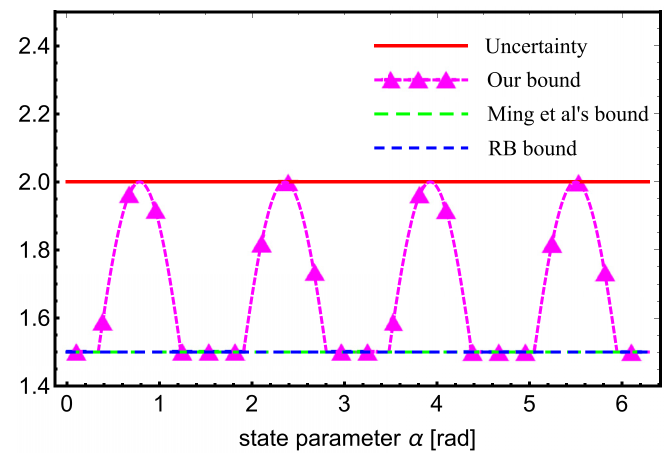

FIG. 1. Uncertainty and the lower bounds versus α in four-qubit GHZ-type states. The red solid line denotes the quantity of the entropy-based uncertainty [left-hand side of Eq. (24)], magenta dashed line with magenta triangle denotes our bound [right-hand side of Eq. (24)], green dashed line denotes Ming *et al.*'s bound result [right-hand side of Eq. (22)], and blue dashed line denotes Renes-Boileau's bound [right-hand side of Eq. (20)].

B. Werner-type states

As another example, we consider a class of Werner-type states, taking the form

$$\hat{\rho}_{ABCD} = p|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}| + \frac{(1-p)}{16}\mathbb{I}_{16\times16}, \tag{27}$$

where the purity of the state $p \in [0, 1]$ and $|\mathrm{GHZ}\rangle = \cos\beta|0000\rangle + \sin\beta|1111\rangle$ ($\beta \in [0, 2\pi]$), and $\mathbb{I}_{16\times16}$ represents a 16×16 identity matrix. In Figs. 2(a) and 2(b), our bound, Ming *et al.*'s bound, and Renes-Boileau's bound vary with the state purity p and state parameter β, where $\beta = \frac{\pi}{4}$ and $p = 0.5$, respectively. As indicated in the figure, our derived bound is higher than those of Ming *et al.* and Renes-Boileau, that is, $B_{RB} \leqslant B_M \leqslant B_O \leqslant U$. Our bound can perfectly capture the characteristics of the behavior of entropic uncertainty, as shown in Fig. 2(a).

C. Symmetric family of mixed four-qubit states

In addition, we consider a mixture of the GHZ and W states, which can be described as the following maximally mixed four-qubit state:

$$\hat{\rho}_{ABCD} = \frac{\eta}{2}|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}| + \frac{\eta}{2}|W\rangle\langle W| + \frac{(1-\eta)}{16}\mathbb{I}_{16\times16}, \tag{28}$$

where $|W\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$, $|\mathrm{GHZ}\rangle = \sin\gamma|0000\rangle + \cos\gamma|1111\rangle$ and the state's parameter $\eta \in [0, 1]$. We plot our bound, the bound of Ming *et al.*, and Renes-Boileau's bound as a function of η in Fig. 3, for $\gamma = \frac{\pi}{3}$. Our bound outperforms the previous ones. The derived bound perfectly matches the magnitude of the entropic uncertainty.

D. Random four-qubit states

Now, we consider more general states, that is, arbitrary sets of random four-qubit states containing both pure and

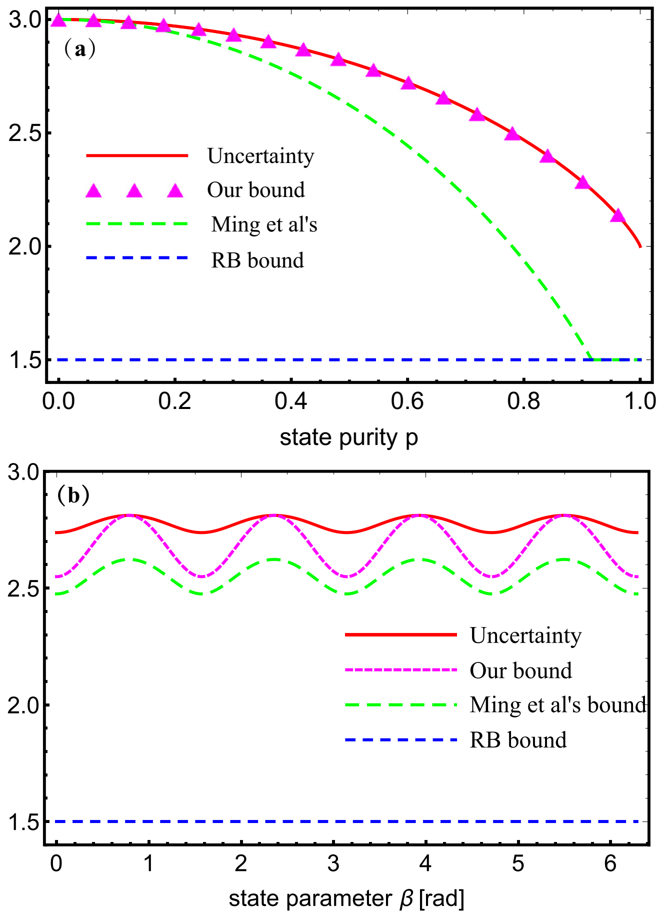

FIG. 2. Entropic uncertainty and the lower bounds for four-qubit Werner-type states. (a) Uncertainty and the lower bounds versus the state's purity p. (b) Uncertainty and the lower bounds versus the state's parameter β. The red solid line denotes the quantity of the entropy-based uncertainty [left-hand side of Eq. (24)], magenta dashed line or magenta triangle denotes our bound [right-hand side of Eq. (24)], green dashed line denotes Ming *et al.*'s bound result [right-hand side of Eq. (22)], and blue dashed line denotes Renes-Boileau's bound [right-hand side of Eq. (20)].

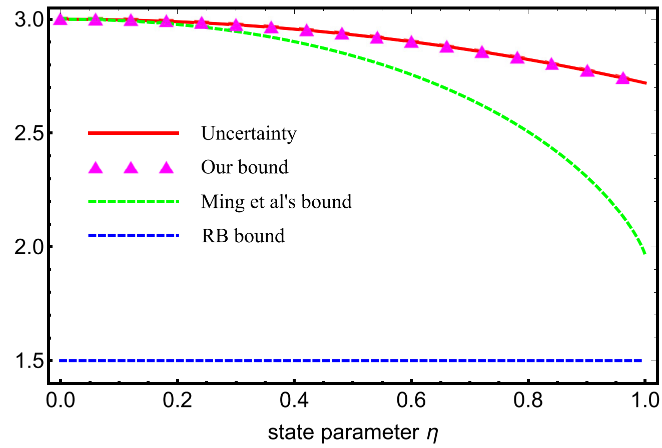

FIG. 3. Uncertainty and the lower bounds versus the state parameter η in a symmetric family of mixed four-qubit states. Red solid line denotes the quantity of the entropy-based uncertainty [left-hand side of Eq. (24)], magenta triangle denotes our bound [right-hand side of Eq. (24)], green dashed line denotes the bound of Ming *et al.* [right-hand side of Eq. (22)], and blue dashed line denotes Renes-Boileau's bound [right-hand side of Eq. (20)].

mixed states, which are generally used to verify whether the proposed relation holds for all ensembles of states. First, we introduce an efficient approach to generating arbitrary random states. According to the spectral decomposition theorem, arbitrary random four-qubit states can be decomposed into the form $\hat{\rho} = \sum_{n=1}^{16} \vartheta_n |\phi_n\rangle\langle\phi_n|$, where ϑ_n and $|\phi_n\rangle$ denote the nth eigenvalues and eigenstates of $\hat{\rho}$. Additionally, the eigenvalue ϑ_n corresponds to the probability that the state of the system $\hat{\rho}$ is in the state $|\phi_n\rangle$. Therefore, we can construct an arbitrary unitary operation Ξ by using the normalized eigenvector $|\phi_n\rangle$. In principle, an arbitrary four-qubit state can be composed of arbitrary probabilities ϑ_n and an arbitrary unitary operation Ξ. For this purpose, we define a random function $\zeta(x_1, x_2)$ that randomly generates a real number in each interval $[x_1, x_2]$. Then, the random number p_m can be generated using the following method:

$$p_1 = \zeta(0, 1), \quad p_{i+1} = \zeta(0, 1)p_i, \tag{29}$$

where $i \in \{1, 2, 3, \ldots, 15\}$. In addition, a set of random probabilities ϑ_n ($n \in \{1, 2, 3, \ldots, 16\}$) consists of p_m, which is given by

$$\vartheta_n = \frac{p_m}{\sum_{m=1}^{16} p_m}. \tag{30}$$

Based on the above two formulas, we can obtain a set of probabilities in descending order.

Technically, the one 16-order real matrix $\mathcal{M}$ can be randomly generated using the random function $\zeta(-1, 1)$ in the interval $[-1, 1]$ by constructing a random unitary operation. Utilizing the real matrix $\mathcal{M}$, a random Hermitian matrix is expressed as

$$\mathcal{A} = \mathcal{D} + (\mathcal{U}^{\mathbb{T}} + \mathcal{U}) + i(\mathcal{L}^{\mathbb{T}} + \mathcal{L}), \tag{31}$$

where $\mathcal{D}$, $\mathcal{L}$, and $\mathcal{U}$ represent the diagonal, strictly lower, and strictly higher triangular parts of the real matrix $\mathcal{M}$, respectively. $\mathcal{U}^{\mathbb{T}}$ represents the transposition of $\mathcal{U}$.

Applying the above procedure, we obtain 16 normalized eigenvectors $|\phi_n\rangle$ of the Hermitian matrix $\mathcal{A}$, which forms a random unitary operation Ξ. Consequently, the spectral decomposition for a random four-qubit state $\hat{\rho}$ is perfectly constructed.

To verify our conclusions, we adopt 2×10^5 random states to show the uncertainty and our bound and that of Ming *et al.*, as shown in Fig. 4, which shows two nontrivial points: (i) our presented EUR in Eq. (15) holds, demonstrating that the relation is universal; (ii) our bound is closer to the measurement uncertainty performed with Ming *et al.*'s bound, that is, $B_O \geqslant B_M$, implying that our bound is stronger than the previous bounds. Meanwhile, we depict the difference between our lower bound and that of Ming *et al.* ($B_O - B_M$) for arbitrary randomly generated four-qubit states in Fig. 5, and this shows that $B_O - B_M \geqslant 0$ always holds, which supports our conclusion. Further, a comparison of our bound with Renes-Boileau's bound is plotted in Fig. 6 in the regime of

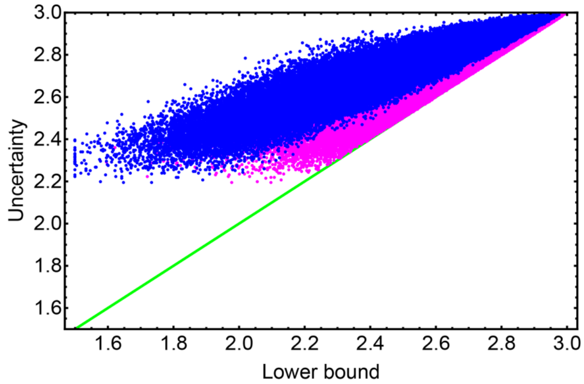

FIG. 4. Uncertainty, our derived bound, and that of Ming *et al.* for 2×10^5 four-qubit random states. The x axis denotes the lower bound and the magenta and blue dots represent our bound and that of Ming *et al.*, respectively. The y axis denotes the entropic uncertainty. The green line represents the proportion function with a unitary slope.

randomly generated four-qubit states. The figure shows the following: our bound is greater than the Renes-Boileau bound in Eq. (12). Considering the comparison results, it is reasonable to conjecture that our derived inequality is universal and optimal.

IV. APPLICATIONS

EUR directly reflects the security of a QKD: a tighter EUR guarantees a higher quantum secret key rate (QSKR) and hence signifies higher security to QKD. Our tighter uncertainty bound is relevant for the security analysis of QKD protocols in practical many-body systems. Here, we focus on the security analysis of QKD protocols in practical many-body systems. There are two honest parts (Alice and Bob) that share a key by communicating over a public channel and the key is secret to any third-party eavesdropper (David). Devetak and Winter [54] proposed that the QSKR $\mathbb{K}$ that can be extracted by Alice and Bob is lower-bounded by

$$\mathbb{K} \geqslant S(\hat{R}|D) - S(\hat{R}|B), \tag{32}$$

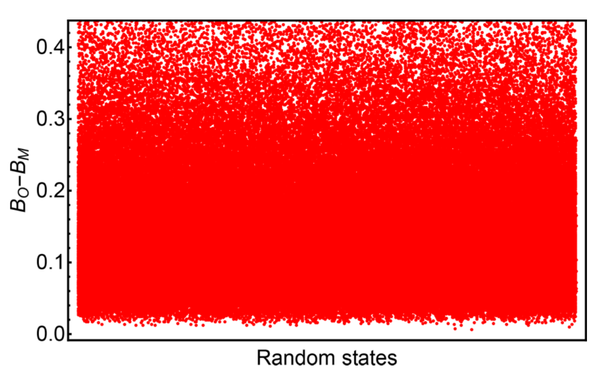

FIG. 5. Comparison of our bound and that of Ming *et al.* using $(B_O - B_M)$ for 2×10^5 four-qubit random states. The x axis represents the randomly generated four-qubit states and the y axis represents $(B_O - B_M)$.

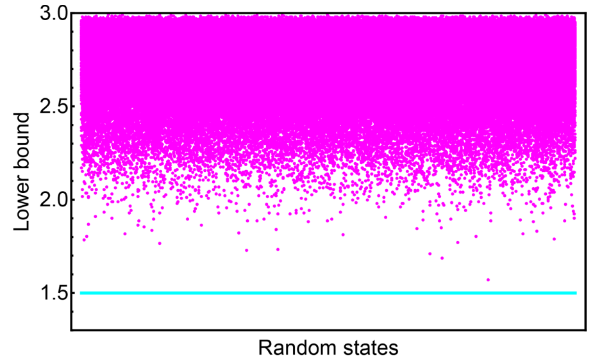

FIG. 6. Our lower bound versus the Renes-Boileau for 2×10^5 four-qubit random states. The x axis is the randomly generated four-qubit states, the y axis represents the lower bound B_O, and the cyan line represents Renes-Boileau bound in B_{RB}.

where the eavesdropper (David) prepares a quantum state ρ_{ABD} and sends particles A and B to Alice and Bob, respectively, while maintaining D. By virtue of Renes and Boileau's result, expressed as $S(\hat{Q}|B) + S(\hat{R}|D) \geqslant q_{MU}$ in Eq. (6), we obtain

$$\mathbb{K} \geqslant q_{MU} - S(\hat{Q}|B) - S(\hat{R}|B). \tag{33}$$

By utilizing $S(\hat{Q}|B) \leqslant S(\hat{Q}|\hat{Q}')$ and $S(\hat{R}|B) \leqslant S(\hat{R}|\hat{R}')$, QSKR can be rewritten as

$$\mathbb{K} \geqslant q_{MU} - S(\hat{Q}|\hat{Q}') - S(\hat{R}|\hat{R}'). \tag{34}$$

Considering the lower bound of the tripartite uncertainty relation in Eq. (8), we obtain a new lower bound for generating the QSKR, that is,

$$\widetilde{\mathbb{K}} \geqslant q_{MU} + \max\{0, \delta\} - S(\hat{Q}|B) - S(\hat{R}|B). \tag{35}$$

As no measurement can reduce the entropy of the system, the lower bound of the QSKR can be improved to

$$\widetilde{\mathbb{K}} \geqslant q_{MU} + \max\{0, \delta\} - S(\hat{Q}|Q') - S(\hat{R}|R'). \tag{36}$$

Compared with Eq. (34), the new lower bound of the QSKR has an additional term $\max\{0, \delta\}$, which is greater than or equal to zero. Hence, it is verified that $\widetilde{\mathbb{K}}$ is greater than $\mathbb{K}$, which means our lower bound enhances the security of prospective quantum communication networks and thus enables us to efficiently improve security analysis in practical QKD protocols.

V. CONCLUSION

To summarize, we presented a tighter lower bound of the tripartite QMA-EUR with the Holevo quantity and derived a generalized entropic uncertainty relation for multiple observable measurements in multipartite systems. The tighter lower bound is essential for processing realistic quantum information. Additionally, by verifying analytical and numerical four-qubit states, we conjecture that our bound outperforms the bounds derived from the results of Ming *et al.* and Renes *et al.* As examples, we analyze the cases of three observable measurements in four-qubit pure and mixed systems, including the GHZ-type states, Werner-type states, symmetric family of mixed four-qubit states, and randomly generated four-qubit states, which supports that our derived relation is universal and optimized compared with previous works [10,52]. We showed that the generalized entropic uncertainty relation can support the improvement of the QSK rate bound in practical QKD protocols, laying foundations for the exploration of more complex, higher-dimensional measurements by state-of-the-art entropy-based information theories. Therefore, we argue that our findings provide in-depth insight into general entropy-based uncertainty relations for multiple measurements in multipartite systems and are of basic importance to the potential applications of QMA-EUR in quantum information.

ACKNOWLEDGMENTS

This study was supported by the National Natural Science Foundation of China (Grants No. 12075001, No. 61601002, and No. 12175001), Anhui Provincial Key Research and Development Plan (Grant No. 2022b13020004), and funding from the CAS Key Laboratory of Quantum Information (Grant No. KQI201701).

[1] W. Heisenberg, Z. Phys. **43**, 172 (1927).
[2] I. Bialynicki-Birula and A. Prystupiuk, Phys. Rev. A **103**, 052211 (2021).
[3] E. H. Kennard, Z. Phys. **44**, 326 (1927).
[4] H. P. Robertson, Phys. Rev. **34**, 163 (1929).
[5] I. Bialynicki-Birula *et al.*, Phys. Scr. **T48**, 113 (1993).
[6] I. Białynicki-Birula and J. Mycielski, Commun. Math. Phys. **44**, 129 (1975).
[7] D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
[8] K. Kraus, Phys. Rev. D **35**, 3070 (1987).
[9] H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
[10] J. M. Renes and J. C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).
[11] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).
[12] M. A. Nielson and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2002).
[13] M. L. Hu and H. Fan, Phys. Rev. A **86**, 032338 (2012).
[14] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Phys. Rev. A **90**, 052327 (2014).
[15] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[16] C. S. Yu, Phys. Rev. A **95**, 042337 (2017).
[17] V. Giovannetti, S. Lloyd, and L. Maccone, Nat. Photonics **5**, 222 (2011).
[18] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Phys. Rev. Lett. **98**, 140402 (2007).
[19] K. Sun, X. J. Ye, Y. Xiao, X. Y. Xu, Y. C. Wu, J. S. Xu, J. L. Chen, C. F. Li, and G. C. Guo, npj Quantum Inf. **4**, 12 (2018).
[20] J. Schneeloch, C. J. Broadbent, S. P. Walborn, E. G. Cavalcanti, and J. C. Howell, Phys. Rev. A **87**, 062103 (2013).
[21] J. M. Renes and J. C. Boileau, Phys. Rev. A **78**, 032335 (2008).
[22] J. M. Renes and M. M. Wilde, IEEE Trans. Inf. Theory **60**, 3090 (1995).
[23] G. Jaeger, A. Shimony, and L. Vaidman, Phys. Rev. A **51**, 54 (1995).
[24] D. Wang, F. Ming, M. L. Hu, and L. Ye, Ann. Phys. (Berlin) **531**, 1900124 (2019).
[25] M. A. Ballester and S. Wehner, Phys. Rev. A **75**, 022319 (2007).
[26] S. Wu, S. Yu, and K. Mølmer, Phys. Rev. A **79**, 022104 (2009).
[27] A. K. Pati, M. M. Wilde, A. R. Usha Devi, A. K. Rajagopal, and Sudha, Phys. Rev. A **86**, 042105 (2012).
[28] T. Pramanik, S. Mal, and A. S. Majumdar, Quantum Inf. Process **15**, 981 (2016).
[29] M. L. Hu and H. Fan, Phys. Rev. A **87**, 022314 (2013).
[30] T. Pramanik, P. Chowdhury, and A. S. Majumdar, Phys. Rev. Lett. **110**, 020402 (2013).
[31] L. Maccone and A. K. Pati, Phys. Rev. Lett. **113**, 260401 (2014).
[32] P. J. Coles and M. Piani, Phys. Rev. A **89**, 022112 (2014).
[33] Ł. Rudnicki, Z. Puchala, and K. Życzkowski, Phys. Rev. A **89**, 052115 (2014).
[34] S. Zozor, G. M. Bosyk, and M. Portesi, J. Phys. A: Math. Theor. **47**, 495302 (2014).
[35] Ł. Rudnicki, Phys. Rev. A **91**, 032123 (2015).
[36] J. Zhang, Y. Zhang, and C. S. Yu, Sci. Rep. **5**, 11701 (2015).
[37] S. Liu, L. Z. Mu, and H. Fan, Phys. Rev. A **91**, 042133 (2015).
[38] F. Adabi, S. Salimi, and S. Haseli, Phys. Rev. A **93**, 062123 (2016).
[39] J. L. Huang, W. C. Gan, Y. L. Xiao, F. W. Shu, and M. H. Yung, Eur. Phys. J. C **78**, 545 (2018).
[40] D. Wang, F. Ming, X. K. Song, L. Ye, and J. L. Chen, Eur. Phys. J. C **80**, 800 (2020).
[41] B. F. Xie, F. Ming, D. Wang, L. Ye, and J. L. Chen, Phys. Rev. A **104**, 062204 (2021).
[42] L. J. Li, F. Ming, X. K. Song, L. Ye, and D. Wang, Eur. Phys. J. C **82**, 726 (2022).
[43] R. Prevedel, D. R. Hamel, R. Colbeck, K. Fisher, and K. J. Resch, Nat. Phys. **7**, 757 (2011).
[44] C. F. Li, J. S. Xu, X. Y. Xu, K. Li, and G. C. Guo, Nat. Phys. **7**, 752 (2011).
[45] W. C. Ma, Z. H. Ma, H. Y. Wang, Z. H. Chen, Y. Liu, F. Kong, Z. K. Li, X. H. Peng, M. J. Shi, F. Z. Shi, S. M. Fei, and J. F. Du, Phys. Rev. Lett. **116**, 160405 (2016).
[46] Z. X. Chen, J. L. Li, Q. C. Song, H. Wang, S. M. Zangi, and C. F. Qiao, Phys. Rev. A **96**, 062123 (2017).
[47] W. M. Lv, C. Zhang, X. M. Hu, H. Cao, J. Wang, Y. F. Huang, B. H. Liu, C. F. Li, and G. C. Guo, Phys. Rev. A **98**, 062337 (2018).
[48] H. Y. Wang, Z. H. Ma, S. J. Wu, W. Q. Zheng, Z. Cao, Z. H. Chen, Z. K. Li, S. M. Fei, X. H. Peng, V. Vedral, and J. F. Du, npj Quantum Inf. **5**, 39 (2019).
[49] Z. X. Chen, H. Wang, J. L. Li, Q. C. Song, and C. F. Qiao, Sci. Rep. **9**, 5687 (2019).

[50] W. M. Lv, C. Zhang, X. M. Hu, Y. F. Huang, H. Cao, J. Wang, Z. B. Hou, B. H. Liu, C. F. Li, and G. C. Guo, Sci. Rep. **9**, 8748 (2019).

[51] Z. Y. Ding, H. Yang, D. Wang, H. Yuan, J. Yang, and L. Ye, Phys. Rev. A **101**, 032101 (2020).

[52] F. Ming, D. Wang, X. G. Fan, W. N. Shi, L. Ye, and J. L. Chen, Phys. Rev. A **102**, 012206 (2020).

[53] H. Dolatkhah, S. Haseli, S. Salimi, and A. S. Khorashad, Phys. Rev. A **102**, 052227 (2020).

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