scientific reports

Check for updates

OPEN

Quantum cryptographic resource distillation and entanglement

Minjin Choi & Soojoon Lee✉

We look into multipartite quantum states on which quantum cryptographic protocols including quantum key distribution and quantum secret sharing can be perfectly performed, and define the quantum cryptographic resource distillable rate as the asymptotic rate at which such multipartite state can be distilled from a given multipartite state. Investigating several relations between entanglement and the rate, we show that there exists a multipartite bound entangled state whose quantum cryptographic resource distillable rate is strictly positive, that is, there exists a multipartite entangled state which is not distillable, but can be useful for quantum cryptography such as quantum key distribution and quantum secret sharing.

Entanglement is one of the most significant resources for quantum cryptography. In particular, it has been well known that any pure entangled state can be useful in performing quantum cryptographic protocols, such as quantum key distribution[1] and quantum secret sharing[2]. However, it has also been known that there exist mixed states, called the private states[3–5] or the (genuine) secret sharing states[6,7], which can distill perfectly secure key bits or secret bits for secret sharing just by measurement. We here call such mixed states the *quantum cryptographic resource* (QCR) states. Hence, it can be seen that a QCR state is not only considered as a generalized version of the private state or the genuine secret sharing state, but is also regarded as a resource unit in a quantum cryptographic theory, while a pure maximally entangled state plays a role of a resource unit in entanglement theory.

We consider a general form of the QCR states with one dealer party. In other words, the QCR state that we here deal with is a multipartite quantum state, and a private state on the parties can be obtained from the state by local quantum operations and classical communication (LOCC) so that perfectly secure key distribution is feasible between the dealer party and any player party of the state. In addition, complete secret sharing on any number of divided parties together with the dealer party of the QCR state is also possible, although dishonest players cooperating with any exterior eavesdropper exist. Thus, players can select one quantum cryptographic protocol among various kinds of ones with the dealer on the same QCR state, as they want.

As in any resource theories including entanglement theory, it is both natural and important to take into account the quantity representing how much amount of QCR can be extracted from a given state, which we call the *QCR distillable rate* of the state. We remark that since the simplest QCR state is a maximally entangled state, the QCR distillable rate in entanglement theory is nothing but the distillable entanglement[8], and since the private state is also a simple form of the QCR state, the QCR distillable rate in quantum key distribution is equal to the distillable key rate[3,5,9]. Hence, in this paper, we discover the properties of the QCR distillable rate, and compare the QCR distillable rate with the distillable entanglement and the distillable key rate.

We say that a multipartite state is *QCR distillable* if its QCR distillable rate is strictly positive. Then it is clear that a QCR distillable state is entangled, since if a multipartite state has a separable bipartite split, then perfectly secure key distribution is impossible between the split, and hence the state is not QCR distillable. However, it does not seem to be true that all entangled states are QCR distillable, because its simplest case is not true, that is, there exists a bipartite bound entangled state with positive secret key distillable rate[3,5,9].

In this paper, we first present necessary and sufficient conditions for the QCR state with a dealer party, and definition of the QCR state, and then show that a given multipartite quantum state is a QCR state if and only if the conditions on the state hold. We also define the QCR distillable rate of a given multipartite state in a mathematical way, and present some properties on the QCR distillable rate. Finally, by providing the method to construct a QCR state with larger number of parties from several QCR states, we prove the existence of multipartite bound entangled but QCR distillable states.

This paper is organized as follows. We first define the QCR state, and justify the definition. After showing the several properties of the QCR states, we also present the mathematical definition of the QCR distillable rate of a given state, and investigate some relations between the QCR distillable rate and other distillable rates such as

Department of Mathematics and Research, Institute for Basic Sciences, Kyung Hee University, Seoul 02447, Korea. ✉email: level@khu.ac.kr

the entanglement distillable rate and secret key distillable rate. We finally show that there exists a multipartite QCR distillable state without any distillable entanglement.

Results

QCR states. Assume that there are one dealer and N players who participate in a quantum cryptographic protocol, and let $D = \bar{D}\widetilde{D}$ be the dealer's quantum system with two subsystems $\bar{D}$ of d dimension and $\widetilde{D}$ of arbitrary dimension in the protocol. Similarly, for each $1 \le i \le N$, let $A_i = \bar{A}_i\widetilde{A}_i$ be the i-th player's quantum system with subsystems $\bar{A}_i$ of d dimension and $\widetilde{A}_i$ of arbitrary dimension. Throughout this paper, we denote $\bar{A}_1 \cdots \bar{A}_N$ and $\widetilde{A}_1 \cdots \widetilde{A}_N$ by $\bar{\mathbf{A}}$ and $\widetilde{\mathbf{A}}$, respectively, and denote $\bar{\mathbf{A}}\widetilde{\mathbf{A}}$ by $\mathbf{A}$. The systems $\bar{\mathbf{A}}$ and $\widetilde{\mathbf{A}}$ are called the *information part* and the *shield part*, respectively.

In order to perform the quantum cryptographic protocol, the dealer's and players' information should satisfy the following cryptographic conditions:

(i) The probability distributions of the dealer's and all players' information must be unbiased and perfectly correlated.
(ii) An eavesdropper and dishonest players cannot get any information about the dealer's information.
(iii) The dealer and any subset of players can perform the same protocol with smaller number of parties after properly applying LOCC.

When $N = 1$, if the dealer and the player share the private states[3–5], or when $N \ge 2$, if the dealer and the players share the genuine secret sharing states[7], then the above three conditions are surely satisfied. However, since any player can be a dealer in the private states and the (genuine) secret sharing states, considering the case where the dealer is predetermined is more general than those in the private states and the (genuine) secret sharing states, Thus, we introduce the class of quantum states suitable for the case where the dealer is determined in advance.

Definition 1 $\Upsilon_{D\mathbf{A}}$ is called a *QCR state* if for any bipartite split $\{\mathbf{P}_1, \mathbf{P}_2\}$ of the players with $\mathbf{P}_1$ consisting of at least one player and $\mathbf{A} = \mathbf{P}_1\mathbf{P}_2$, the given state $\Upsilon_{D\mathbf{A}}$ can be written as

$$\frac{1}{d^N} \sum_{iI_1I_2, jJ_1J_2 \in \mathfrak{S}_N^0} |iI_1I_2\rangle_{\bar{D}\bar{\mathbf{P}}_1\bar{\mathbf{P}}_2} \langle jJ_1J_2| \otimes \left(U^{iI_1}_{\widetilde{D}\widetilde{\mathbf{P}}_1} V^{I_2}_{\widetilde{D}\widetilde{\mathbf{A}}}\right) \sigma_{\widetilde{D}\widetilde{\mathbf{A}}} \left(U^{jJ_1}_{\widetilde{D}\widetilde{\mathbf{P}}_1} V^{J_2}_{\widetilde{D}\widetilde{\mathbf{A}}}\right)^\dagger, \tag{1}$$

where

$$\mathfrak{S}_N^t \equiv \left\{ jJ = jj_1j_2 \cdots j_N \in \mathbb{Z}_d^{N+1} : j + \sum_{k=1}^N j_k \equiv t \pmod d \right\}, \tag{2}$$

$\bar{D}\bar{\mathbf{P}}_1\bar{\mathbf{P}}_2 = \bar{D}\bar{\mathbf{A}}$ and $\widetilde{D}\widetilde{\mathbf{A}}$ are the information part and the shield part of the QCR state $\Upsilon_{D\mathbf{A}}$, respectively, $\sigma_{\widetilde{D}\widetilde{\mathbf{A}}}$ is an arbitrary state, and the $\left\{U^{iI_1}_{\widetilde{D}\widetilde{\mathbf{P}}_1}\right\}$ and $\left\{V^{I_2}_{\widetilde{D}\widetilde{\mathbf{A}}}\right\}$ are unitary operators on the systems $\widetilde{D}\widetilde{\mathbf{P}}_1$ and $\widetilde{D}\widetilde{\mathbf{A}}$, respectively.

For instance, let $|\Upsilon\rangle_{\bar{D}\bar{A}\bar{B}\widetilde{D}\widetilde{A}\widetilde{B}}$ be the following state.

$$|\Upsilon\rangle_{\bar{D}\bar{A}\bar{B}\widetilde{D}\widetilde{A}\widetilde{B}} = \frac{1}{2}(|000\rangle_{\bar{D}\bar{A}\bar{B}}|000\rangle_{\widetilde{D}\widetilde{A}\widetilde{B}} + |011\rangle_{\bar{D}\bar{A}\bar{B}}|100\rangle_{\widetilde{D}\widetilde{A}\widetilde{B}} + |101\rangle_{\bar{D}\bar{A}\bar{B}}|100\rangle_{\widetilde{D}\widetilde{A}\widetilde{B}} + |110\rangle_{\bar{D}\bar{A}\bar{B}}|000\rangle_{\widetilde{D}\widetilde{A}\widetilde{B}}). \tag{3}$$

Then we can readily check that the state $\Upsilon_{\bar{D}\bar{A}\bar{B}\widetilde{D}\widetilde{A}\widetilde{B}} = |\Upsilon\rangle\langle\Upsilon|$ is a QCR state, but not a genuine secret sharing state in Reference[7]. Furthermore, when $N = 1$, the QCR state $\Upsilon_{\bar{D}\bar{A}\widetilde{D}\widetilde{A}}$ in Definition 1 can be written as

$$\frac{1}{d} \sum_{i,j \in \mathbb{Z}_d} |i, -i\rangle_{\bar{D}\bar{A}} \langle j, -j| \otimes \left(U^i_{\widetilde{D}\widetilde{A}}\right) \sigma_{\widetilde{D}\widetilde{A}} \left(U^j_{\widetilde{D}\widetilde{A}}\right)^\dagger, \tag{4}$$

which is essentially equivalent to a private state, and all genuine secret sharing states in Reference[7] are QCR states. Hence, the QCR state can be regarded as a generalization of the private states and the genuine secret sharing states with respect to quantum cryptography.

Theorem 1 *Suppose that a dealer and N players share a quantum state $\rho_{D\mathbf{A}}$. The dealer and players can obtain information satisfying the above cryptographic conditions (i) and (ii) after they measure their information parts in the computational basis if and only if the state $\rho_{D\mathbf{A}}$ is a QCR state.*

Theorem 2 *Assume that a dealer D and N players $\mathbf{A}$ share an $(N+1)$-party QCR state. For any bipartite split $\{\mathbf{P}_1, \mathbf{P}_2\}$ of the players $\mathbf{A} = \mathbf{P}_1\mathbf{P}_2$ with $|\mathbf{P}_1| = M \ge 1$, if players $\mathbf{P}_2$ measure their information parts and correctly announce the measurement outcomes, then $D\mathbf{P}_1$ can share an $(M+1)$-party QCR state after the dealer applies a proper unitary operation on the dealer's part.*

Theorem 2 tells us that from a given QCR state, a QCR state on any smaller number of players and the dealer as well as a private state between any player and the dealer can be shared by LOCC, as seen in the Fig. 1. In other words, Theorem 2 implies that any QCR state satisfies the cryptographic condition (iii).

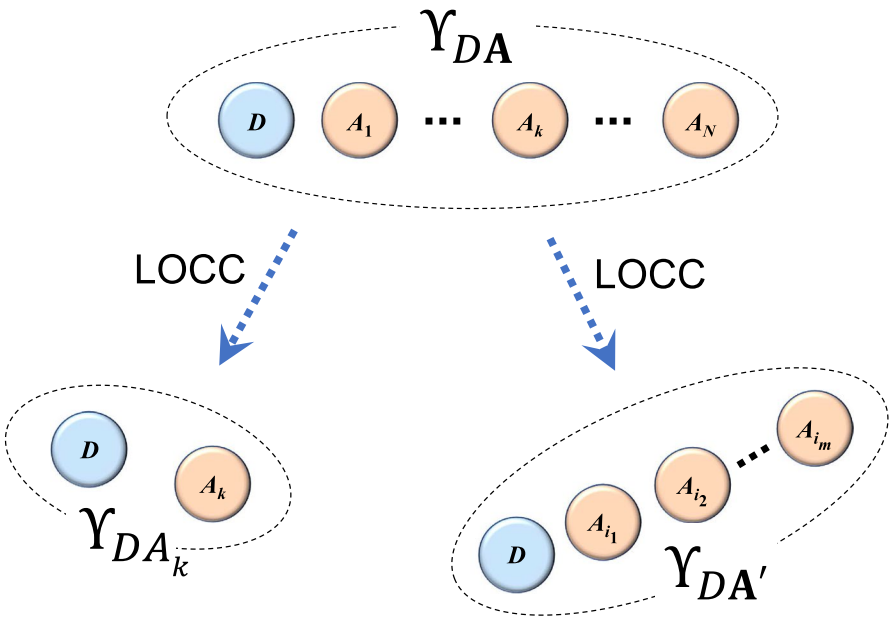

Figure 1. As in Theorem 2, from the $\Upsilon_{D\mathbf{A}}$, a private state Υ_{DA_k} or a QCR state $\Upsilon_{D\mathbf{A}'}$ with smaller number of parties can be obtained by LOCC, where $\mathbf{A}' = A_{i_1}A_{i_2}\cdots A_{i_m}$.

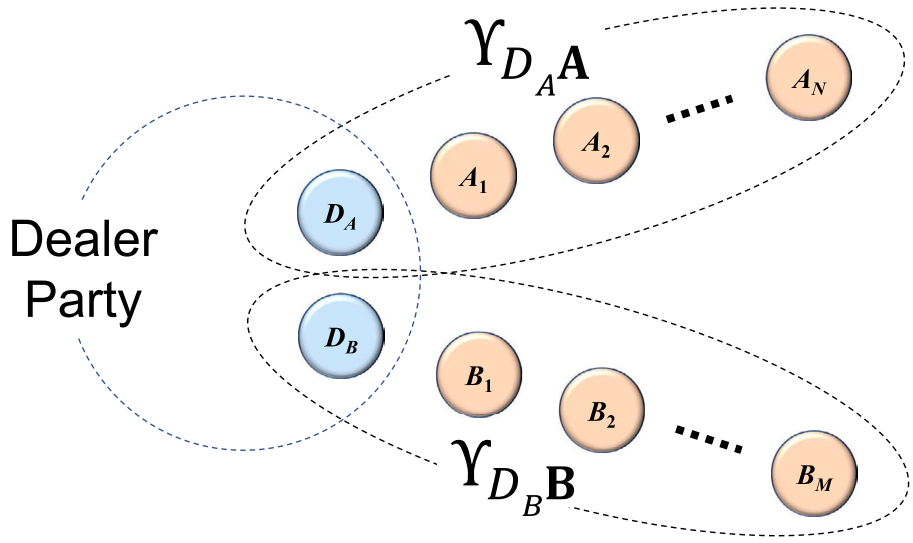

Figure 2. Constructing a QCR state with larger number of parties from two QCR states $\Upsilon_{D_A\mathbf{A}}$ and $\Upsilon_{D_B\mathbf{B}}$ in Theorem 3.

Theorem 3 *Assume that there are two QCR states $\Upsilon_{D_A\mathbf{A}}$ and $\Upsilon_{D_B\mathbf{B}}$, where both D_A and D_B are the dealer's parties, and $\mathbf{A} = A_1\cdots A_N$ and $\mathbf{B} = B_1\cdots B_M$ are two different sets of players. Then the dealer and all players share a QCR state $\Upsilon_{D\mathbf{AB}}$ via the dealer's proper local operations, where $D = D_AD_B$.*

By Theorem 3, we can see that a larger QCR state can be obtained from two different QCR states with the same dealer party as seen in the Fig. 2. Furthermore, we note that the private state is considered as a QCR state with one dealer and one player. Hence, by mathematical induction, we have the following corollary.

Corollary 4 *Suppose that each of N players shares a private state with one dealer. Then they can have an $(N+1)$ -party QCR state by applying the dealer's proper local operations.*

QCR distillable rate and bound entangled states. Before defining the QCR distillable rate, we look at the distillable entanglement and the distillable key rate. Let Φ_{AB}^m and $\gamma_{ABA'B'}^m$ be denoted by the maximally entangled state with $m = \log\dim(A) = \log\dim(B)$ and the private state with $m = \log\dim(A) = \log\dim(B)$, respectively, where $\dim(\cdot)$ is the dimension of the system. The distillable entanglement E_{D} is defined as the rate at which maximally entangled states can be distilled under LOCC[10], that is,

$$E_{\mathrm{D}}(\rho_{AB}) = \lim_{\delta\to 0}\lim_{n\to\infty}\sup_{\Lambda_{A:B}}\left\{E : \|\Lambda\left(\rho_{AB}^{\otimes n}\right) - \Phi_{AB}^{nE}\|_1 \le \delta\right\}, \tag{5}$$

where $\Lambda_{A:B}$ is an LOCC protocol between Alice and Bob. Similarly, the distillable key rate K_{D} is defined as the rate at which private states can be distilled under LOCC[3,5], that is,

$$K_{\mathrm{D}}(\rho_{AB}) = \lim_{\delta\to 0}\lim_{n\to\infty}\sup_{\Lambda_{A:B}}\left\{K : \left\|\Lambda\left(\rho_{AB}^{\otimes n}\right) - \gamma_{AB}^{nK}\right\|_1 \le \delta\right\}. \tag{6}$$

Since we can define the QCR distillable rate for any state in a similar way to the above definitions, from the definition, we can know how many copies of the given state are required to asymptotically distill a QCR state through LOCC. The QCR distillable rate CR_{D} of a given multipartite quantum state $\rho_{D\mathbf{A}}$ is defined as

$$CR_{\mathrm{D}}(\rho_{D\mathbf{A}}) = \lim_{\delta\to 0}\lim_{n\to\infty}\sup_{\Lambda}\left\{K : \left\|\Lambda\left(\rho_{D\mathbf{A}}^{\otimes n}\right) - \Upsilon_{D\mathbf{A}}^{nK}\right\|_1 \le \delta\right\}, \tag{7}$$

where Λ is the dealer's and all players' LOCC operation, and $\Upsilon_{D\mathbf{A}}^m$ denotes a QCR state whose information part $\bar{D}\bar{A}_1\bar{A}_2\cdots\bar{A}_N$ satisfies $m = \log\dim(\bar{D}) = \log\dim(\bar{A}_i)$ for all i.

Let us now investigate the connection between the distillable key rate and the QCR distillable rate. It follows from Theorem 2 that

$$CR_{\mathrm{D}}(\rho_{D\mathbf{A}}) \le K_{\mathrm{D}}^{D\mathbf{P}_1:\mathbf{P}_2}(\rho_{D\mathbf{A}}) \tag{8}$$

for any bipartite split $\{\mathbf{P}_1, \mathbf{P}_2\}$ of the players $\mathbf{A} = \mathbf{P}_1\mathbf{P}_2$. In addition, by Theorem 3, we have the following theorem.

Theorem 5 *Let $\mathbf{A} = A_1\cdots A_N$ and $\mathbf{B} = B_1\cdots B_M$ be two different sets of players, and let D_A and D_B be the dealer's parties. For given two states $\rho_{D_A\mathbf{A}}$ and $\rho_{D_B\mathbf{B}}$,*

$$CR_{\mathrm{D}}\left(\rho_{D_A\mathbf{A}}\otimes\rho_{D_B\mathbf{B}}\right) \ge \min\{\mathrm{CR_D}\left(\rho_{\mathrm{D_A}\mathbf{A}}\right), \mathrm{CR_D}\left(\rho_{\mathrm{D_B}\mathbf{B}}\right)\}. \tag{9}$$

Hence, the following corollary clearly comes from Theorem 5 and Corollary 4.

Corollary 6 *For each $i = 1, 2, \ldots, N$, let $\rho_{D_iA_i}$ be the quantum state shared by the dealer D_i and the i-th player A_i. Then the following inequality holds.*

$$CR_{\mathrm{D}}\left(\bigotimes_{i=1}^{N}\rho_{D_iA_i}\right) \ge \min_{\mathrm{i}}\left\{\mathrm{K_D}(\rho_{\mathrm{D_iA_i}})\right\}. \tag{10}$$

Corollary 6 implies that if each $\rho_{D_iA_i}$ has a positive distillable key rate, then $\bigotimes_{i=1}^N\rho_{D_iA_i}$ has a positive QCR distillable rate. We note that if each $\rho_{D_iA_i}$ is a bipartite state with positive partial transposition (PPT), then $\bigotimes_{i=1}^N\rho_{D_iA_i}$ is also an $(N+1)$-partite state with PPT, since it is a PPT state with respect to any bipartite split of $D\mathbf{A}$ with one dealer $D = D_1D_2\cdots D_N$ and N players $\mathbf{A} = A_1A_2\cdots A_N$. Hence, we can readily construct multipartite PPT bound entangled states with positive QCR distillable rate from bipartite PPT bound entangled states with positive distillable key rate, which are presented in References[5,9]. Therefore, we can finally present our theorem showing the existence of such states as follows.

Theorem 7 *For any natural number $N \ge 2$, there exists an $(N+1)$-partite bound entangled state $\rho_{D\mathbf{A}}$ with $CR_{\mathrm{D}}(\rho_{D\mathbf{A}}) > 0$.*

Discussion

We have defined the QCR state with a dealer party, and have shown that a given multipartite quantum state is a QCR state if and only if the two cryptographic conditions on the state hold. We have also defined the QCR distillable rate of a given multipartite state, and have presented several important properties on the QCR distillable rate. In the sequel, we have presented how to construct a QCR distillable state with larger number of parties from several QCR distillable states. Moreover, we have proved that there exist multipartite bound entangled states which are QCR distillable. This result implies that there exists a multipartite quantum state on which a dealer and players can perform one of several kinds of quantum cryptographic protocols to some extent, and from which they cannot distill any bipartite nor multipartite entanglement by LOCC. Hence, we can conclude that any bipartite or multipartite distillable entanglement is not necessarily required for quantum cryptography.

The QCR states that we have dealt with in this paper have one specific dealer party. Thus several kinds of perfectly secure classical communication feasible on the quantum state can be performed between the dealer party and any number of players. Therefore, the QCR state can be considered as a resource unit in quantum

cryptographic theory, and hence we could construct the quantum cryptographic network consisting of the QCR states instead of the bipartite maximally entangled states or the private states.

Methods

Proof of Theorem 1. This proof is almost the same as that of the theorem related to the genuine secret sharing state in Reference[7]. The details are as follows.

Let us consider the state

$$\left|\Gamma_{\rho}\right\rangle_{\bar{D}\bar{\mathbf{A}}\widetilde{D}\widetilde{\mathbf{A}}E}=\sum_{I\in\mathbb{Z}_d^{N+1}}\sqrt{p_I}|I\rangle_{\bar{D}\bar{\mathbf{A}}}|\psi_I\rangle_{\widetilde{D}\widetilde{\mathbf{A}}E}, \tag{11}$$

which is a purification of $\rho_{D\mathbf{A}}$. Assume that the dealer and players can have cryptographic information that satisfies the cryptographic condition (i) by measuring the information part of $\rho_{D\mathbf{A}}$. Then we have $p_I=1/d^N$ for $I\in\mathfrak{S}_{N+1}^0$ and $p_I=0$ for $I\notin\mathfrak{S}_{N+1}^0$.

Regarding the condition (ii), we first take account of the worst case that all players except one player, say A_k, are dishonest. Then the subsystem $\bar{\mathbf{A}}'=\bar{A}_1\cdots\bar{A}_{k-1}\bar{A}_{k+1}\cdots\bar{A}_N$ is the information part of the dishonest players.

Let i be the dealer's measurement outcome. Then the eavesdropper and dishonest players' state after measurement becomes

$$\gamma^{(i)}_{\bar{\mathbf{A}}'\widetilde{D}\widetilde{\mathbf{A}}E}=\frac{1}{d^{N-1}}\sum_{i_k\in\mathbb{Z}_d}\sum_{\xi,\xi'\in\mathfrak{S}_{N-1}^{-i-i_k}}|\xi\rangle_{\bar{\mathbf{A}}'}\langle\xi'|\otimes\mathrm{tr}_{\widetilde{D}\widetilde{A}_k}\left|\psi_{i,i_k,\xi}\right\rangle_{\widetilde{D}\widetilde{\mathbf{A}}E}\left\langle\psi_{i,i_k,\xi'}\right| \tag{12}$$

if reordering the systems. From the cryptographic condition (ii), we have $\gamma^{(i)}_{\bar{\mathbf{A}}'\widetilde{D}\widetilde{\mathbf{A}}E}=\gamma^{(i')}_{\bar{\mathbf{A}}'\widetilde{D}\widetilde{\mathbf{A}}E}$ for any $i,i'\in\mathbb{Z}_d$. It follows from the Hughston-Jozsa-Wootters theorem[11] that for $i,i_k,i',i'_k\in\mathbb{Z}_d$ with $i+i_k=i'+i'_k\pmod d$, there is a unitary operator $U^{i,i_k\to i',i'_k}_{\widetilde{D}\widetilde{A}_k}$ on the system $\widetilde{D}\widetilde{A}_k$ such that

$$U^{i,i_k\to i',i'_k}_{\widetilde{D}\widetilde{A}_k}\left|\psi_{i,i_k,\xi}\right\rangle_{\widetilde{D}\widetilde{\mathbf{A}}E}=\left|\psi_{i',i'_k,\xi}\right\rangle_{\widetilde{D}\widetilde{\mathbf{A}}E} \tag{13}$$

for all $\xi\in\mathfrak{S}_{N-1}^{-i-i_k}$.

Let $\{\mathbf{P}_1,\mathbf{P}_2\}$ be an arbitrary bipartite split of the players with $\mathbf{P}_1$ consisting of at least one player and $\mathbf{A}=\mathbf{P}_1\mathbf{P}_2$. Without loss of generality, we may assume that $\mathbf{P}_1=A_1\cdots A_M$ and $\mathbf{P}_2=A_{M+1}\cdots A_N$. Then by Eq. (13), it can be shown that if $iI_1I_2=ii_1\cdots i_Mi_{M+1}\cdots i_N\in\mathfrak{S}_{N+1}^0$, then

$$|\psi_{00\cdots0}\rangle_{\mathbf{A}'E}=U^{j_{N-1},i_N}_{\widetilde{D}\widetilde{A}_N}\cdots U^{j_1,i_2}_{\widetilde{D}\widetilde{A}_2}U^{i,i_1}_{\widetilde{D}\widetilde{A}_1}\left|\psi_{ii_1i_2\cdots i_N}\right\rangle_{\mathbf{A}'E}, \tag{14}$$

where $U^{i,j}_{\widetilde{D}\widetilde{A}_k}=U^{i,j\to i+j,0}_{\widetilde{D}\widetilde{A}_k}$ and $j_t\equiv i+i_1+\cdots+i_t\pmod d$. Let $\mathrm{tr}_{\widetilde{D}\widetilde{\mathbf{A}}}(|\psi_{00\cdots0}\rangle\langle\psi_{00\cdots0}|)=\sum_{\mathrm{x}}\lambda_{\mathrm{x}}|\eta_{\mathrm{x}}\rangle_{\mathrm{E}}\langle\eta_{\mathrm{x}}|$ be its spectral decomposition. Then we have

$$\left|\psi_{iI_1I_2}\right\rangle_{\widetilde{D}\widetilde{\mathbf{A}}E}=\sum_x\sqrt{\lambda_x}U^{iI_1}_{\widetilde{D}\widetilde{\mathbf{P}}_1}V^{I_2}_{\widetilde{D}\widetilde{\mathbf{A}}}|\phi_x\rangle_{\widetilde{D}\widetilde{\mathbf{A}}}|\eta_x\rangle_E \tag{15}$$

for some unitary operators $U^{iI_1}_{\widetilde{D}\widetilde{\mathbf{P}}_1}$, $V^{I_2}_{\widetilde{D}\widetilde{\mathbf{A}}}$ and orthonormal set $\{|\phi_x\rangle\}$ for the system $\widetilde{D}\widetilde{\mathbf{A}}$. Therefore, $\rho_{D\mathbf{A}}$ is of the form in Eq. (1).

Conversely, assume that $\rho_{D\mathbf{A}}$ has the form in Eq. (1). Then it can be readily shown that players have cryptographic information that obeys the cryptographic condition (i) after measuring their information parts in the computational basis.

We now show that players' cryptographic information satisfies the condition (ii). Suppose that $\{\mathbf{P}_1,\mathbf{P}_2\}$ is a bipartite split of the players $\mathbf{A}=\mathbf{P}_1\mathbf{P}_2$ with $\mathbf{P}_1$ consisting of at least one player and $\mathbf{P}_2$ representing K dishonest players. Let $\sigma_{\widetilde{D}\widetilde{\mathbf{A}}}=\sum_x\kappa_x|\mu_x\rangle_{\widetilde{D}\widetilde{\mathbf{A}}}\langle\mu_x|$ be a spectral decomposition of $\sigma_{\widetilde{D}\widetilde{\mathbf{A}}}$, and let

$$\left|\varphi_{iI_1I_2}\right\rangle_{\widetilde{D}\widetilde{\mathbf{A}}E}=\sum_x\sqrt{\kappa_x}U^{iI_1}_{\widetilde{D}\widetilde{\mathbf{P}}_1}V^{I_2}_{\widetilde{D}\widetilde{\mathbf{A}}}|\mu_x\rangle_{\widetilde{D}\widetilde{\mathbf{A}}}|\nu_x\rangle_E, \tag{16}$$

where $\{|\nu_x\rangle\}$ forms an orthonormal set for the eavesdropper's system E. Then the state

$$|\Upsilon\rangle_{D\mathbf{P}_1\mathbf{P}_2E}=\frac{1}{\sqrt{d^N}}\sum_{iI_1I_2\in\mathfrak{S}_{N+1}^0}|iI_1\rangle_{\bar{D}\bar{\mathbf{P}}_1}|I_2\rangle_{\bar{\mathbf{P}}_2}\left|\varphi_{iI_1I_2}\right\rangle_{\widetilde{D}\widetilde{\mathbf{A}}E} \tag{17}$$

is a purification of $\rho_{D\mathbf{A}}$. If the dealer has the measurement outcome i after measuring the dealer's information part in the computational basis, then the quantum state of dishonest players and eavesdropper after the measurement becomes

$$\Upsilon^{(i)}_{\mathbf{P}_2E}=\frac{1}{d^K}\sum_{\alpha\in\mathbb{Z}_d}\sum_{I_2,J_2\in\mathfrak{S}_K^{-\alpha}}|I_2\rangle_{\bar{\mathbf{P}}_2}\langle J_2|\otimes\mathrm{tr}_{\widetilde{D}\widetilde{\mathbf{P}}_1}\left|\varphi_{I_2}\right\rangle_{\widetilde{D}\widetilde{\mathbf{P}}E}\left\langle\varphi_{J_2}\right|, \tag{18}$$

where $\left|\varphi_{I_2}\right\rangle_{\widetilde{D}\widetilde{\mathbf{P}}E}=\sum_x\sqrt{\kappa_x}V^{I_2}_{\widetilde{D}\widetilde{\mathbf{P}}}|\xi_x\rangle_{\widetilde{D}\widetilde{\mathbf{P}}}|e_x\rangle_E$. Since $\Upsilon^{(i)}_{\mathbf{P}_2E}=\Upsilon^{(j)}_{\mathbf{P}_2E}$ for any $i,j\in\mathbb{Z}_d$, dishonest players and eavesdropper cannot get any information about the dealer's cryptographic information.

Proof of Theorem 2. The proof of Theorem 2 is also similar to that of the theorem associated with the genuine secret sharing states in Reference[7]. However, we here present its simple proof compared to that in Reference[7] as follows.

Without loss of generality, we may assume that $\mathbf{P}_1 = A_1 \cdots A_M$ and $\mathbf{P}_2 = A_{M+1} \cdots A_N$. Let $\Upsilon_{D\mathbf{A}}$ be an $(N+1)$ -party QCR state shared by a dealer and N players. Since $\Upsilon_{D\mathbf{A}}$ has the form in Eq. (1), if let $I_2 \in \mathfrak{S}_{N-M}^{\beta}$ be the measurement outcomes for some β when players $\mathbf{P}_2$ measure their information parts in the computational basis, then the resulting state of the dealer D and the players $\mathbf{P}_1$ after the measurement becomes

$$\Upsilon_{D\mathbf{P}_1}^{(I_2)} = \frac{1}{d^M} \sum_{iI_1, jJ_1 \in \mathfrak{S}_{M+1}^{-\beta}} |iI_1\rangle_{\bar{D}\bar{\mathbf{P}}_1} \langle jJ_1| \otimes U_{\bar{D}\bar{\mathbf{P}}_1}^{iI_1} \tilde{\sigma}_{\tilde{D}\tilde{\mathbf{P}}_1} \left(U_{\tilde{D}\tilde{\mathbf{P}}_1}^{jJ_1}\right)^{\dagger}, \tag{19}$$

where $\tilde{\sigma}_{\tilde{D}\tilde{\mathbf{P}}_1} = \mathrm{tr}_{\tilde{\mathbf{P}}_2} \tilde{V}_{\tilde{D}\tilde{\mathbf{A}}}^{I_2} \sigma_{\tilde{D}\tilde{\mathbf{A}}} \left(\tilde{V}_{\tilde{D}\tilde{\mathbf{A}}}^{I_2}\right)^{\dagger}$.

We note that unitary operators on the shield part of the state $\Upsilon_{D\mathbf{A}}$ can be expressed as in Eq. (14), and it can be easily shown that $W_{\bar{D}} \Upsilon_{D\mathbf{P}_1}^{(I_2)} W_{\bar{D}}^{\dagger}$ is an $(M+1)$-party QCR state, where $W = \sum_{i=0}^{d-1} |i+\beta\rangle\langle i|$. Therefore, if the players $\mathbf{P}_2$ announces the value β, then the dealer D and the players $\mathbf{P}_1$ can share the $(M+1)$-party QCR state after applying the unitary operator W on the dealer's information part.

Proof of Theorem 3. Let

$$|\Upsilon\rangle_{D_A\mathbf{A}E_A} = \frac{1}{\sqrt{d^N}} \sum_{iI \in \mathfrak{S}_{N+1}^0} |iI\rangle_{\bar{D}_A\bar{\mathbf{A}}} \otimes |\psi_{iI}\rangle_{\tilde{D}_A\tilde{\mathbf{A}}E_A} \tag{20}$$

be a purification of the QCR state $\Upsilon_{D_A\mathbf{A}}$, and let

$$|\Upsilon\rangle_{D_B\mathbf{B}E_B} = \frac{1}{\sqrt{d^M}} \sum_{jJ \in \mathfrak{S}_{M+1}^0} |jJ\rangle_{\bar{D}_B\bar{\mathbf{B}}} \otimes |\phi_{jJ}\rangle_{\tilde{D}_B\tilde{\mathbf{B}}E_B} \tag{21}$$

be a purification of the QCR state $\Upsilon_{D_B\mathbf{B}}$. For $I = i_1 i_2 \cdots i_L \in \mathbb{Z}_d^L$, let $|I|$ be defined as $|I| = i_1 + \cdots + i_L$. Then the states $|\Upsilon\rangle_{D_A\mathbf{A}E_A}$ and $|\Upsilon\rangle_{D_B\mathbf{B}E_B}$ in Eqs. (20) and (21) can be rewritten as

$$|\Upsilon\rangle_{D_A\mathbf{A}E_A} = \frac{1}{\sqrt{d^N}} \sum_{I \in \mathbb{Z}_d^N} |-|I|, I\rangle_{\bar{D}_A\bar{\mathbf{A}}} \otimes |\psi_{-|I|,I}\rangle_{\tilde{D}_A\tilde{\mathbf{A}}E_A} \tag{22}$$

and

$$|\Upsilon\rangle_{D_B\mathbf{B}E_B} = \frac{1}{\sqrt{d^M}} \sum_{J \in \mathbb{Z}_d^M} |-|J|, J\rangle_{\bar{D}_B\bar{\mathbf{B}}} \otimes |\phi_{-|J|,J}\rangle_{\tilde{D}_B\tilde{\mathbf{B}}E_B} \tag{23}$$

respectively.

Let cX be the unitary operator defined as

$$cX = \sum_{j,k=0}^{d-1} |j+k, k\rangle\langle j, k|. \tag{24}$$

If the dealer applies the unitary operator $cX_{\bar{D}_A\bar{D}_B}$ on the system $\bar{D}_A\bar{D}_B$ in the state $|\Upsilon\rangle_{D_A\mathbf{A}E_A} \otimes |\Upsilon\rangle_{D_B\mathbf{B}E_B}$, then after properly rearranging the order of the systems, the state becomes

$$\frac{1}{\sqrt{d^{N+M}}} \sum_{I \in \mathbb{Z}_d^N} \sum_{J \in \mathbb{Z}_d^M} |-|I| - |J|, I, J\rangle_{\bar{D}_A\bar{\mathbf{A}}\bar{\mathbf{B}}} \otimes |-|J|\rangle_{\bar{D}_B} \otimes |\psi_{-|I|,I}\rangle_{\tilde{D}_A\tilde{\mathbf{A}}E_A} \otimes |\phi_{-|J|,J}\rangle_{\tilde{D}_B\tilde{\mathbf{B}}E_B}. \tag{25}$$

We remark that if the dealer and all players measure their information part $\bar{D}_A\bar{\mathbf{A}}\bar{\mathbf{B}}$ in the computational basis, then they have cryptographic information that satisfies the cryptographic condition (i). In order to show that the cryptographic information obeys the cryptographic condition (ii), we consider the worst case as in the proof of Theorem 1.

Let us assume that the dealer measures the information part $\bar{D}_A$, and let i be the dealer's measurement outcome. By tracing out the system $\bar{D}_A\bar{D}_B\tilde{D}_A\tilde{D}_B$ of the resulting state, we have

$$\frac{1}{d^{N+M-1}} \sum_{\alpha \in \mathbb{Z}_d} \sum_{I,I' \in \mathfrak{S}_N^{\alpha}} \sum_{J,J' \in \mathfrak{S}_M^{-\alpha-i}} |I,J\rangle_{\bar{\mathbf{A}}\bar{\mathbf{B}}}\langle I',J'| \otimes \mathrm{tr}_{\tilde{D}_A} |\psi_{-\alpha,I}\rangle_{\tilde{D}_A\tilde{\mathbf{A}}E_A}\langle \psi_{-\alpha,I'}| \otimes \mathrm{tr}_{\tilde{D}_B} |\phi_{\alpha+i,J}\rangle_{\tilde{D}_B\tilde{\mathbf{B}}E_B}\langle \phi_{\alpha+i,J'}|. \tag{26}$$

Let us now consider the situation where all players except the dealer and one player are dishonest as the worst case. Without loss of generality, we may assume that the honest player is A_1, by symmetry. When $N \geq 2$, after tracing out the system A_1, the dishonest players and eavesdropper's state becomes

$$\frac{1}{d^{N+M-1}}\sum_{\alpha,\beta\in\mathbb{Z}_d}\sum_{\hat{I},\hat{I}'\in\mathfrak{S}_{N-1}^{\alpha-\beta}}\sum_{J,J'\in\mathfrak{S}_M^{-\alpha-i}}\left|\hat{I}\right\rangle_{\hat{\mathbf{A}}}\left\langle\hat{I}'\right|\otimes|J\rangle_{\bar{\mathbf{B}}}\langle J'|\otimes\mathrm{tr}_{\widetilde{D}_A\widetilde{A}_1}\left|\psi_{-\alpha,\beta,\hat{I}}\right\rangle_{\widetilde{D}_A\widetilde{\mathbf{A}}E_A}\left\langle\psi_{-\alpha,\beta,\hat{I}'}\right|\otimes\mathrm{tr}_{\widetilde{D}_B}\left|\phi_{\alpha+i,J}\right\rangle_{\widetilde{D}_B\widetilde{\mathbf{B}}E_B}\left\langle\phi_{\alpha+i,J'}\right|, \tag{27}$$

where $\hat{I}=i_2\cdots i_L\in\mathbb{Z}_d^{L-1}$ for $I=i_1i_2\cdots i_L\in\mathbb{Z}_d^L$ and $\hat{\mathbf{A}}=\bar{A}_2\cdots\bar{A}_L$ for $\bar{\mathbf{A}}=\bar{A}_1\bar{A}_2\cdots\bar{A}_L$. Since $\Upsilon_{D_A\mathbf{A}}$ is a QCR state,

$$\mathrm{tr}_{\widetilde{D}_A\widetilde{A}_1}\left|\psi_{-\alpha,\beta,\hat{I}}\right\rangle_{\widetilde{D}_A\widetilde{\mathbf{A}}E_A}\left\langle\psi_{-\alpha,\beta,\hat{I}'}\right|=\mathrm{tr}_{\widetilde{D}_A\widetilde{A}_1}\left|\psi_{0,\beta-\alpha,\hat{I}}\right\rangle_{\widetilde{D}_A\widetilde{\mathbf{A}}E_A}\left\langle\psi_{0,\beta-\alpha,\hat{I}'}\right| \tag{28}$$

for any $\alpha,\beta\in\mathbb{Z}_d$ and $\hat{I},\hat{I}'\in\mathfrak{S}_{N-1}^{\alpha-\beta}$. Hence, the state in Eq. (27) can be rewritten as

$$\frac{1}{d^{N+M-1}}\sum_{s,t\in\mathbb{Z}_d}\sum_{\hat{I},\hat{I}'\in\mathfrak{S}_{N-1}^{s}}\sum_{J,J'\in\mathfrak{S}_M^{t}}\left|\hat{I}\right\rangle_{\hat{\mathbf{A}}}\left\langle\hat{I}'\right|\otimes|J\rangle_{\bar{\mathbf{B}}}\langle J'|\otimes\mathrm{tr}_{\widetilde{D}_A\widetilde{A}_1}\left|\psi_{0,-s,\hat{I}}\right\rangle_{\widetilde{D}_A\widetilde{\mathbf{A}}E_A}\left\langle\psi_{0,-s,\hat{I}'}\right|\otimes\mathrm{tr}_{\widetilde{D}_B}\left|\phi_{-t,J}\right\rangle_{\widetilde{D}_B\widetilde{\mathbf{B}}E_B}\left\langle\phi_{-t,J'}\right|. \tag{29}$$

We can here see that the state in Eq. (29) is independent on the dealer's measurement outcome *i*. In other words, the dealer's cryptographic information is perfectly secure against the dishonest players and any exterior eavesdropper, which implies that the dealer's and all players' cryptographic information satisfies the cryptographic condition (ii).

Now assume that $N=1$, that is, $\mathbf{A}=A_1$. Then the state of the dishonest players $\mathbf{B}$ and eavesdropper E_AE_B after the dealer's measurement is

$$\frac{1}{d^M}\sum_{\alpha\in\mathbb{Z}_d}\sum_{J,J'\in\mathfrak{S}_M^{-\alpha-i}}|J\rangle_{\bar{\mathbf{B}}}\langle J'|\otimes\mathrm{tr}_{\widetilde{\mathrm{D}}_\mathrm{A}\widetilde{\mathbf{A}}}\left|\psi_{-\alpha,\alpha}\right\rangle_{\widetilde{\mathrm{D}}_\mathrm{A}\widetilde{\mathbf{A}}\mathrm{E}_\mathrm{A}}\left\langle\psi_{-\alpha,\alpha}\right|\otimes\mathrm{tr}_{\widetilde{\mathrm{D}}_\mathrm{B}}\left|\phi_{\alpha+\mathrm{i},\mathrm{J}}\right\rangle_{\widetilde{\mathrm{D}}_\mathrm{B}\widetilde{\mathbf{B}}\mathrm{E}_\mathrm{B}}\left\langle\phi_{\alpha+\mathrm{i},\mathrm{J}'}\right|, \tag{30}$$

where the dealer's measurement outcome is *i*. Since

$$\mathrm{tr}_{\widetilde{\mathrm{D}}_\mathrm{A}\widetilde{\mathbf{A}}}\left|\psi_{-\alpha,\alpha}\right\rangle_{\widetilde{\mathrm{D}}_\mathrm{A}\widetilde{\mathbf{A}}\mathrm{E}_\mathrm{A}}\left\langle\psi_{-\alpha,\alpha}\right|=\mathrm{tr}_{\widetilde{\mathrm{D}}_\mathrm{A}\widetilde{\mathbf{A}}}\left|\psi_{0,0}\right\rangle_{\widetilde{\mathrm{D}}_\mathrm{A}\widetilde{\mathbf{A}}\mathrm{E}_\mathrm{A}}\left\langle\psi_{0,0}\right| \tag{31}$$

for all $\alpha\in\mathbb{Z}_d$, the state in Eq. (30) does not depend on the measurement outcome *i*, and hence the cryptographic information is perfectly secure against the dishonest players and any exterior eavesdropper.

Let $|\Upsilon\rangle_{D\mathbf{A}\mathbf{B}E}$ be the pure state in Eq. (25), which is the resulting state after the dealer applies the unitary operator $cX_{\bar{D}_A\bar{D}_B}$ on the system $\bar{D}_A\bar{D}_B$ in the state $|\Upsilon\rangle_{D_A\mathbf{A}E_A}\otimes|\Upsilon\rangle_{D_B\mathbf{B}E_B}$, where $D=D_AD_B$ and $E=E_AE_B$. Then, for any cases, the cryptographic information from the state $|\Upsilon\rangle_{D\mathbf{A}\mathbf{B}E}$ obeys the cryptographic conditions (i) and (ii). Therefore, the state $cX_{\bar{D}_A\bar{D}_B}\left(\Upsilon_{D_A\mathbf{A}}\otimes\Upsilon_{D_B\mathbf{B}}\right)cX_{\bar{D}_A\bar{D}_B}^\dagger$ is an $(N+M+1)$-party QCR state by Theorem 1, since the state is equal to $\mathrm{tr}_\mathrm{E}|\Upsilon\rangle_{\mathrm{D}\mathbf{A}\mathbf{B}\mathrm{E}}\langle\Upsilon|$.

Proof of Theorem 5. We first note that the set of all LOCC operations $\Lambda_{D\mathbf{A}\mathbf{B}}$ on the dealer $D=D_AD_B$ and all players $\mathbf{AB}$ contains LOCC operations of the form $\Lambda_{D_A\mathbf{A}}\otimes\Lambda_{D_B\mathbf{B}}$. Hence, $CR_\mathrm{D}\left(\rho_{D_A\mathbf{A}}\otimes\rho_{D_B\mathbf{B}}\right)$ is lower bounded by

$$\lim_{\delta\to0}\lim_{n\to\infty}\sup_{U_D}\sup_{\Lambda_{D_A\mathbf{A}},\Lambda_{D_B\mathbf{B}}}\left\{K:\left\|U_D\left(\Lambda_{D_A\mathbf{A}}\left(\rho_{D_A\mathbf{A}}^{\otimes n}\right)\otimes\Lambda_{D_B\mathbf{B}}\left(\rho_{D_B\mathbf{B}}^{\otimes n}\right)\right)U_D^\dagger-\Upsilon_{D\mathbf{A}\mathbf{B}}^{nK}\right\|_1\le\delta\right\}, \tag{32}$$

where U_D's are unitary operators acting on the system D. In addition, as seen in the proof of Theorem 3, there exists a unitary operator $\bar{U}_D$ such that

$$\bar{U}_D\left(\Upsilon_{D_A\mathbf{A}}^{nK}\otimes\Upsilon_{D_B\mathbf{B}}^{nK}\right)\bar{U}_D^\dagger=\Upsilon_{D\mathbf{A}\mathbf{B}}^{nK}. \tag{33}$$

Then it follows from Eq. (33) that

$$\left\|\bar{U}_D\left(\Lambda_{D_A\mathbf{A}}\left(\rho_{D_A\mathbf{A}}^{\otimes n}\right)\otimes\Lambda_{D_B\mathbf{B}}\left(\rho_{D_B\mathbf{B}}^{\otimes n}\right)\right)\bar{U}_D^\dagger-\Upsilon_{D\mathbf{A}\mathbf{B}}^{nK}\right\|_1=\left\|\Lambda_{D_A\mathbf{A}}\left(\rho_{D_A\mathbf{A}}^{\otimes n}\right)\otimes\Lambda_{D_B\mathbf{B}}\left(\rho_{D_B\mathbf{B}}^{\otimes n}\right)-\Upsilon_{D_A\mathbf{A}}^{nK}\otimes\Upsilon_{D_B\mathbf{B}}^{nK}\right\|_1. \tag{34}$$

By the telescoping property of the trace distance[12,13], that is,

$$\|\sigma_1\otimes\sigma_2-\tau_1\otimes\tau_2\|_1\le\|\sigma_1-\tau_1\|_1+\|\sigma_2-\tau_2\|_1, \tag{35}$$

we can see that the lower bound on $CR_\mathrm{D}\left(\rho_{D_A\mathbf{A}}\otimes\rho_{D_B\mathbf{B}}\right)$ in Eq. (32) is also lower bounded by

$$\lim_{\delta\to0}\lim_{n\to\infty}\sup_{\Lambda_{D_A\mathbf{A}},\Lambda_{D_B\mathbf{B}}}\left\{K:\left\|\Lambda_{D_A\mathbf{A}}\left(\rho_{D_A\mathbf{A}}^{\otimes n}\right)-\Upsilon_{D_A\mathbf{A}}^{nK}\right\|_1\le\frac{\delta}{2},\left\|\Lambda_{D_B\mathbf{B}}\left(\rho_{D_B\mathbf{B}}^{\otimes n}\right)-\Upsilon_{D_B\mathbf{B}}^{nK}\right\|_1\le\frac{\delta}{2}\right\}, \tag{36}$$

which is greater than or equal to both $CR_\mathrm{D}\left(\rho_{D_A\mathbf{A}}\right)$ and $CR_\mathrm{D}\left(\rho_{D_B\mathbf{B}}\right)$. This completes the proof, that is,

$$CR_\mathrm{D}\left(\rho_{D_A\mathbf{A}}\otimes\rho_{D_B\mathbf{B}}\right)\ge\min\{\mathrm{CR_D}\left(\rho_{\mathrm{D_A}\mathbf{A}}\right),\mathrm{CR_D}\left(\rho_{\mathrm{D_B}\mathbf{B}}\right)\}. \tag{37}$$

Received: 15 September 2021; Accepted: 14 October 2021
Published online: 26 October 2021

References

1. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
2. Hillery, M., Bužek, V. & Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **59**, 1829 (1999).
3. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. Secure key from bound entanglement. *Phys. Rev. Lett.* **94**, 160502 (2005).
4. Horodecki, P. & Augusiak, R. Quantum states representing perfectly secure bits are always distillable. *Phys. Rev. A* **74**, 010302 (2006).
5. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. General paradigm for distilling classical key from quantum states. *IEEE Trans. Inf. Theory* **55**, 1898 (2009).
6. Chi, D. P., Choi, J. W., Kim, J. S., Kim, T. & Lee, S. Quantum states for perfectly secure secret sharing. *Phys. Rev. A* **78**, 012351 (2008).
7. Choi, M. & Lee, S. Genuine secret-sharing states. *Quantum Inf. Process.* **20**, 47 (2021).
8. Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. & Wootters, W. K. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54**, 3824–3850 (1996).
9. Chi, D. P., Choi, J. W., Kim, J. S., Kim, T. & Lee, S. Bound entangled states with a nonzero distillable key rate. *Phys. Rev. A* **78**, 012351 (2007).
10. Bennett, C. H. *et al.* Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.* **76**, 722–725 (1996).
11. Hughston, L. P., Jozsa, R. & Wootters, W. K. A complete classification of quantum ensembles having a given density matrix. *Phys. Rev. A* **183**, 14–18 (1993).
12. Wilde, M.M. *From Classical to Quantum Shannon Theory* (2011). arXiv:1106.1445.
13. Wilde, M. M. *Quantum Information Theory* (Cambridge University Press, 2017).

Acknowledgements

This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Science and ICT (MSIT) (Grants No. NRF-2019R1A2C1006337 and No. NRF-2020M3E4A1079678). S.L. acknowledges support from the MSIT, Korea, under the Information Technology Research Center support program (Grant No. IITP-2021-2018-0-01402) supervised by the Institute for Information and Communications Technology Planning and Evaluation, and the Quantum Information Science and Technologies program of the NRF funded by the MSIT (Grant No. 2020M3H3A1105796).

Author contributions

M.C. and S.L. conceived the idea. M.C. performed the calculations and the proofs, and S.L. checked them. M.C. wrote the main manuscript. and S.L. improved the manuscript. All authors contributed to the discussion and reviewed the manuscript.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to S.L.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.