Editors' Suggestion

Quantum Secure Direct Communication with Private Dense Coding Using a General Preshared Quantum State

Jiawei Wu,[1,2] Gui-Lu Long,[1,3,4,5,*] and Masahito Hayashi[2,6,7,8,†]

[1] *State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China*
[2] *Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China*
[3] *Beijing National Research Center for Information Science and Technology, Beijing 100084, China*
[4] *Innovative Center of Quantum Matter, Beijing 100084, China*
[5] *Beijing Academy of Quantum Information Science, Beijing 100193, China*
[6] *International Quantum Academy (SIQA), Shenzhen 518048, China*
[7] *Guangdong Provincial Key Laboratory of Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China*
[8] *Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan*

(Received 31 December 2021; revised 10 March 2022; accepted 21 April 2022; published 6 June 2022)

We study quantum secure direct communication using a general preshared quantum state and a generalization of dense coding. In this scenario, Alice is allowed to apply a unitary operation on the preshared state to encode her message, and the set of allowed unitaries forms a group. To decode the message, Bob is allowed to apply a measurement across his system and the system he receives. In the worst scenario, we guarantee that Eve obtains no information for the message even when Eve accesses the joint system between the system that she intercepts and her original system of the preshared state. For a practical application, we propose a concrete protocol and derive an upper bound of information leakage in the finite-length setting. We also discuss how to apply our scenario to the case with discrete Weyl-Heisenberg representation when the preshared state is unknown.

DOI: 10.1103/PhysRevApplied.17.064011

I. INTRODUCTION

Dense coding is known as an attractive quantum information protocol. While the original study considers the noiseless setting [1], many subsequent studies extended this result to more general settings [2–7]. However, all of them focused only on the communication speed in various noisy settings. While dense coding with the noiseless setting realizes twice the communication speed, it also realizes quantum secure direct communication (QSDC) as follows [8]. In dense coding, the sender, Alice, and the receiver, Bob, share perfect Bell states and Alice encodes her message by application of a unitary. Since Alice's local state is a completely mixed state, the eavesdropper, Eve, cannot obtain any information about the message even when Eve intercepts the transmitted quantum state. However, it is not easy to prepare a perfect Bell state between Alice and Bob. In fact, when we apply entanglement distillation or entanglement concentration [9–12], we can generate a perfect Bell state or its approximation. Such entanglement distillation operations can be combined with conventional quantum key distribution (QKD) [13–15]. However, such operations require extra quantum operations in addition to quantum operations for QSDC. Hence, it is preferable to find a protocol to realize secure communication without generating a perfect Bell state. Since secure information transmission over quantum channels is one of major topics in quantum information, it is more important to investigate secure communication via dense coding in a realistic noisy setting. Of course, QSDC can also be realized without dense coding [16–18].

In addition, the preceding studies [2,3,6] allowed Alice to use any quantum operation on a single input system. However, implementing arbitrary quantum operations even on a single quantum system is difficult and unnecessary. From a practical viewpoint, it is sufficient to restrict allowed quantum operations to only a subset of unitaries. Since a combination of several possible unitaries is also available, it is natural that such a subset forms a group G. When the message-encoding operations are limited to a subgroup of unitary operators, the limit of information

*gllong@mail.tsinghua.edu.cn
†hayashi@sustech.edu.cn

transmission has been studied by exploiting the resource theory of asymmetry [3,5,7,19–25]. However, their analyses did not cover the secrecy analysis. Therefore, it is desirable to investigate secure information transmission via preshared entanglement in the framework of the resource theory of asymmetry. On the other hand, many existing studies [2,3,6,26–29] addressed the asymptotic analysis, which shows only the transmission rate. However, no upper bound or finite-length effect for this setting were given. In this paper, we derive an upper bound for information leakage under a finite-length practical code and the corresponding asymptotic transmission rate.

Now, we present our communication model in detail. Alice and Bob are assumed to share n copies of a quantum state τ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, and Eve has her own system $\mathcal{H}_E$ correlated to the above state. Hence, their total state is n copies of a quantum state τ_{ABE}. To send her message, Alice is allowed to apply unitaries from the set $\{U_g\}_{g\in G}$, where U_g forms a projective unitary representation on $\mathcal{H}_A$ of a group G. Then, after the application of her unitaries, Alice sends her encoded system to Bob. In the worst case, Eve intercepts the transmitted quantum system via a noiseless channel and keeps it. If the transmitted state is not intercepted, Bob receives the quantum system as the output of n times use of a certain quantum channel Λ_A. Bob decodes the message from the joint system composed of his original system and his receiving system. Finally, to check the correct decoding, Alice and Bob apply the error verification. If the verification fails, the communication aborts.

In this scenario, we have two requirements. The first is completeness, in which, the communication aborts with low probability when the transmitted state is not intercepted and the channel from Alice to Bob is the channel Λ_A. The second is soundness, which is composed of secrecy and reliability. Even when Eve intercepts the transmitted quantum system via a noiseless channel, the amount of information leakage to Eve is negligible [secrecy; see (S1) below]. Here information leakage is evaluated using the trace distance. If the communication does not abort, Bob can recover the message correctly with high probability [reliability; see (S2) below].

Although QKD is also required to satisfy these requirements [30–33], our method is different from QKD in the following point. Our method requires a prior shared quantum state, but QKD does not require it. Because of this difference, our method has the following advantages. In QKD, Eve can intercept all the states sent by Alice and the state information leaks out inevitably. Because of this possibility, QKD can be used only for random number distribution and cannot be used for sending messages. However, in our model, even when Eve intercepts the quantum channel from Alice to Bob, Eve cannot obtain any information about Alice's message while Bob cannot recover it.

To satisfy reliability, Alice and Bob apply error verification, which requires a negligible amount of secure keys shared by Alice and Bob [34, Section VIII]. This method allows Bob to verify whether he can recover the message correctly. Hence, if the above two conditions of soundness are satisfied, even if Bob cannot recover the message, Alice and Bob can repeat the same procedure because there is no information leakage. Therefore, the above pair of requirements is reasonable.

Indeed, some existing papers studied a similar problem setting [8,35–38],[39, Chapter 7] and proposed a corresponding coding scheme [40,41]. However, their analysis is limited to the asymptotic analysis in a special example, and did not cover the finite-length setting or the general case. Some of the above studies employed the classical-quantum (CQ) wire-tap channel model [26,27,42,43], which is a quantum analogue of the wire-tap channel model [44–46] and is composed of two channels: the CQ channel W_B from Alice to Bob and the CQ channel W_E from Alice to Eve. In the above scenario, we discuss the channel W_E to guarantee secrecy [(S1) below], and the channel W_B to guarantee the reliability requirement [(S2) below]. Using the wire-tap channel model, we derive an achievable transmission rate dependently of the shared entangled state and the channel from Alice to Bob. This achievable transmission rate is given as the difference between the error correcting rate and the sacrificed rate. In addition, we derive finite-length evaluations dependently of the error correcting rate and the sacrificed rate. In the evaluation of information leakage, we derive a finite-length bound for information leakage for the quantum wire-tap channel.

Usually, to achieve the above transmission rate, the receiver is required to apply measurement across many received quantum systems. Such a measurement is called a collective measurement and its implementation is quite difficult. However, when all encoded states on the joint system consisting of a received system and a memory system on Bob's side are commutative, the above rate can be achieved without the use of a collective measurement. That is, when Bob applies a specific measurement on each joint system, the given achievable rate can be attained by a combination of classical encoding and decoding operations by Alice and Bob. In addition, when group G is a vector space over a finite field, such classical encoding and decoding have calculation complexity $O(n \log n)$, where n is the coding block length. Under this type of coding, we derive formulae for secrecy and reliability dependently of the block length n and the sacrificed rate. In this way, our results are useful in practical cases.

Here, we emphasize that, while the preceding studies [37,38],[39,Chapter 7] simply applied the wire-tap channel model to their problem setting, our protocol is not a simple application of the wire-tap channel model. In fact, when Eve receives the output of W_E, Bob cannot receive the output of W_B. That is, Bob can decode the message only when Eve does not receive the output of W_E. Therefore, Bob needs to check whether Eve intercepts the transmitted system. Indeed, such an additional step is not needed if the channel is given as a broadcast channel, as in the preceding studies [47–49]. To this end, while the existing studies [8,35–38,40,41],[39, Chapter 7] did not consider the error verification, we propose a protocol to combine the conventional wire-tap code and the error verification.

In the next step, we apply our general results to the case when the unitary operation is given as the Weyl-Heisenberg representation and the preshared state is the Bell diagonal state, which is almost the same as the setting of quantum secure direct communication in Refs. [8,50]. Such a preshared state can be generated by distributing a Bell state over a Pauli channel. Then, we numerically calculate the asymptotic transmission rate. Also, to clarify the finite-length effect, we make numerical plots for the sacrificed rate, error correcting rate, and the transmission rate as a function of the coding block length n when we fix other parameters. Furthermore, in a realistic case, the preshared entangled state is not necessarily known. To cover this case, we propose another protocol to include the estimation process. This protocol is designed so that it works well even when the preshared entangled state is not necessarily a Bell diagonal state.

Indeed, our setting covers various situations beyond the above example. For example, our method can be applied to the case in which Alice, Bob, and Eve share correlated classical variables, as discussed in Refs. [51, Section VI],[52,53]. More generally, it is possible to apply it to the case in which Alice and Bob share correlated classical variables and Eve has a correlated quantum state [54]. Such a situation can be realized when Eve makes a collective attack in QKD and Alice and Bob estimate Eve's attack operation perfectly. In addition, recent research [7, Section IV] presented three other interesting quantum examples for a pair comprising a group G and an entangled state. Our method can be applied to the noisy situations in these examples. These cases show the generality of our problem setting.

The remaining part of this paper is organized as follows. Section II summarizes our results for a general model of private dense coding with a preshared state. Section III applies these general results to the case with Weyl-Heisenberg representation. Section IV presents our protocol for the unknown preshared state in the above setting. Section V discusses the modular code for a quantum wire-tap channel, and derives a finite-length evaluation for information leakage for a quantum wire-tap channel. Section VI describes the error verification process. Section VII gives a practical code construction with a vector space over a finite field. Section VIII discusses our results. Appendix D proposes an estimation method for a Bell diagonal state using one-way local operation and classical communication (LOCC). This estimation method works even for the general unknown state, though it is designed for the Bell diagonal state.

II. PRIVATE DENSE CODING MODEL

A. General model description

Assume that Alice, Bob, and Eve share n copies of the quantum state τ_{ABE} on the system $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$. We consider a (projective) unitary group representation of a finite group G on $\mathcal{H}_A$. That is, for $g \in G$, we have a unitary operator U_g such that, for $g, g' \in G$, there exists a complex number $c(g, g')$ satisfying

$$U_g U_{g'} = c(g, g') U_{gg'}. \tag{1}$$

When $c(g, g')$ is 1, $\{U_g\}_{g \in G}$ is called a unitary group representation. Otherwise, it is called a projective group representation. We also consider a quantum channel from Alice to Bob, which is a trace preserving completely positive (TP-CP) map $\Lambda_A : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_{B'})$, where $\mathcal{D}(\mathcal{H})$ expresses the set of density operators on the system $\mathcal{H}$. Then, we impose the group covariance condition to channel Λ_A as

$$\Lambda_A(U_g \rho U_g^\dagger) = U_g \Lambda_A(\rho) {U_g}^\dagger \quad \text{for all } g \in G \text{ and all } \rho \in \mathcal{D}(\mathcal{H}). \tag{2}$$

Initial state τ_{ABE}, available operation set $\{U_g\}$, and channel Λ_A constitute a private dense coding setting $\mathrm{PDC}(\tau_{ABE}, \{U_g\}_{g \in G}, \Lambda_A)$.

Our task is the secure transmission of message $M \in \mathcal{M}$ from Alice to Bob by using n copies of their shared state under the following conditions. Alice is allowed to freely communicate to Bob via a public channel. Alice can apply a unitary U_g for $g \in G$ on her local states and sends it to Bob; after Bob receives the quantum systems sent by Alice, he acknowledges the fact. This task has the following criteria.

(C) *Completeness.*—The PDC protocol is ϵ_C complete if the error verification aborts with probability no larger than ϵ_C when the state is not intercepted and the channel from Alice to Bob is exactly Λ_A.

(S) *Soundness.*—This part is composed of two conditions.

(S1) *Secrecy.*—The PDC protocol is ϵ_E secure if the amount of the information leakage to Eve is upper bounded by ϵ_E even in the worst case, i.e., when Eve intercepts the whole transmitted quantum state via a noiseless channel.

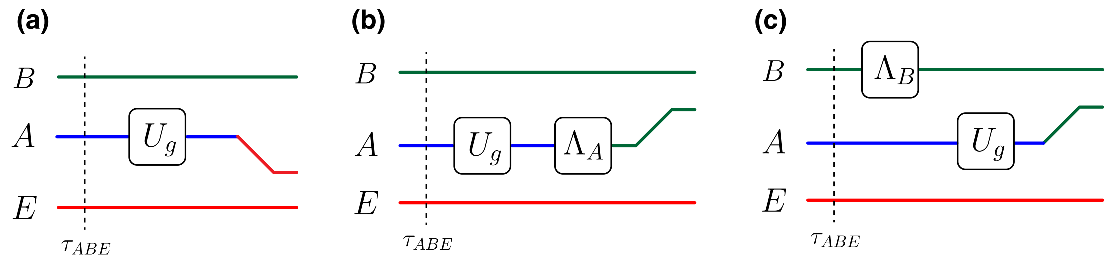

FIG. 1. An illustration of the basic setting of private dense coding with a general preshared state. (a) In the worst case, the encoded state is intercepted by Eve. (b) Without interception by Eve, Bob receives Alice's state through channel Λ_A. (c) The case when there exists a channel Λ_B such that $\Lambda_A(\tau_{AB}) = \Lambda_B(\tau_{AB})$.

The information leakage is evaluated by

$$d(M,\bar{E})_{\tau_{M\bar{E},f}} := \min_{\sigma_{\bar{E}}} \|\tau_{M\bar{E},f} - P_{\mathcal{M}} \otimes \sigma_{\bar{E},f}\|_1, \quad (3)$$

where $\bar{E}$ expresses all the systems that Eve obtains during the protocol, including the intercepted system A; $\tau_{M\bar{E},f}$ expresses the final state of our protocol; and $P_{\mathcal{M}}$ is the uniform distribution for message M.

(S2) *Reliability.*—The PDC protocol is ϵ_B reliable if the relation $M = \hat{M}$ holds with significance level ϵ_B, where M is Alice's original message and $\hat{M}$ expresses Bob's recovered message. The significance level is the probability of accepting the hypothesis to be shown, given that the hypothesis is assumed to be incorrect. Now, Ab is the event that Bob aborts the protocol, so that Ab^c is the event that Bob does not abort the protocol. Hence, $\Pr[\mathrm{Ab}^c|M = m, \hat{M} = \hat{m}]$ expresses the probability that Bob does not abort the protocol when Alice's original message and Bob's recovered message are m and $\hat{m}$, respectively. Then, the above condition is rewritten as $\sup_{m\neq\hat{m}} \Pr[\mathrm{Ab}^c|M = m, \hat{M} = \hat{m}] \leq \epsilon_B$.

For a given protocol P_n for private dense coding with n copies of $\tau_{ABE}^{\otimes n}$, its parameters ϵ_C, ϵ_E, and ϵ_B are denoted by $\epsilon_C(P_n)$, $\epsilon_E(P_n)$, and $\epsilon_B(P_n)$, respectively. Also, the rate of message $\log|\mathcal{M}|/n$ is denoted by $R(P_n)$. In this setting, soundness is more important than completeness because soundness shows the quality of our private communication when it is successful. Hence, the parameter of completeness ϵ_C is not required to be too small. For the parameter of completeness ϵ_C, the value $1 - \epsilon_C$ is called a power in the context of statistical hypothesis testing. While there is no definite value for the power, Cohen [55] suggested 0.8 as a conventional level, which corresponds to the choice $\epsilon_C = 0.2$. However, a larger power (i.e., smaller ϵ_C) can be chosen in practice. The reason is the following. Consider the case when Alice and Bob abort the protocol mistakenly while it runs without Eve's interception. They can run the same protocol again until it is successful. In contrast, the two parameters ϵ_E and ϵ_B of soundness need to be very small rigorously. Hence, the two parameters ϵ_E and ϵ_B are called security parameters because they express our confidence level.

B. Protocol with a finite-length setting

In Sec. VII A we construct our PDC protocol by combining the wire-tap code and error verification. Since the cost of error verification is negligible, it is sufficient to consider the cost for the wire-tap code. That is, we focus on a CQ wire-tap channel model [26,27,42,43], where the channel W_B to Bob is the CQ channel $g(\in G) \mapsto W_B(g) := \Lambda_A(U_g\tau_{AB}U_g^\dagger) = U_g\Lambda_A(\tau_{AB})U_g{}^\dagger$, and the channel W_E to Eve is the CQ channel $g(\in G) \mapsto W_E(g) := U_g\tau_{AE}U_g^\dagger$.

For n copies of the state τ_{ABE}, combining wire-tap codes and error verification with the parameters R_1, R_2, and t, in Sec. VII A we construct a PDC protocol P_n of private dense coding such that $R(P_n) = R_1 - R_2 - \mathsf{t}/n$ and

$$\epsilon_C(P_n) \leq 4 \min_{0\leq t\leq 1} 2^{tn[R_1 - \log d_A + H^{\downarrow}_{1-t}(A|B|\Lambda_A(\tau_{AB}))]}, \quad (4)$$

$$\epsilon_E(P_n) \leq \min_{0\leq t\leq 1} 2^{-2t/(1+t)} 2^{[tn/(1+t)][-R_2 + \log d_A - \tilde{H}^{\uparrow}_{1+t}(A|E|\tau_{AE})]}, \quad (5)$$

$$\epsilon_B(P_n) \leq 2^{-\mathsf{t}}, \quad (6)$$

where d_A is the dimension of $\mathcal{H}_A$. Here, R_1 and R_2 are called the error correcting rate and the sacrificed rate for secrecy, respectively, and t is called the sacrificed length for reliability. In the above formulae, two types of Rényi conditional entropies $H^{\downarrow}_{1-t}(A|B|\Lambda_A(\tau_{AB}))$ and $\tilde{H}^{\uparrow}_{1+t}(A|E|\tau_{AE})$ are used:

$$H^{\downarrow}_{1+t}(A|B|\rho_{AB}) := -D_{1+t}(\rho_{AB}\|I_A \otimes \rho_B), \quad (7)$$

$$\tilde{H}^{\uparrow}_{1+t}(A|B|\rho_{AB}) := -\inf_{\sigma_B\in\mathcal{D}(\mathcal{H}_B)} \tilde{D}_{1+t}(\rho_{AB}\|I_A \otimes \sigma_B). \quad (8)$$

Here I is the identity operator and we put the measured quantum state as the last entry of information quantities. The Petz version [56] and the sandwiched version [57,58] of quantum relative entropy are defined as follows. For $t \in (-1, \infty)$,

$$D_{1+t}(\rho\|\sigma) := \frac{1}{t}\log \mathrm{Tr}\rho^{1+t}\sigma^{-t}, \tag{9}$$

$$\tilde{D}_{1+t}(\rho\|\sigma) := \frac{1}{t}\log \mathrm{Tr}(\rho^{-t/2(1+t)}\sigma\rho^{-t/2(1+t)})^{1+t}. \tag{10}$$

The sandwiched form is always no larger than the Petz form according to the Araki-Lieb-Thirring trace inequality [59]. In the $t = 0$ case, the above quantities are defined by taking the limit $t \to 0$, which is exactly $D(\rho\|\sigma) := \mathrm{Tr}\rho(\log\rho - \log\sigma)$. Hence, $\lim_{t\to 0} H^{\downarrow}_{1+t}(A|B|\rho_{AB}) = \lim_{t\to 0}\tilde{H}^{\uparrow}_{1+t}(A|B|\rho_{AB}) = H(A|B|\rho) := H(AB|\rho) - H(B|\rho)$, where $H(AB|\rho) = -\mathrm{Tr}\rho_{AB}\log\rho_{AB}$ and $H(B|\rho) = -\mathrm{Tr}\rho_B \log\rho_B$.

In addition, as explained in Sec. V, when the following conditions hold, it is possible to make a PDC protocol with small calculation complexity.

(B1) The group G forms a vector space over a finite field $\mathbb{F}_q$.

(B2) The states $\{U_g\Lambda_A(\tau_{AB})U_g^{\dagger}\}_{g\in G}$ are commutative with each other.

C. Asymptotic setting

In the asymptotic setting of the PDC model, we impose the condition $\epsilon_C(P_n), \epsilon_E(P_n), \epsilon_B(P_n) \to 0$ as $n \to \infty$ for a sequence of PDC protocols $\{P_n\}$ from a theoretical viewpoint. Under the above condition, the rate $\lim_{n\to\infty} R(P_n)$ is called an achievable private rate for a private dense coding setting $\mathrm{PDC}(\tau_{ABE}, \{U_g\}_{g\in G}, \Lambda_A)$. The supremum of achievable private rates is called the private capacity for $\mathrm{PDC}(\tau_{ABE}, \{U_g\}_{g\in G}, \Lambda_A)$, and is written as $C(\tau_{ABE}, \{U_g\}_{g\in G}, \Lambda_A)$. As stated as Lemma 4 below, the capacity of the above wire-tap channel model (W_E, W_B) equals the private capacity for $\mathrm{PDC}(\tau_{ABE}, \{U_g\}_{g\in G}, \Lambda_A)$. However, the capacity of the wire-tap channel does not have a known single-letterized expression while the classical setting has [45]. Hence, we consider an achievable private rate R_* by using Eqs. (4), (5), and (6). To this end, we define the map $\mathcal{G}$ as $\mathcal{G}(\rho) := \sum_{g\in G} U_g\rho U_g^{\dagger}/|G|$.

Since $\lim_{t\to 0} H^{\downarrow}_{1-t}(A|B|\Lambda_A(\tau_{AB})) - \log d_A$ equals

$$\begin{aligned} R_{1,*} &:= H(\Lambda_A \circ \mathcal{G}(\tau_{AB})) - H(\Lambda_A(\tau_{AB})) \\ &= H(\mathcal{G}(\Lambda_A(\tau_{AB}))) - H(\Lambda_A(\tau_{AB})), \end{aligned} \tag{11}$$

the parameter $\epsilon_C(P_n)$ goes to zero with $R_1 < R_{1,*}$. Similarly, since $\lim_{t\to 0}\tilde{H}^{\uparrow}_{1+t}(A|E|\tau_{AE}) - \log d_A$ equals

$$R_{2,*} = H(\mathcal{G}(\tau_{AE})) - H(\tau_{AE}), \tag{12}$$

the parameter $\epsilon_E(P_n)$ goes to zero with $R_2 > R_{2,*}$. When $\mathsf{t} = \sqrt{n}$, $\epsilon_B(P_n)$ and t/n go to zero. Hence, the following is an achievable private rate:

$$\begin{aligned} R_* = {} & H(\mathcal{G}(\Lambda_A(\tau_{AB}))) - H(\Lambda_A(\tau_{AB})) - H(\mathcal{G}(\tau_{AE})) \\ & + H(\tau_{AE}). \end{aligned} \tag{13}$$

In fact, the above achievable rate can be considered as the difference between two mutual information terms. When we denote the choice of an element $g \in G$ by the random variable X, Eqs. (11) and (12) become $R_{1,*} = I(X; BB'), R_{2,*} = I(X; AE)$ and the achievable private rate of the above wire-tap channel model is given as $I(X; BB') - I(X; AE)$ [26,27,42,43].

D. Asymptotic analysis with the noiseless channel

For further analysis, we assume that Λ_A is the noiseless channel and $\{U_g\}_{g\in G}$ is irreducible. Then the rates $R_*, R_{1,*}$, and $R_{2,*}$ are simplified to

$$\begin{aligned} & R_{1,*} = \log d_A - H(A|B)_\tau, \quad R_{2,*} = \log d_A - H(A|E)_\tau, \\ & R_* = H(A|E)_\tau - H(A|B)_\tau \end{aligned} \tag{14}$$

because $H(\mathcal{G}(\tau_{AB})) = H(I_A/d_A \otimes \tau_B) = \log d_A + H(\tau_B)$, $H(\mathcal{G}(\tau_{AE})) = H(I_A/d_A \otimes \tau_E) = \log d_A + H(\tau_E)$, where $d_A := \dim \mathcal{H}_A$. Here, $H(A|E)_\tau$ expresses the conditional entropy when the density matrix is τ_{AE}. When the total state τ_{ABE} is a pure state and Λ_A is the noiseless channel, we have the relations $H(\tau_{AE}) = H(\tau_B)$ and $H(\tau_{AB}) = H(\tau_E)$. Hence, the rate R_* is simplified to

$$R_* = 2(H(\tau_{A,E}) - H(\tau_E)) = 2H(A|E)_\tau = -2H(A|B)_\tau. \tag{15}$$

In fact, as shown in Appendix A, when Λ_A is the noiseless channel, τ_{ABE} is a pure state, and τ_{AB} is maximally correlated, i.e., there exist bases $|v_j^A\rangle$ and $|v_j^B\rangle$ on $\mathcal{H}_A$ and $\mathcal{H}_B$ such that $\tau_{AB} = \sum_{j,j'} a_{j,j'}|v_j^A, v_j^B\rangle\langle v_{j'}^A, v_{j'}^B|$, then the above CQ wire-tap channel W_B, W_E is degraded [42,60], i.e., there exists a TP-CP map Γ such that $W_E(g) = \Gamma(W_B(g))$. In this case, as shown in Corollary 3 below, due to the group symmetric condition, quantity (15) gives the private capacity of our PDC model, i.e., the maximum secure transmission rate.

Here, we should remark on the relation with the method studied in the preceding research [61]. Devetak and Winter [61] considered the secure key distillation from a preshared state τ_{ABE} with the same condition as in this subsection. They showed that their one-way method achieves the key generation rate $H(A|E)_\tau$. However, since our method is allowed to use quantum communication from Alice to Bob, it achieves twice their rate.

E. Reduction to the noiseless case

In the latter part of the above subsection, we assumed that the channel Λ_A is noiseless. When our model with noisy channel Λ_A satisfies the following condition, its analysis can be reduced to the case with the noiseless channel.

(A1) There exists a TP-CP map Λ_B on $\mathcal{H}_B$ such that $\Lambda_A(\tau_{AB}) = \Lambda_B(\tau_{AB})$.

Indeed, the reliability of PDC$(\tau_{ABE}, \{U_g\}, \Lambda_A)$ is equivalent to the reliability of PDC$(\Lambda_B(\tau_{ABE}), \{U_g\}, \mathrm{id}_A)$ because the reduced state of $\Lambda_B(\tau_{ABE})$ to $\mathcal{H}_A \otimes \mathcal{H}_B$ equals $\Lambda_A(\tau_{AB})$, where id_A is the identical channel. The secrecy is also equivalent because the reduced state of τ_{ABE} to $\mathcal{H}_A \otimes \mathcal{H}_E$ equals the reduced state of $\Lambda_B(\tau_{ABE})$ to $\mathcal{H}_A \otimes \mathcal{H}_E$. Therefore, the analysis with preshared state τ_{ABE} and noisy channel Λ_A is reduced to the analysis with preshared state $\Lambda_B(\tau_{ABE})$ and the noiseless channel.

III. APPLICATION TO THE WEYL-HEISENBERG REPRESENTATION

A. PDC model with Weyl-Heisenberg representation

In this section, we discuss the private dense coding with preshared state with Weyl-Heisenberg representation. That is, the dimension of space $\mathcal{H}_A$ is a prime $d_A = p$, the group G is the Weyl-Heisenberg group $\mathbb{F}_p^2$, and the group representation is given as a set of implementable operations as follows. In addition, the rate R_* can be achieved by a protocol with small calculation complexity, as explained below. The $\mathbf{X}$ and $\mathbf{Z}$ operators on the p-dimensional quantum system are defined as

$$\mathbf{W}(x,z) = \mathbf{X}^x\mathbf{Z}^z,$$
$$\mathbf{X} = \sum_{j\in\mathbb{F}_p} |j+1\rangle\langle j|,$$
$$\mathbf{Z} = \sum_{j\in\mathbb{F}_p} \omega^j |j\rangle\langle j|,$$

with $\omega = e^{i2\pi/p}$. In this case, the private dense coding with preshared state is the same as the protocol discussed in Refs. [37,50].

As a typical noise model, we employ a generalized Pauli channel acting on a d-dimensional quantum system defined as

$$\Lambda[P_{XZ}](\rho) = \sum_{(x,z)\in\mathbb{F}_p^2} P_{XZ}(x,z)\mathbf{W}(x,z)\rho\mathbf{W}(x,z)^\dagger. \quad (16)$$

That is, we assume that the preshared state is generated by transmission of a maximally entangled state $|\Phi\rangle = (1/\sqrt{p})\sum_i |i\rangle_A|i\rangle_B$ from Bob to Alice via the channel $\Lambda[P_{XZ}]$ acting on $\mathcal{H}_A$. In this case, the joint state τ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$ is given as the generalized Bell diagonal state

$$\rho[P_{XZ}] := \sum_{(x,z)\in\mathbb{F}_p^2} P_{XZ}(x,z)\mathbf{W}(x,z)|\Phi\rangle\langle\Phi|\mathbf{W}(x,z)^\dagger. \quad (17)$$

To guarantee the secrecy under the worst case, we assume that Eve controls all the environment of channel $\Lambda[P_{XZ}]$. Hence, the state on system $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ is the pure state $\tau_{ABE} = |\Psi\rangle\langle\Psi|$, i.e., the purification of $\rho[P_{XZ}]$, which is given as

$$|\Psi\rangle_{ABE} = \frac{1}{\sqrt{d}}\sum_{x,z}\sqrt{P(x,z)}\mathbf{W}(x,z)|\Phi\rangle_{AB}|x,z\rangle_E. \quad (18)$$

Also, channel Λ_A from Alice to Bob is given as another generalized Pauli channel $\Lambda_A[\tilde{P}_{XZ}]$. That is, we focus on private dense coding PDC$(|\Psi\rangle, \{\mathbf{W}(x,z)\}, \Lambda[\tilde{P}_{XZ}]_A)$ as depicted in Fig. 2, where $(x,z) \in \mathbb{F}_p^2$ by default. Since we have

$$\Lambda[\tilde{P}_{X,Z}]_A \circ \Lambda[P_{XZ}]_A(|\Phi\rangle\langle\Phi|)$$
$$= \Lambda[\tilde{P}_{-X,Z}]_B \circ \Lambda[P_{XZ}]_A(|\Phi\rangle\langle\Phi|), \quad (19)$$

we can alternatively apply the model PDC$(\omega_{ABE}, \{\mathbf{W}(x,z)\}, \mathrm{id}_A)$, where $\omega_{ABE} := \Lambda[\tilde{P}_{-X,Z}]_B(|\Psi\rangle\langle\Psi|)$.

In the private dense coding model PDC$(\omega_{ABE}, \{\mathbf{W}(x,z)\}, \mathrm{id}_A)$, it can be shown that the state received by Bob is always Bell diagonal (see Appendix B), i.e., condition (B2) holds. Therefore, Bob can extract information via the

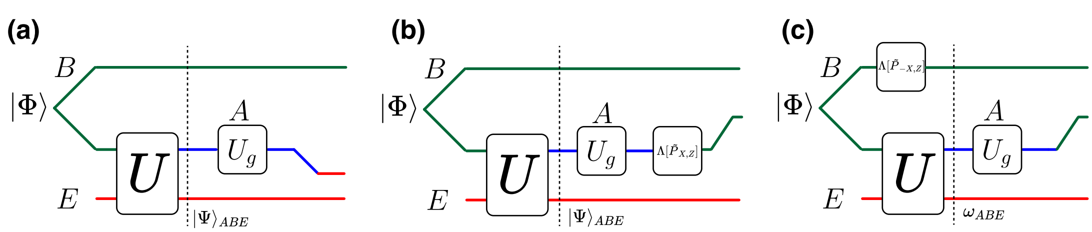

FIG. 2. An illustration of the setting PDC$(|\Psi\rangle, \{\mathbf{W}(x,z)\}, \Lambda[\tilde{P}_{XZ}]_A)$. Here U is the unitary that reduces to the Pauli channel $\Lambda[P_{XZ}]$ by tracing out system E. Entanglement distribution is done via the application of the unitary U to the maximally entangled state. The output state of the above entanglement distribution is $|\Psi\rangle_{ABE}$. (a) In the worst case, Alice's state is intercepted by Eve through a noiseless channel. (b) Without interception by Eve, Bob receives Alice's state through channel $\Lambda[\tilde{P}_{X,Z}]$. (c) The noiseless reduction of the original setting.

measurement $\Pi_{x,z} = \text{Proj}(\mathbf{W}(x,z)|\Phi\rangle)$ without any state demolition. Once this measurement is applied, the channel from Alice to Bob is given as a classical channel W^c, which is given as $W^c(x,z|x',z') := (\tilde{P}_{XZ} * P_{XZ})(x-x', z-z')$, where the convolution $\tilde{P}_{XZ} * P_{XZ}$ is defined by

$$\tilde{P}_{XZ} * P_{XZ}(x,z) := \sum_{x'z'} \tilde{P}_{XZ}(x',z') P_{XZ}(x-x', z-z'). \tag{20}$$

That is, Bob can apply classical decoding to channel W^c without any information loss.

Since group G forms a vector space over a finite field $\mathbb{F}_p$ and the states received by Bob are commutative with each other in the above way, conditions (B1) and (B2) are satisfied so that the rate R_* can be achieved by a protocol with small calculation complexity. For this model, we have the following lemma, whose proof is given in Appendix C.

Lemma 1. *The key information quantities in the setting* $\text{PDC}(\omega_{ABE}, \{\mathbf{W}(x,z)\}, \text{id}_A)$ *can be expressed as*

$$H(A|B)_\omega = H(XZ|\tilde{P}_{XZ} * P_{XZ}) - \log d_A, \tag{21}$$

$$H(A|E)_\omega = \log d_A - H(XZ|P_{XZ}), \tag{22}$$

$$\tilde{H}^{\downarrow}_{1-t}(A|B)_\omega = H_{1-t}(\tilde{P}_{XZ} * P_{XZ}) - \log d_A, \tag{23}$$

$$\tilde{H}^{\uparrow}_{1+t}(A|E)_\omega \geq \log d_A - H_{1/(1+t)}(P_{XZ}), \tag{24}$$

where $H_{1+t}(\rho) := -D_{1+t}(\rho\|I)$.

By applying Eqs. (21) and (22) to Eqs. (11), (12), and (13), the rates $R_*, R_{1,*}$, and $R_{2,*}$ are calculated as

$$R_{1,*} = 2\log d_A - H(\tilde{P}_{XZ} * P_{XZ}), \tag{25}$$

$$R_{2,*} = H(P_{XZ}), \tag{26}$$

$$R_* = 2\log d_A - H(P_{XZ}) - H(\tilde{P}_{XZ} * P_{XZ}). \tag{27}$$

B. Application of the PDC protocol

High-dimensional QSDC [50] is similar to our PDC model. As its generalization, we propose the following protocol based on our PDC model. The aim of the following protocol is that Alice transmits her message $M \in \mathcal{M} := \mathbb{F}_p^{n_2}$ to Bob using two quantum channels, i.e., $\Lambda[P_{XZ}]$ from Bob to Alice and $\Lambda[\tilde{P}_{XZ}]$ from Alice to Bob, and a free public channel in both directions. In the following scenario, Bob distributes quantum states via $\Lambda[P_{XZ}]$ initially. Next, Alice sends back the received system to Bob via $\Lambda[\tilde{P}_{XZ}]$ after her coding operation. While we assume that there is no possibility that channel $\Lambda[P_{XZ}]$ from Bob to Alice is changed or intercepted, Eve is assumed to receive the environment of channel $\Lambda[P_{XZ}]$. That is, by using a unitary U from $\mathcal{H}_B$ to $\mathcal{H}_A \otimes \mathcal{H}_E$ whose reduction to $\mathcal{H}_A$ is $\Lambda[P_{XZ}]$, the transmission process from Bob to Alice is regarded as the application of the unitary U, and Eve has the system $\mathcal{H}_E$ of the output of the unitary U. In addition, we consider that Eve intercepts the second quantum communication from Alice to Bob in the worst case. Because of the above assumption, completeness (C) and soundness (S) can be applied to this problem setting in the same way as the PDC model.

To state our protocol, we prepare a classical error correcting code $\varphi = (\varphi_e, \varphi_d)$ for n uses of the classical channel W^c with decoding error probability $\epsilon(\varphi)$, where φ_e is a classical linear encoder that maps $\mathbb{F}_p^{n_1}$ to a linear subspace $\mathcal{L}$ of $\mathbb{F}_p^{2n}$, and φ_d is a classical decoder that maps $\mathbb{F}_p^{2n}$ to $\mathbb{F}_p^{n_1}$. Here, n_1 is called the coding length of the code φ. Then, we prepare the message set $\mathcal{M} := \mathbb{F}_p^{n_2}$, the set for covering variable $\mathcal{Y} := \mathbb{F}_p^{n_3}$, which will be used to cover the message in error verification, the message set for wire-tap code $\mathcal{M}' := \mathcal{Y} \times \mathcal{M} = \mathbb{F}_q^{n_2+n_3}$, and two sets of random seeds $\mathcal{S} := \mathbb{F}_p^{n_1-1}$, $\mathcal{S}' := \mathbb{F}_p^{n_2+n_3-1}$. We prepare two universal hash function (UHF) families $f_S : \mathbb{F}_p^{n_1} \to \mathcal{M}'$ and $g_{S'} : \mathcal{M}' \to \mathcal{Y}$, which are defined in Eqs. (64) and (65) below, respectively. Then, combining the encoder of classical error correcting code φ_e and random seed S, we define the function ψ_S in Eq. (66) below. Under the above preparation, we propose Protocol 1, which is also illustrated in Fig. 3.

Protocol 1.

Entanglement distribution: *Bob starts the protocol by generating n entangled states* $|\Phi\rangle = (1/\sqrt{d})\sum_j |j\rangle_B|j\rangle_A$. *Then he sends system A of states to Alice and keeps system B.*

Encoding: *When Alice intends to send message* $M \in \mathcal{M}$, *Alice generates random variables* $S \in \mathcal{S}$, $S' \in \mathcal{S}'$, $Y \in \mathcal{Y}$, *and* $L_2 \in \mathbb{F}_p^{n_1-(n_2+n_3)}$ *independently according to the uniform distribution. Alice chooses elements* $X^n = (X_1X_2, \ldots, X_n) := \psi_S(Y, M, L_2) \in \mathbb{F}_p^{2n}$. *Alice applies the private dense coding operation* $\mathbf{W}(x_i, z_i)$ *on the ith state and sends her encoded system back to Bob.*

Reception: *Bob applies projective measurement* $\Pi = \{\Pi_{x,z}\}$ *with* $\Pi_{x,z} = \text{Proj}(\mathbf{W}(x,z)_A|\Phi\rangle)$ *on the composite system of the received states and the kept states to obtain the classical string* $\hat{X}^n = (\hat{X}_1\hat{X}_2, \ldots, \hat{X}_n)$ *with* $\hat{X}_i \in \mathbb{F}_p^2$, *where the projection operator on state* $|\psi\rangle$ *is denoted by* $\text{Proj}(|\psi\rangle)$. *Specifically, if* $p = 2$, *the measurement becomes the Bell state measurement. Finally, Bob acknowledges this reception to Alice via the public channel.*

Public communication from Alice to Bob: *Alice sends the variables* S, S', *and* $C := g_{S'}(M, Y)$ *to Bob via the public channel.*

Decoding and verification: *Bob performs classical decoding to* $\hat{X}^n$, *i.e., he obtains* $(\hat{M}, \hat{Y}) := f_S(\varphi_d(\hat{X}^n))$. *If* $g_{S'}(\hat{M}, \hat{Y}) = C$, *he accepts message* $\hat{M}$. *Otherwise, he aborts the protocol.*

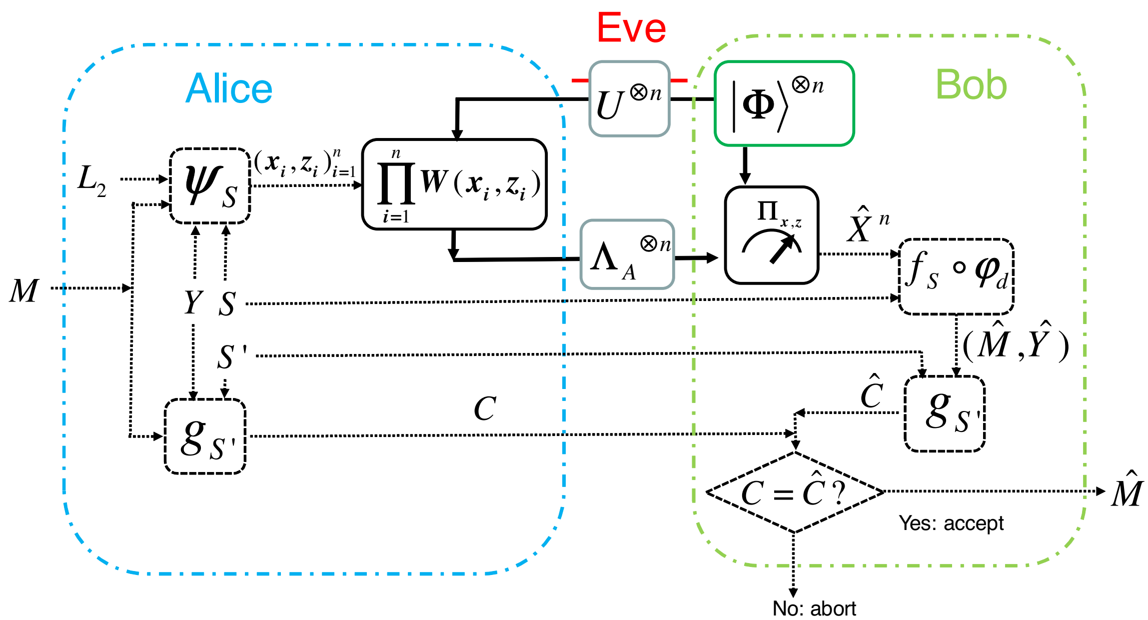

FIG. 3. An illustration of Protocol 1. Real lines express quantum information flow. Dotted lines express classical information flow. Here $|\Phi\rangle = (1/\sqrt{d}) \sum_i |i\rangle_{A'}|i\rangle_B$ is the initial state generated by Bob and U is a unitary performed by Eve. In Alice's encoding part, ψ_S is the encoder acting on message M and random numbers Y, L_2. The encoding operation on the ith state is $\mathbf{W}(x_i, z_i)$. In Bob's decoding part, $\Pi_{x,z}$ is a generalized Bell state measurement and the classical decoder $f_S \circ \varphi_d$ is a concatenation of the decoder of a classical error correcting code and a universal hash function. In addition, they decide if the protocol aborts by comparing the results of the universal hash function $g_{S'}$. Note that C and the random seeds S, S' are transmitted via a public channel. The explicit definitions for $\psi_S, g_{S'}, f_S$ are given in Sec. VII A.

Because of Eq. (69) below, we find that this protocol has $\epsilon(\varphi)$ completeness. Using Eqs. (70) and (71) below with Eq. (23), we find that this protocol has soundness with parameters ϵ_E and ϵ_B when $n_1 - (n_2 + n_3)$ and n_3 are chosen to be $\hat{m}_2(\epsilon_E)$ and $\hat{m}_3(\epsilon_B)$ defined as

$$\hat{m}_2(\epsilon_E) := \frac{1}{\log p} \min_{0 \le t \le 1} H_{1/(1+t)}(P_{XZ}) - \frac{1+t}{t} \log \epsilon_E - 2, \tag{28}$$

$$\hat{m}_3(\epsilon_B) := -\frac{\log \epsilon_B}{\log p}. \tag{29}$$

As explained in Proposition 1 below, there exists an error correcting code φ with the average decoding error probability ϵ_C and coding length

$$\hat{m}_1(\epsilon_C) = \frac{1}{\log p} \max_{0 \le t \le 1} 2 \log d_A - H_{1-t}(P_{XZ} * P_{XZ}) + \frac{1}{t}(\log \epsilon_C - 2). \tag{30}$$

These relations show the existence of a protocol that is ϵ_C complete, ϵ_E secure, and ϵ_B reliable. A simulation of the rates $R_1 = \hat{m}_1(\epsilon_C)/n, R_2 = \hat{m}_2(\epsilon_E)/n, R_3 = \hat{m}_3(\epsilon_B)/n$, and $R = R_1 - R_2 - R_3$ in the qubit case is shown in Fig. 4. The values defined in Eqs. (28) and (29) have a practical meaning because ϵ_E-secure and ϵ_B-reliable conditions can be satisfied with the numbers $\hat{m}_2(\epsilon_E)$ and $\hat{m}_3(\epsilon_B)$ and calculation complexity $O(n \log n)$, as explained in Sec. VII A. However, Eq. (30) does not have such a practical meaning for completeness because it assumes combination of the random coding and maximum likelihood decoder. In contrast, asymptotic rate (25) has a practical meaning because there exist error correcting codes to achieve the rate (25) with a small calculation complexity as explained in Sec. VII while their finite-length analysis is not so simple.

IV. APPLICATION TO AN UNKNOWN STATE WITH WEYL-HEISENBERG REPRESENTATION

In the PDC model, we consider the case when the preshared state τ_{ABE} is unknown. This case corresponds to the case when the channel from Bob to Alice is unknown in the model stated in Sec. III B. In this case, Alice and Bob need to estimate it before their secure communication. As a simple problem setting, we assume that Alice and Bob share n' copies of state τ_{AB} while they do not know the form of τ_{AB}, which is called the independent and identical density (i.i.d.) condition. In the worst case, Eve controls the whole of the environment system of the state $\tau_{AB}^{\otimes n'}$. To satisfy the secrecy requirement, Alice and Bob need to identify the form of τ_{AB} and assume the worst case.

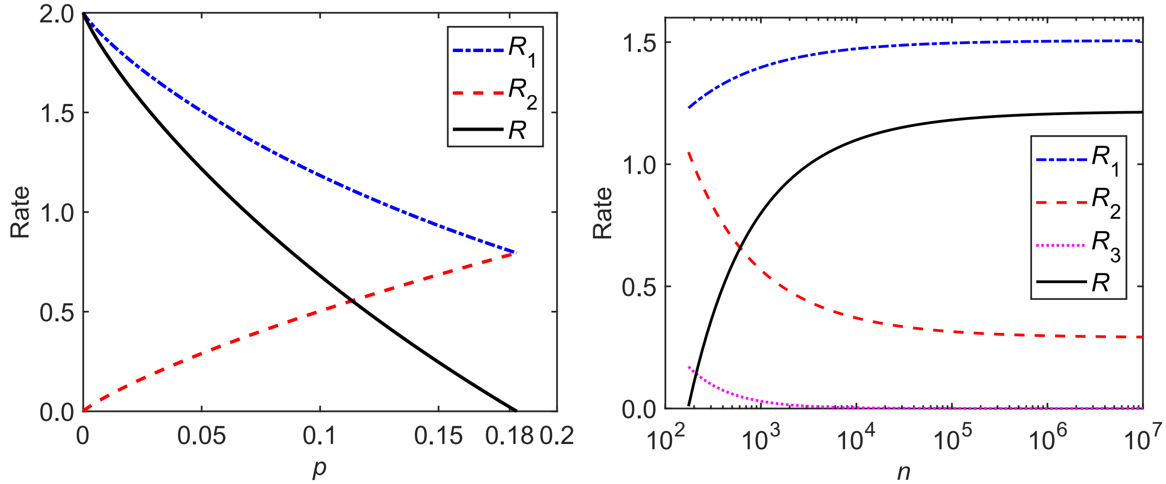

FIG. 4. An illustration of the error correcting rate R_1, the sacrificed rate for secrecy R_2, the sacrificed rate for error verification R_3, and the message rate $R = R_1 - R_2 - R_3$ in asymptotic and finite block length settings. (a) Asymptotic rate in depolarizing channel $\mathcal{E}(\rho) = (1-p)\rho + p\rho_{\text{mix}}$. Note that $R_3 = 0$ asymptotically and the message rate reaches zero when $p \approx 0.18$. (b) Finite-length rate in the depolarizing channel with depolarizing probability $p = 0.05$ with criteria $\epsilon_C \leq 0.2, \epsilon_B \leq 10^{-9}, \epsilon_E \leq 10^{-9}$. It is shown that the rates almost achieve the asymptotic limit at block length 10^6.

Suppose that Alice and Bob use $n' - n$ copies for the estimation of τ_{AB}. In this case, they estimate τ_{AB} by using only two-way LOCC, which is often called local tomography. However, the estimation of the unknown state without any assumption requires many types of measurements. If $\mathcal{H}_A$ and $\mathcal{H}_B$ have the same dimension and the unknown state τ_{AB} is a Bell diagonal state $\rho[P_{XZ}]$, we can reduce the number of measurements for the estimation as explained in Appendix D.

When $\mathcal{H}_B$ is of the same dimension as $\mathcal{H}_A$ and τ_{AB} is a general state, we can apply discrete twirling to state τ_{AB}:

$$T(\tau_{AB}) := \frac{1}{d^2}\sum_{x,z}(\mathbf{W}(x,z)_A \otimes \overline{\mathbf{W}(x,z)_B})\tau_{AB}(\mathbf{W}(x,z)_A \otimes \overline{\mathbf{W}(x,z)_B})^\dagger. \tag{31}$$

Here $\overline{\mathbf{W}(x,z)_B}$ is the complex conjugate of $\mathbf{W}(x,z)_B$. It is known that the above state is a Bell diagonal state [62, Example 4.22],[63,64]. Hence, when Alice and Bob apply the above discrete twirling and apply the estimation of a Bell diagonal state, they can apply private dense coding whose shared state is the estimated Bell diagonal state. However, as shown in Appendix D, the twirled state $T(\tau_{AB})$ can be estimated by applying the estimation method given in Appendix D to state τ_{AB}.

Therefore, combining the above method with Protocol 1, we propose Protocol 2, in which the encoding and decoding processes contain the procedure for the discrete twirling. In the following protocol, we assume that the communication channel from Bob to Alice is given as the n' times use of the same channel from Bob to Alice while the channel is not known.

Protocol 2.

Entanglement distribution: *Bob starts the protocol by generating n' entangled states $|\Phi\rangle = (1/\sqrt{d})\sum_j |j\rangle_B|j\rangle_{A'}$. Then he sends the A' halves of the states to Alice and keeps system $\mathcal{H}_B$. Then, they share state $\tau_{AB}^{\otimes n'}$.*

Estimation: *Alice and Bob choose $n' - n$ samples, and estimate the twirled state $T(\tau_{AB})$ of the shared state τ_{AB} by using the method explained in Appendix D. Based on the estimation of τ_{AB}, they decide their error correcting code φ and the integers n_1, n_2, n_3.*

Encoding: *Alice generates a string $\bar{X}^n = (\bar{X}_1, \bar{X}_2, \ldots, \bar{X}_n)$ with $X_i = (x_i, z_i) \in \mathbb{F}_d^2$ according to the uniform distribution. Alice encodes her message M into a string $X^n = (X_1X_2, \ldots, X_n) := \psi_S(Y, M, L_2)$ with $X_i \in \mathbb{F}_p^2$. For every element $(x_i, z_i) := \bar{X}_i + X_i$, Alice applies operation $\mathbf{W}(\bar{x}_i, \bar{z}_i)\mathbf{W}(x_i, z_i)$ on the remaining* i*th state and sends her encoded system back to Bob.*

Pubic communication from Alice to Bob 1: *Alice sends the string $\bar{X}^n$ to Bob via the public channel.*

Reception: *Bob applies unitaries $\overline{\mathbf{W}(\bar{x}_1, \bar{z}_1)} \cdots \overline{\mathbf{W}(\bar{x}_n, \bar{z}_n)}$ to $\mathcal{H}_B^{\otimes n}$, where $(\bar{x}_i, \bar{z}_i) := \bar{X}_i$. Then, Bob applies projective measurement $\Pi = \{\Pi_{x,z}\}$ on the composite system of the received states and the kept states to obtain the classical string $\hat{X}^n = (\hat{X}_1\hat{X}_2, \ldots, \hat{X}_n)$.*

Pubic communication from Alice to Bob 2: *The same procedure as the same step of Protocol 1.*

Decoding and verification: *Bob performs classical decoding to $\hat{X}^n$, i.e., he obtains $(\hat{M}, \hat{Y}) := f_S(\varphi_d(\hat{X}^n))$.*

If $g_{S'}(\hat{M},\hat{Y}) = C$, he accepts message $\hat{M}$. Otherwise, he aborts the protocol.

Since the estimation method given in Appendix D works well, due to the discussion in Sec. III B, this protocol achieves the rate given in Eq. (27) with the limit $n \to \infty$. For further analysis on the above protocol, note the relation

$$W(\hat{x},\hat{z})_A \otimes (\overline{W(\bar{x},\bar{z})_B})^\dagger |\Phi\rangle\langle\Phi| W(\hat{x},\hat{z})_A^\dagger \otimes \overline{W(\bar{x},\bar{z})_B} \quad (32)$$

$$= W(\hat{x}+\bar{x},\hat{z}+\bar{z})_A \otimes I_B |\Phi\rangle\langle\Phi| W(\hat{x}+\bar{x},\hat{z}+\bar{z})_A^\dagger \otimes I_B. \quad (33)$$

Operator (32) expresses a positive operator-valued measurement (POVM) element of the unitary $\overline{\mathbf{W}(\bar{x}_i,\bar{z}_i)}$ and the measurement Π as a whole performed in the reception step. The above relation shows that Bob can apply the measurement with POVM elements given in line (33) instead of line (32). That is, when the outcome of the measurement corresponding to operator (33) is given by $(\underline{x},\underline{z}) := (\hat{x}+\bar{x},\hat{z}+\bar{z})$, Bob's outcome $(\hat{x},\hat{z})$ of the above protocol is given as $(\underline{x}-\bar{x},\underline{z}-\bar{z})$. Therefore, Protocol 2 is converted to the following protocol.

Protocol 3.

Same steps as Protocol 2: *They make the same entanglement distribution, estimation, and encoding steps as in Protocol 2.*

Reception: *Bob applies projective measurement $\Pi = \{\Pi_{x,z}\}$ on the composite system of the received states and the kept states to obtain the classical string $\underline{X}^n = (\underline{X}_1\underline{X}_2,\ldots,\underline{X}_n)$.*

Pubic communication from Alice to Bob: *Alice sends the variables S, S', $C := g_{S'}(M,Y)$, and $\bar{X}^n$ to Bob via the public channel.*

Decoding and verification: *Bob performs classical decoding to $\underline{X}^n - \bar{X}^n$, i.e., he obtains $(\hat{M},\hat{Y}) := f_S(\varphi_d(\underline{X}^n - \bar{X}^n))$. If $g_{S'}(\hat{M},\hat{Y}) = C$, he accepts message $\hat{M}$. Otherwise, he aborts the protocol.*

V. MODULAR CODE FOR THE QUANTUM WIRE-TAP CHANNEL

A. Formulation for the quantum wire-tap channel

This section proposes a modular coding scheme with fixed error correcting code for quantum wire-tap channels and analyzes its performance in finite-length settings because this code construction is used for our PDC protocol. In the wire-tap channel model, the legitimate user Alice wants to send messages to another legitimate user Bob through a channel reliably and secretly in the presence of an eavesdropper Eve. The classical wire-tap channel has been extensively investigated since the debut of Wyner's wire-tap channel model [44], which was subsequently generalized by Csiszár and Körner [45]. The quantum wire-tap channel was also explored in both the asymptotic setting [26,27] and finite setting [43]. It acts as an approach to analyze the secrecy of QKD protocols [61] and QSDC protocols [36,37].

Here we focus on the CQ wire-tap channel, which consists of two CQ channels: $W_B : x(\in \mathcal{X}) \to W_B(x)$ from Alice to Bob and $W_E : x(\in \mathcal{X}) \to W_E(x)$ from Alice to Eve. Here, $W_B(x)$ and $W_E(x)$ are states on quantum systems $\mathcal{K}_B$ and $\mathcal{K}_E$, respectively. Alice's and Bob's procedures are called an encoder Γ and a decoder Π, respectively. When they use the above channel n times, an encoder is a map Γ from a message set $\mathcal{M}$ to $\mathcal{X}^n$. A decoder Π is a POVM $\{\Pi_m\}_{m\in\mathcal{M}}$ on $\mathcal{K}_B^{\otimes n}$. A pair comprising an encoder Γ and a decoder Π is called a code Φ. The decoding error probability is denoted by $\epsilon(W_B|\Phi)$. The ratio $\log|\mathcal{M}|/n$ is called the transmission rate and is denoted by $R(\Phi_n)$.

Here we measure the information leakage with a slightly different quantity from Eq. (3),

$$\bar{d}(M;E)_{\tau_{ME}} := \|\tau_{ME} - P_{\mathcal{M}} \otimes \tau_E\|_1, \quad (34)$$

where τ_{ME} is the joint state between Eve's system E and message M with uniform distribution. Note that mutual information $I(M;E)$ as another frequently used criterion can be upper bounded by the trace norm through Fannes' inequality. When Alice's encode is Γ, we denote the above value by $\bar{d}(M;E)[\Gamma]$.

A rate R is said to be achievable for the wire-tap channel (W_B,W_E) if there exists a sequence of codes $\Phi_n = (\Gamma_n,\Pi_n)$ such that, when the time channel use n goes to infinity, the decoding error probability $\epsilon(W_B|\Phi_n)$ and information leakage $\bar{d}(M;E)[\Gamma_n]$ go to zero and the transmission rate $R(\Phi_n)$ goes to R. The secrecy capacity for the wire-tap channel is defined as the supreme of all possible achievable rates, which is calculated as [27]

$$C(W_B,W_E) = \lim_{n\to\infty} \frac{1}{n} \max_{P_{TX^n}} [I(T;B^n) - I(T;E^n)]. \quad (35)$$

As a corollary, the rate $I(X;B) - I(X;E)$ is always achievable.

To ensure that the transmitted message can be decoded reliably, an error correcting code for channel W_B is needed. To keep the eavesdropper ignorant of the message, some randomization should be performed on the message. Hence, the modular coding scheme here is constructed as a concatenation of an inverse UHF family and an ordinary error correcting code. Such a structure has been introduced in classical situations [65]. In contrast to random coding [27,43] and *ad hoc* coding inspired by a specific error correcting code [66–68], our scheme is more practical for implementation thanks to the modular structure. Also, our secrecy bound is improved compared with that of Ref. [43].

We use the following notation for the next parts. If a probability transition matrix $\Gamma : \mathcal{V} \to \mathcal{X}$ is applied to a random variable V, we use the symbol $\Gamma \circ P_V$ to denote the probability distribution of the transition output, and the symbol $\Gamma \times P_V$ to denote the joint distribution of both the input and the output. In other words, we define $\Gamma \circ P_V(x) := \sum_v P_V(v)\Gamma(x|v)$ and $\Gamma \times P_V(x, v) := P_V(v)\Gamma(x|v)$. Similarly, for the quantum channel W_E, we have the notation $W_E \circ P_X := \sum_x P_X(x)W_E(x)$ and $W_E \times P_X := \sum_x P_X(x) |x\rangle \langle \otimes| W_E(x)$. Also, we define the CQ channel $W_E \circ \Gamma$ as $W_E \circ \Gamma(v) := \sum_x \Gamma(x|v)W_E(x)$. In addition, for any set $\mathcal{X}$, we denote the uniform distribution on the set $\mathcal{X}$ by $P_{\mathcal{X}}$.

B. Modular code construction

The modular code is constructed based on an existing error correcting code. Before the construction, we introduce a UHF family $\{f_s\}_{s\in\mathcal{S}}$, where f_S is a function from a set $\mathcal{L}$ to another set $\mathcal{M}'$ and $S \in \mathcal{S}$ is a variable to identify the function and is subject to the uniform distribution $P_{\mathcal{S}}$ on $\mathcal{S}$.

The function family $\{f_S\}_{S\in\mathcal{S}}$ is called a UHF family when the following condition holds.

(C1) The relation

$$\Pr[f_S(l) = f_S(l')] \le \frac{1}{\mathsf{M}'} \tag{36}$$

holds for any $l \ne l' \in \mathcal{L}$, where $\mathsf{M}' := |\mathcal{M}'|$.

Specifically, we impose an additional balanced condition.

(C2) The relation

$$|\{l \in \mathcal{L} : f_s(l) = m'\}| = \mathsf{L}_2 := \frac{\mathsf{L}_1}{\mathsf{M}'} \tag{37}$$

holds for any $s \in \mathcal{S}, m' \in \mathcal{M}'$, where $\mathsf{L}_1 := |\mathcal{L}|$.

Throughout this paper we always mean the balanced version when we refer to the UHF family. The inverse of f_s generates a random map. That is, for a given $m' \in \mathcal{M}'$, we define the distribution $\Gamma[f_s]_{m'}$ as the uniform distribution on the set $\{l : f_s(l) = m\}$.

Suppose that our existing error correcting code is given as $(\mathcal{L}, \{\Pi_l\}_{l\in\mathcal{L}})$, where $\mathcal{L}$ is a subset of channel input set $\mathcal{X}$ and $\{\Pi_l\}_{l\in\mathcal{L}}$ is a POVM for decoding $\mathcal{L}$. We prepare a UHF family $\{f_s\}_{s\in\mathcal{S}}$ from $\mathcal{L}$ to $\mathcal{M}'$. Before communication, Alice randomly chooses $S = s$, which will be shared via the public channel. When Alice intends to send message $m' \in \mathcal{M}'$, she generates L subject to the distribution $\Gamma[f_s]_{m'}$. Therefore, when Alice intends to send $m' \in \mathcal{M}'$, Bob receives the state $W_B \circ \Gamma[f_s]_{m'}$.

The decoder at Bob's side is a POVM $\Pi[f_s]$ with elements

$$\Pi[f_s]_m = \sum_{l:f_s(l)=m} \Pi_l. \tag{38}$$

Then the encoder and the decoder constitute the code $\Phi[f_s] = (\Gamma[f_s], \Pi[f_s])$. The performance of a wire-tap code consists of error probability and secrecy. When the message M is subjected to a uniform distribution, we have the average error probability

$$\epsilon(W_B|\Phi[f_s]) = \sum_{m'\in\mathcal{M}'} \frac{1}{\mathsf{M}'} \mathrm{Tr}(1 - \Pi[f_s]_{m'}) W_B \circ \Gamma[f_s]_{m'}. \tag{39}$$

When we denote the decoding error probability of the code φ by $\epsilon(W_B|\varphi)$, we have

$$\epsilon(W_B|\Phi[f_s]) \le \epsilon(W_B|\varphi). \tag{40}$$

For the information leakage, taking the average for S, we have

$$\begin{aligned} \bar{d}(M'; ES)[\Gamma[f_S]] &:= \|\tau_{M'ES} - P_{\mathcal{M}'} \otimes \tau_{ES}\|_1 \\ &= \mathbb{E}_S\|\tau_{M'E|S} - P_{\mathcal{M}'} \otimes \tau_{E|S}\|_1, \\ &= \mathbb{E}_S\bar{d}(M'; E)[\Gamma[f_S]], \end{aligned} \tag{41}$$

where $\tau_{M'ES} = \sum_s P_S(s) |s\rangle \langle \otimes| W_E \circ \Gamma[f_s] \times P_{\mathcal{M}'}$ and M' and S are subjected to independent and uniform distribution. The quantity $\bar{d}(M'; ES)$ is often useful for our analysis.

C. Finite-length analysis for the general wire-tap channel

For our finite-length analysis, we introduce Rényi mutual information as

$$I^{\uparrow}_{1+t}(A; B|\rho_{AB}) := D_{1+t}(\rho_{AB}\|\rho_A \otimes \rho_B), \tag{42}$$

$$\tilde{I}^{\uparrow}_{1+t}(A; B|\rho_{AB}) := \tilde{D}_{1+t}(\rho_{AB}\|\rho_A \otimes \rho_B). \tag{43}$$

Another version of Rényi mutual information is given as

$$I^{\downarrow}_{1+t}(A; B|\rho_{AB}) := \inf_{\sigma_B\in\mathcal{D}(\mathcal{H}_B)} D_{1+t}(\rho_{AB}\|\rho_A \otimes \sigma_B), \tag{44}$$

$$\tilde{I}^{\downarrow}_{1+t}(A; B|\rho_{AB}) := \inf_{\sigma_B\in\mathcal{D}(\mathcal{H}_B)} \tilde{D}_{1+t}(\rho_{AB}\|\rho_A \otimes \sigma_B). \tag{45}$$

For the secrecy, we have the following theorem, whose proof is given in Appendix E 1.

Theorem 1. *Assume that W_E is a CQ channel. For any subset $\mathcal{L} \subset \mathcal{X}$, we choose a UHF family $\{f_s\}_{s\in\mathcal{S}}$ defined on*

$\mathcal{L}$. Then, the wire-tap code $\Phi[f_s]$ with encoder $\Gamma[f_s]$ satisfies the following relation for the average information leakage:

$$\bar{d}(M;ES)[\Gamma[f_S]] \leq \min_{0\leq t\leq 1} 2^{(1-t)/(1+t)} 2^{[t/(1+t)](-\log \mathsf{L}_2 + \tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times P_{\mathcal{L}}))}. \tag{46}$$

Since an error correcting code for a CQ channel can always be transformed into a modular wire-tap code, we have the following proposition on the error probability according to the previous result [69].

Proposition 1. *Assume that W_B is a CQ channel. There exists an error correcting code $\varphi = (\mathcal{L}, \{\Pi_l\}_{l\in\mathcal{L}})$ such that*

$$\epsilon(W_B|\varphi) \leq 4 \min_{P_X, 0\leq t\leq 1} 2^{t[\log \mathsf{L}_1 - I^{\uparrow}_{1-t}(X;B|W_B\times P_X)]}. \tag{47}$$

When we choose a UHF family $\{f_s\}_{s\in\mathcal{S}}$ defined on a subset $\mathcal{L}$ chosen according to Proposition 1, combining Eqs. (40) and (47) implies the inequality

$$\epsilon(W_B|\Phi[f_s]) \leq 4 \min_{P_X, 0\leq t\leq 1} 2^{t[\log \mathsf{L}_1 - I^{\uparrow}_{1-t}(X;B|W_B\times P_X)]} \tag{48}$$

for any $s \in \mathcal{S}$.

Theorem 1 gives a single shot bound on information leakage. However, the Rényi mutual information term in Eq. (46) is inconvenient to evaluate because of the dependence on the subset $\mathcal{L}$. The following corollary shows an evaluable bound independent of $\mathcal{L}$ in the n-fold channel situation (see Appendix E 2 for the proof).

Corollary 1. *When the CQ channels W_E, W_B take the n-fold form W_E^n, W_B^n, there exists a wire-tap code $\Phi[f_s]$ generated from $\varphi = (\mathcal{L}, \{\Pi_l\}_{l\in\mathcal{L}})$ such that*

$$\epsilon(W_B|\Phi[f_s]) \leq 4 \min_{0\leq t\leq 1} 2^{t[\log \mathsf{L}_1 - n\max_{Q_X} I^{\uparrow}_{1-t}(X;B|W_B\times Q_X)]}. \tag{49}$$

Corollary 2. *For any subset $\mathcal{L} \subset \mathcal{X}^n$, we choose a UHF family $\{f_s\}_{s\in\mathcal{S}}$ defined on $\mathcal{L}$. Then, the wire-tap code $\Phi[f_s]$ with encoder $\Gamma[f_s]$ satisfies the following relation for the average information leakage:*

$$\bar{d}(M';ES)[\Gamma[f_S]] \leq \min_{0\leq t\leq 1} 2^{(1-t)/(1+t)} \times 2^{[t/(1+t)](-\log \mathsf{L}_2 + n\max_{Q_X} \tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times Q_X))}. \tag{50}$$

For any $0 < t < 1$ and arbitrarily small δ, take $\log \mathsf{L}_1 = n\max_{Q_X} I^{\uparrow}_{1-t}(X;B|W_B\times Q_X) - n\delta$, $\log \mathsf{L} = \max_{Q_X} \tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times Q_X) + n\delta$; then any coding rate below $\max_{Q_X} I(X;B|W_E\times Q_X) - \max_{Q_X} I(X;E|W_E\times Q_X)$ is achievable by taking $t \to 0$.

D. Finite-length analysis for the symmetric wire-tap channel

Next we discuss the symmetric channel case. A channel $W: \mathcal{X} \to \mathcal{D}(\mathcal{H})$ is symmetric if the input set $\mathcal{X}$ is a group and there exist a unitary projective representation $\{U_x\}_{x\in\mathcal{X}}$ and a state $\rho_0 \in \mathcal{D}(\mathcal{H})$ such that $W(x) = U_x\rho_0 U_x^{\dagger}$. When W_E is symmetric, the security evaluation in our criterion automatically implies the semantic security [43, Lemma 7]. Although Lemma 7 of Ref. [43] showed the semantic security by using the additive condition, i.e., the commutativity of $\mathcal{X}$, this derivation uses only the above symmetric condition and does not use the commutativity of $\mathcal{X}$. In fact, while we will discuss a wire-tap channel (W_B, W_E) for our analysis on private dense coding, both channels W_E and W_B satisfy the symmetric condition. In the following theorem, whose proof is given in Appendix E 3, we simplify our upper bounds for the error probability and secrecy in the symmetric case.

Theorem 2. *When W_E is a symmetric CQ channel, the upper bound in Eq. (50) is simplified to*

$$\bar{d}(M';ES)[\Gamma[f_S]] \leq \min_{0\leq t\leq 1} 2^{(1-t)/(1+t)} 2^{[t/(1+t)](-\log \mathsf{L}_2 + n\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times P_{\mathcal{X}}))}. \tag{51}$$

When W_B is a symmetric CQ channel, the upper bound in Eq. (49) is simplified to

$$\epsilon(W_B|\Phi[f_s]) \leq 4 \min_{0\leq t\leq 1} 2^{t[\log \mathsf{L}_1 - nI^{\uparrow}_{1-t}(X;B|W_B\times P_{\mathcal{X}})]}. \tag{52}$$

Theorem 2 shows that the rate

$$R_* = I(X;B|W_E\times P_{\mathcal{X}}) - I(X;E|W_E\times P_{\mathcal{X}}) \tag{53}$$

is achievable for our modular code in the symmetric case, while this achievability is known in existing studies [26,27,43]. To see our advantage over existing studies, we focus on the exponential decreasing rate of information leakage for an encoder $\Gamma[f_S]$. When the sacrificed rate $R_2 = \log \mathsf{L}_2/n$ is fixed, $\bar{d}(M';ES)[\Gamma[f_S]]$ should decrease exponentially as $n \to \infty$. The exponential decreasing rate (exponent) is defined by

$$e_d(R_s|W_E) := \lim_{n\to\infty} -\frac{1}{n}\log \bar{d}(M';ES)[\Gamma[f_S]]. \tag{54}$$

Then Eq. (51) yields

$$e_d(R_2|W_E) \geq \max_{0\leq t\leq 1} \frac{t}{1+t}(R_2 - \tilde{I}^{\downarrow}_{1+t}(X;E|W_E \times P_{\mathcal{X}})). \tag{55}$$

The above lower bound of the exponent is strictly larger than the result

$$e_d(R_2|W_E) \geq \max_{0\leq t\leq 1} \frac{t}{2}(R_2 - I^{\downarrow}_{1+t}(X;E|W_E \times P_X)) \tag{56}$$

obtained in Ref. [43] using the random coding method.

Also, we have the following lemma, whose proof is given in Appendix E 4.

Lemma 2. *When the CQ wire-tap channel (W_B, W_E) is degraded and both the W_B, W_E channels are symmetric, the secrecy capacity is $I(X;\hat{B}) - I(X;\hat{E})$, where X expresses the random variable that takes values in the finite group G according to the uniform distribution on G.*

VI. ERROR VERIFICATION

Now, we explain how the reliability can be realized by error verification [34, Section VIII],[70]. Assume that Alice sends the information $(M, Y) \in \mathcal{M} \times \mathcal{Y}$ via the wire-tap code and Bob obtains $(\hat{M}, \hat{Y}) \in \mathcal{M} \times \mathcal{Y}$. Here M and Y are assumed to obey the uniform distribution on $\mathcal{M}$ and $\mathcal{Y}$ independently. They intend to check whether $M = \hat{M}$ holds without leaking the information for M. To this end, Alice prepares a UHF family $\{g_{S'}\} : \mathcal{M} \times \mathcal{Y} \to \mathcal{Y}$, where S' is the random seed, to decide the hash function. Here, we additionally impose the following condition.

(C3) For any $m \in \mathcal{M}$, $c \in \mathcal{Y}$, and $s' \in \mathcal{S}'$, there uniquely exists $y(m, s', c) \in \mathcal{Y}$ such that

$$c = g_{s'}(m, y(m, s', c)). \tag{57}$$

Condition (C3) implies the balanced condition (C2). Then, Alice sends the random seed S' and $C := g_{S'}(M, Y)$ to Bob via the public channel. When $g_{S'}(\hat{M}, \hat{Y}) = C$, Bob accepts his decoded message $\hat{M}$. Otherwise, he aborts the protocol.

Denote the length of $\mathcal{Y}$ by t, i.e., $t = \log|\mathcal{Y}|$. In the following, we show that the relation

$$\sup_{m\neq \hat{m}} \Pr[\mathrm{Ab}^c\,|m, \hat{m}] \leq 2^{-t} \tag{58}$$

holds when S' is independent of $M, Y, \hat{M}, \hat{Y}$. To this end, it is sufficient to show the relation

$$\Pr[g_{S'}(m, Y) = g_{S'}(\hat{m}, \hat{Y})|M = m, \hat{M} = \hat{m}] \leq 2^{-t} \tag{59}$$

for any $m \neq \hat{m} \in \mathcal{M}$. The above relation follows from the relation

$$\Pr[g_{S'}(m, y) = g_{S'}(\hat{m}, \hat{y})] \leq 2^{-t} \tag{60}$$

for any $m \neq \hat{m} \in \mathcal{M}$ and $y, \hat{y} \in \mathcal{Y}$. However, this relation follows from the definition of UHF. Hence, we obtain Eq. (58), which is reliability (S2).

The following lemma shows that the publicly shared variables for error verification give no information about message M.

Lemma 3. *Assume that $M' = (M, Y)$ is subject to the uniform distribution and E' is a quantum system correlated to M'. When S' is an independent variable of other systems M', E, and $C = g_{S'}(M, Y)$, we have*

$$d(M; E'S'C) \leq d(M'; E'). \tag{61}$$

The proof of this lemma is given in Appendix F.

VII. DETAILED ANALYSIS FOR PRIVATE DENSE CODING

In this section, we provide the concrete protocol construction for the general private dense coding setting and derive the nonasymptotic and asymptotic performance of the protocol. Then we show that the code can be practically implemented when certain conditions are satisfied.

A. Protocol construction

We propose our concrete protocol for private dense coding $\mathrm{PDC}(\tau_{ABE}, \{U_g\}_{g\in G}, \Lambda_A)$ by combining a wire-tap channel code and error verification. Assume that n copies of ρ_{ABE} are given among Alice, Bob, and Eve. Alice and Bob prepare an error correcting code $\varphi = (\mathcal{L}, \{\Pi_l\}_{l\in\mathcal{L}})$ for n uses of CQ channel $g(\in G) \mapsto \Lambda_A(U_g \rho_{AB} U_g^{\dagger})$. For the efficient construction of our protocol, we choose a prime power q, which corresponds to the size of our finite field $\mathbb{F}_q$ to be used. Then, we assume the condition for the code φ:

$$|\mathcal{L}| = q^{n_1}. \tag{62}$$

If this condition does not hold, we decrease the number of $|\mathcal{L}|$ to satisfy this condition. We choose a bijective map φ_e from $\mathbb{F}_q^{n_1}$ to $\mathcal{L}$. We prepare the message set $\mathcal{M} := \mathbb{F}_q^{n_2}$, the set for covering variable $\mathcal{Y} := \mathbb{F}_q^{n_3}$, and the message set for wire-tap code $\mathcal{M}' := \mathcal{Y} \times \mathcal{M} = \mathbb{F}_q^{n_2+n_3}$.

For $V \in \mathbb{F}_q^{d_1+d_2-1}$, we introduce the $d_1 \times d_2$ Toeplitz matrix $T_{d_1,d_2}(V)$, which is defined as

$$T_{d_1,d_2}(V)_{i,j} := V_{i-j+d_2}. \tag{63}$$

We employ two UHF families $f_S : \mathbb{F}_q^{n_1} \to \mathcal{M}'$ and $g_{S'} : \mathcal{M}' \to \mathcal{Y}$, where $S \in \mathcal{S} := \mathbb{F}_q^{n_1-1}$ and $S' \in \mathcal{S}' := \mathbb{F}_q^{n_2+n_3-1}$

are uniform random variables. The UHF f_S is defined as

$$f_S(L) = \begin{pmatrix} f_{S,1}(L) \\ f_{S,2}(L) \end{pmatrix} := (I, T_{n_2+n_3,n_1-(n_2+n_3)}(S)) \begin{pmatrix} L_1 \\ L_2 \end{pmatrix}, \tag{64}$$

where $L = (L_1, L_2)$, $L_1 \in \mathbb{F}_q^{n_2+n_3}$, $L_2 \in \mathbb{F}_q^{n_1-(n_2+n_3)}$, and $f_{S,1}(L) \in \mathcal{Y}, f_{S,2}(L) \in \mathcal{M}$. Similarly, the UHF $g_{S'}$ are defined with $S' \in \mathcal{S}' := \mathbb{F}_q^{n_2+n_3-1}$ as

$$g_{S'}(M, Y) := (I, T_{n_3,n_2}(S')) \begin{pmatrix} Y \\ M \end{pmatrix}. \tag{65}$$

When Alice intends to send message $M \in \mathcal{M}$, Alice generates random variables $S \in \mathcal{S}$, $S' \in \mathcal{S}'$, $Y \in \mathcal{Y}$, and $L_2 \in \mathbb{F}_q^{n_1-(n_2+n_3)}$ independently according to the uniform distribution. Alice applies the encoder ψ_S defined as [52, Appendix A-B]

$$\psi_S(M, Y, L_2) := \varphi_e \left(\begin{pmatrix} I & -T_{n_2+n_3,n_1-(n_2+n_3)}(S) \\ 0 & I \end{pmatrix} \begin{pmatrix} M' \\ L_2 \end{pmatrix} \right), \tag{66}$$

where $M' = (M, Y)^T$. It is easy to verify that the encoder ψ_s is an example of the encoder $\Gamma[f_s]_{m'}$ proposed in Sec. V B. Then, based on an error correcting code φ for the CQ channel, and integers n_2, n_3, prime power q, we give our protocol $P(\varphi, n_2, n_3, q)$ as follows.

Protocol 4.

Encoding: *To begin with, there are n preshared states τ_{ABE} between Alice, Bob, and Eve. When Alice intends to send message $M \in \mathcal{M}$, Alice generates random variables $S \in \mathcal{S}$, $S' \in \mathcal{S}'$, $Y \in \mathcal{Y}$, and $L_2 \in \mathbb{F}_q^{n_1-(n_2+n_3)}$ independently according to the uniform distribution. Alice chooses elements $(g_1 g_2, \ldots, g_n) := \psi_S(Y, M, L_2)$. Alice applies the private dense coding operation U_{g_i} on the* i*th state and sends her encoded system to Bob.*

Decoding 1: *Bob applies measurement $\Pi = \{\Pi_l\}_{l\in\mathcal{L}}$ on the composite system $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ and obtains $\hat{L} \in \mathcal{L}$. Bob acknowledges this decoding to Alice via the public channel.*

Pubic communication from Alice to Bob: *Alice sends the variables S, S′, and $C := g_{S'}(M, Y)$ to Bob via the public channel.*

Decoding 2 and verification: *When $g_{S'} \circ f_S \circ \varphi_e^{-1}(\hat{L}) \neq C$, Bob aborts the protocol. Otherwise, he recovers the message as $\hat{M} := f_{S,2} \circ \varphi_e^{-1}(\hat{L})$.*

In the above protocol, the part except for the error correcting code $\varphi = (\mathcal{L}, \{\Pi_l\}_{l\in\mathcal{L}})$ has calculation complexity $O(n \log n)$ due to the following reason. The Toeplitz matrix can be constructed as part of a circulant matrix. For example, Hayashi and Tsurumaru [71, Appendix C-B] provided a method to obtain a circulant matrix. Hayashi and Tsurumaru [71, Appendix C-A] also provided an algorithm for the multiplication of a circulant matrix with calculation complexity $O(n \log n)$. Hence, if the error correcting part can be efficiently implemented, this protocol can be efficiently implemented.

Remark 1. In the above protocol, Alice needs to perform the public communication to Bob after Bob receives the quantum states. If Eve knows the variables S' and $C = g_{S'}(M, Y)$ before Bob receives the quantum states, Eve has a possibility that she can send the quantum state ρ to Bob such that Bob's outcomes $\hat{M}, \hat{Y}$ satisfy $C = g_{S'}(\hat{M}, \hat{Y})$ and $\hat{M} = M$. To avoid this risk, Alice needs to perform the public communication to Bob in this order.

B. Performance of our PDC protocol

To apply the analysis of the wire-tap channel in the evaluation of our PDC protocol, we have the following lemma, whose proof is given in Appendix G.

Lemma 4. *Given a PDC model* $\mathrm{PDC}(\tau_{ABE}, \{U_g\}_{g\in G}, \Lambda_A)$, *we consider the two channels $W_B(x) = U_x \Lambda_A(\tau_{AB}) U_x^\dagger$ and $W_E(x) = U_x \tau_{AE} U_x^\dagger$. Then, the information quantities can be expressed as*

$$I_{1-t}^{\uparrow}(X; BB'|W_B \times P_{\mathcal{X}}) = \log d_A - H_{1-t}^{\downarrow}(A|B|\Lambda_A(\tau_{AB})), \tag{67}$$

$$\tilde{I}_{1+t}^{\downarrow}(X; AE|W_E \times P_{\mathcal{X}}) = \log d_A - \tilde{H}_{1+t}^{\uparrow}(A|E|\tau_{AE}). \tag{68}$$

Using this lemma and Theorem 2, as performance evaluation of our PDC protocol, we have the following theorem, whose proof is given at the end of this subsection.

Theorem 3. *Given integers n_2, n_3, a prime power q, and an error correcting code $\varphi = (\mathcal{L}, \{\Pi_l\}_{l\in\mathcal{L}})$ such that $|\mathcal{L}| = q^{n_1}$, the protocol $P(\varphi, n_2, n_3, q)$ satisfies the inequalities*

$$\epsilon_C(P(\varphi, n_2, n_3, q)) \leq \epsilon(\varphi), \tag{69}$$

$$\begin{aligned} &\epsilon_E(P(\varphi, n_2, n_3, q)) \\ &\quad \leq \min_{0\leq t\leq 1} 2^{-(1-t)/(1+t)} \\ &\qquad \times 2^{[tn/(1+t)](-(n_1-n_2-n_3)(\log q)/n + \log d_A - \tilde{H}_{1+t}^{\uparrow}(A|E|\tau_{AE}))}, \end{aligned} \tag{70}$$

$$\epsilon_B(P(\varphi, n_2, n_3, q)) \leq q^{-n_3}, \tag{71}$$

where $\epsilon(\varphi)$ is the decoding error probability of the error correcting code φ.

For a more concrete bound on $\epsilon_C(P(\varphi, n_2, n_3, q))$, we apply Proposition 1 to the case with $\log \mathsf{L}_1 = n_1 \log q$.

When φ is an error correcting code given in Proposition 1, we have

$$\epsilon_C(P, n_2, n_3, q) \leq 4 \min_{0\leq t\leq 1} 2^{tn[n_1(\log q)/n - \log d_A + H^{\downarrow}_{1-t}(A|B|\Lambda_A(\tau_{AB}))]}. \quad (72)$$

The right-hand side of Eq. (72) follows from the application of Eq. (67) to the right-hand side of Eq. (47) in Proposition 1. Hence, Eq. (69) implies Eq. (72).

Therefore, the key evaluations (4), (5), and (6) in Sec. II A are obtained as follows. That is, Eqs. (72), (70), and (71) imply Eqs. (4), (5), and (6), respectively. That is, combining Theorem 3 and Proposition 1 guarantees the existence of the PDC protocol stated in Sec. II A.

Proof of Theorem 3: When the error correcting code recovers L correctly, the protocol does not abort. Hence, combining Eq. (40) with the above fact, we obtain Eq. (69). Relation (71) follows from Eq. (58).

The CQ channel $g(\in G) \mapsto \Lambda_A(U_g\rho_{AE}U_g^{\dagger})$ is symmetric; Theorem 2 guarantees that

$$\begin{aligned} d(M', EAS) &\leq \bar{d}(M', EAS) \\ &\leq \min_{0\leq t\leq 1} 2^{-2t/(1+t)} \\ &\quad \times 2^{[tn/(1+t)](-(n_1-n_2-n_3)(\log q)/n + \log d_A - \tilde{H}^{\uparrow}_{1+t}(A|E|\tau_{AE}))}. \end{aligned} \quad (73)$$

To derive the right-hand side of Eq. (73), we used Eq. (68). Applying Lemma 3 to the case with $E' = EA$, we obtain Eq. (70) from Eq. (73). Therefore, we obtain Theorem 3. ∎

C. Capacity formulae

The private capacity characterizes the asymptotic performance from a theoretical viewpoint. The following theorem, whose proof is given in Appendix H, shows the equivalence between private capacity of private dense coding and secrecy capacity of the corresponding wire-tap channel.

Theorem 4. *For the PDC model* PDC$(\tau_{ABE}, \{U_g\}_{g\in G}, \Lambda_A)$ *and corresponding wire-tap channels* $W_B(x) = U_x\Lambda_A(\tau_{AB}) U_x^{\dagger}$ *and* $W_E(x) = U_x\tau_{AE}U_x^{\dagger}$*, the private capacity of the PDC model equals the secrecy capacity of* (W_B, W_E)*, i.e.,*

$$C(\tau_{ABE}, \{U_g\}_{g\in G}, \Lambda_A) = C(W_B, W_E). \quad (74)$$

Then, we have the following corollary.

Corollary 3. *When* τ_{ABE} *is a pure state, and* τ_{AB} *is maximally correlated, we have*

$$\begin{aligned} &C(\tau_{ABE}, \{U_g\}_{g\in G}, \mathrm{id}_A) \\ &\quad = 2(H(\tau_{A,E}) - H(\tau_E)) = 2H(A|E)_{\tau} = -2H(A|B)_{\tau}, \end{aligned} \quad (75)$$

where id_A *is the noiseless channel on* $\mathcal{H}_A$.

This corollary can be shown as follows. Appendix A shows that the wire-tap channel (W_B, W_E) of the above case is degraded. Because of Lemma 2 and the group symmetric condition, the secrecy capacity of (W_B, W_E) is given by the right-hand side of Eq. (75). Then, Theorem 4 guarantees Eq. (75).

D. Practical code construction with a vector space over a finite field

Next, we show that the error correcting part φ can be efficiently implemented, under conditions (B1) and (B2) introduced in Sec. II. For convenience, the conditions are restated below.

(B1) The group G forms a vector space $\mathcal{X}$ over a finite field $\mathbb{F}_q$.

(B2) The states $\{U_x\Lambda_A(\tau_{AB})U_x^{\dagger}\}_{x\in\mathcal{X}}$ are commutative with each other.

To discuss the calculation complexity for the error correcting code, it is sufficient to consider the case when the channel from Alice to Bob is Λ_A, i.e., is not intercepted by Eve. Because of (B2), we can choose a basis $\{|e_\omega\rangle\}_{\omega\in\Omega}$ on $\mathcal{H}_{B'}\otimes\mathcal{H}_B$ that commonly diagonalizes $U_x\Lambda_A(\tau_{AB})U_x^{\dagger}$ for all $x \in \mathcal{X}$. We denote the measurement corresponding to this basis by $\{\Pi_\omega\}_{\omega\in\Omega}$, and define the distribution $P_\Omega(\omega) := \mathrm{Tr}\Pi_\omega\Lambda_A(\tau_{AB})$. We obtain the classical channel $W^c(\omega|x) := \mathrm{Tr}\Pi_\omega U_x\Lambda_A(\tau_{AB})U_x^{\dagger}$. Without any information loss, Bob's decoding can be reduced to the application of classical decoding for the classical channel W^c to the outcomes via the measurement $\{\Pi_\omega\}_{\omega\in\Omega}$.

Since the density matrix $U_x\Lambda_A(\tau_{AB})U_x^{\dagger}$ has the same eigenvalue as $\Lambda_A(\tau_{AB})$, including the multiplicity, there exists a permutation π_x on Ω such that $P_\Omega(\pi_x(\omega)) = \mathrm{Tr}\Pi_\omega U_x\Lambda_A(\tau_{AB})U_x^{\dagger}$. Since $\pi_x\pi_{x'} = \pi_{x+x'}$, the relation $W^c(\omega|x) = P_\Omega(\pi_x(\omega))$ implies that the channel W^c is a symmetric channel.

In this symmetric setting, we can choose an error correcting code as a linear subspace $\mathcal{L} \subset \mathcal{X}^n$ on $\mathbb{F}_q$. Such an error correcting code $\mathcal{L}$ can be constructed by using LDPC codes [66] or polar codes [67]. It has been demonstrated that polar codes can achieve channel capacity for any discrete symmetric channels with a sufficiently small decoding error probability ϵ_C such that the encoder ϕ_e

and the decoder ϕ_d have calculation complexity $O(n \log n)$ [72–75].

VIII. CONCLUSION AND DISCUSSION

We formulate the framework of private dense coding to realize quantum secure direct communication. While this method requires a preshared quantum state, it works even when noise exists. This method guarantees secrecy against the eavesdropper, Eve, even when Eve intercepts the quantum system transmitted by Alice. To cover the finite-length effect, we derive a formula for the amount of information leakage dependently of the block length of our code and the sacrificed rate. When the channel to Eve is symmetric, this formula has better bound (Theorem 2) than an existing bound [43, Eq. (78)].

In our method, Alice's encoding operation is limited to a unitary operation given as a projective unitary representation of a group G. Also, when a certain commutative condition holds, we show that Bob's decoding measurement can be restricted to a special measurement over a single joint system between Bob's receiving system and Bob's local system. That is, Bob does not need to make any measurement across multiple joint systems. Furthermore, when the group is a vector space over a finite field, we propose a practical coding method, whose encoding and decoding operations have calculation complexity $O(n \log n)$, where n is the block length.

We apply our results to the case when Alice's encoding operation is limited to the Weyl-Heisenberg representation. Although this case is similar to the case studied in preceding papers [50], we derive a security formula for information leakage in the finite-length setting. In this setting, to cover an unknown preshared state, we propose another protocol that contains an estimation process of the preshared state.

There are many protocols and experiments that fit into our setting [8,50,76–79]. However, the rigorous performance in a practical situation is unclear. Our results reduce the gap between the theoretical performance and experimental setting. For a realistic application, we need to combine the error estimation and our evaluation for information leakage (28). Such an evaluation is a future study. This paper assumes that the preshared state satisfies the n-fold i.i.d. condition. However, the realistic case does not necessarily satisfy this condition. Removing this condition is another future topic.

Unfortunately, in this study we have not analytically derived the asymptotically tight transmission rate, which is called the capacity. As stated in Corollary 3, our analytically obtained transmission rate is tight when τ_{ABE} is a pure state, and τ_{AB} is maximally correlated. This problem was inherited by the following property of the wire-tap channel. When the wire-tap channel model is degraded, $\max_{P_X} I(X;B) - I(X;E)$ is the capacity, i.e., the optimal transmission rate. Otherwise, this value is not the capacity in general and the analytical derivation of the capacity is an open problem. Hence, to resolve this problem, it is necessary to derive the capacity for a wire-tap channel model under the symmetric condition. This is another future problem. In addition, recently, the one-step QSDC protocol was proposed [80,81]. Since this protocol has a form different from our private dense coding, we cannot directly apply our result to this problem. Hence, the analysis on this problem is another future study.

ACKNOWLEDGMENTS

This works is supported in part by the Guangdong Provincial Key Laboratory (Grant No. 2019B121203002), the Tsinghua University Initiative Scientific Research Program, and the National Natural Science Foundation of China (Grant No. 62171212).

APPENDIX A: MAXIMALLY CORRELATED STATE

In this appendix, we show that the CQ wire-tap channel W_B, W_E is degraded when Λ_A is the noiseless channel, τ_{ABE} is a pure state, and τ_{AB} is maximally correlated.

We choose bases $|v_j^A\rangle$ and $|v_j^B\rangle$ on $\mathcal{H}_A$ and $\mathcal{H}_B$ such that $\tau_{AB} = \sum_{j,j'} a_{j,j'} |v_j^A, v_j^B\rangle\langle v_{j'}^A, v_{j'}^B|$. We diagonalize τ_{AB} as $\tau_{AB} = \sum_j s_j |u_j\rangle\langle u_j|$ and $|u_j\rangle = \sum_{j'} b_{j,j'} |v_{j'}^A, v_{j'}^B\rangle$, where $(b_{j,j'})$ is a unitary matrix. Then, by choosing a basis $|v_j^E\rangle$, the pure state τ_{ABE} is written as $\sum_j \sqrt{s_j} |u_j\rangle |v_j^E\rangle$. We choose $t_{j'}$ and normalized vectors $(c_{j|j'})_j$ for j' as $t_{j'} := \sum_j s_j |b_{j,j'}|^2$ and $\sqrt{s_j} b_{j,j'} = \sqrt{t_{j'}} c_{j'|j}$. We define $|u_{j'}^E\rangle := \sum_j c_{j|j'} |v_j^E\rangle$. Hence, we have $\sum_j \sqrt{s_j} |u_j\rangle |v_j^E\rangle = \sum_{j,j'} \sqrt{s_j} b_{j,j'} |v_{j'}^A, v_{j'}^B\rangle |v_j^E\rangle = \sum_{j'} \sqrt{t_{j'}} |v_{j'}^A, v_{j'}^B\rangle |u_{j'}^E\rangle$, which implies that

$$\tau_{AE} = \sum_{j'} t_{j'} |v_{j'}^A, u_{j'}^E\rangle\langle v_{j'}^A, u_{j'}^E|. \tag{A1}$$

We define the TP-CP map Γ as

$$\Gamma(\rho) := \sum_{j'} \langle v_{j'}^B | \rho | v_{j'}^B \rangle |u_{j'}^E\rangle\langle u_{j'}^E|. \tag{A2}$$

Then, we have

$$\begin{aligned}\Gamma(\tau_{AB}) &= \sum_{j'} \langle v_{j'}^B | \tau_{AB} | v_{j'}^B \rangle |u_{j'}^E\rangle\langle u_{j'}^E| \\ &= \sum_{j'} t_{j'} |v_{j'}^A, u_{j'}^E\rangle\langle v_{j'}^A, u_{j'}^E| \\ &= \tau_{AE}.\end{aligned} \tag{A3}$$

Since U_g acts only on $\mathcal{H}_A$, the CQ wire-tap channel W_B, W_E is degraded.

APPENDIX B: BOB RECEIVES THE BELL DIAGONAL STATE

Here, we show that Bob's received state is Bell diagonal in the setting PDC($|\Psi\rangle, \{\mathbf{W}(x,z)\}, \Lambda[\tilde{P}_{XZ}]_A$). When Alice's operation is $\mathbf{W}(x,z)$, Bob's state on $\mathcal{H}_B \otimes \mathcal{H}_{B'}$ is

$$\begin{aligned}
&\Lambda[\tilde{P}_{XZ}]_A(\mathbf{W}(x,z)\Lambda[P_{XZ}]_A(|\Phi\rangle\langle\Phi|)\mathbf{W}(x,z)^\dagger) \\
&\quad = \mathbf{W}(x,z)(\Lambda[\tilde{P}_{XZ}]_A \circ \Lambda[P_{XZ}]_A(|\Phi\rangle\langle\Phi|))\mathbf{W}(x,z)^\dagger \\
&\quad = \mathbf{W}(x,z)\Lambda[\tilde{P}_{XZ} * P_{XZ}]_A(|\Phi\rangle\langle\Phi|)\mathbf{W}(x,z)^\dagger \\
&\quad = \Lambda[F_{x,z}[\tilde{P}_{XZ} * P_{XZ}]]_A(|\Phi\rangle\langle\Phi|) \\
&\quad = \rho[F_{x,z}[\tilde{P}_{XZ} * P_{XZ}]],
\end{aligned} \tag{B1}$$

where the distributions $\tilde{P}_{XZ} * P_{XZ}$ and $F_{x,z}[P_{XZ}]$ on $\mathbb{F}_p^2$ are defined as

$$\tilde{P}_{XZ} * P_{XZ}(x,z) := \sum_{x'z'} \tilde{P}_{XZ}(x',z')P_{XZ}(x-x',z-z'), \tag{B2}$$

$$F_{x,z}[P_{XZ}](x',z') := P_{XZ}(x'-x,z'-z), \tag{B3}$$

and the density matrix $\rho[P_{XZ}]$ is defined as

$$\rho[P_{XZ}] := \sum_{x,z} P_{XZ}(x,z)\mathbf{W}(x,z)|\Phi\rangle\langle\Phi|\mathbf{W}(x,z)^\dagger. \tag{B4}$$

APPENDIX C: PROOF OF LEMMA 1

For the setting PDC($\omega_{ABE}, \{\mathbf{W}(x,z)\}, \mathrm{id}_A$), recall that $\omega_{ABE} = \Lambda[\tilde{P}_{-X,Z}]_B(|\Psi\rangle\langle\Psi|)$, where

$$|\Psi\rangle_{ABE} = \frac{1}{\sqrt{d}}\sum_{x,z}\sqrt{P(x,z)}\mathbf{W}_A(x,z)|\Phi\rangle_{AB}|x,z\rangle_E \tag{C1}$$

is the purification of $\rho[P_{XZ}]$. Then the reduced density matrices are

$$\begin{aligned}
\omega_{AE} &= \sum_j \frac{1}{d}\mathrm{Proj}\left(\sum_{x,z}\sqrt{P(x,z)}\mathbf{W}(x,z)|j\rangle_A|x,z\rangle_E\right), \\
\omega_E &= \sum_{x,z} P_{XZ}(x,z)|x,z\rangle_E\langle x,z|, \\
\omega_{AB} &= \rho[\tilde{P}_{XZ} * P_{XZ}], \\
\omega_B &= \rho_{B,\mathrm{mix}}.
\end{aligned}$$

The quantities for the asymptotic rate are

$$\begin{aligned}
H(A|E)_\omega &= H(\omega_{AE}) - H(\omega_E) \\
&= \log d_A - H(XZ|P_{XZ}), \\
H(A|B)_\omega &= H(\omega_{AB}) - H(\omega_B) \\
&= H(XZ|\tilde{P}_{XZ} * P_{XZ}) - \log d_A.
\end{aligned}$$

The quantities for finite analysis are

$$\begin{aligned}
\tilde{H}^\uparrow_{1+t}(A|E)_\omega &\geq \tilde{H}^\downarrow_{1+t}(A|E)_\omega \\
&= -\tilde{D}_{1+t}(\omega_{AE}\|\omega_E) \\
&= -\frac{1}{t}\log \mathrm{Tr}\left(\omega_E^{-t/2(1+t)}\omega_{AE}\omega_E^{-t/2(1+t)}\right)^{1+t} \\
&= -\frac{1}{t}\log\frac{1}{d_A^s}\left(\sum_{x,z}P_{XZ}(x,z)^{1/(1+t)}\right)^{1+t} \\
&= \log d_A - H^\downarrow_{1/(1+t)}(P_{XZ}), \\
H^\downarrow_{1-t}(A|B)_\omega &= -D_{1-t}(\omega_{AB}\|\omega_B) \\
&= \frac{1}{t}\log \mathrm{Tr}\rho[\tilde{P}_{XZ} * P_{XZ}]^{1-t}\rho_{B,\mathrm{mix}}^s \\
&= -\log d_A + H^\downarrow_{1-t}(\tilde{P}_{XZ} * P_{XZ}).
\end{aligned}$$

APPENDIX D: ESTIMATION OF THE BELL DIAGONAL STATE

1. Case with the Bell diagonal state

We consider state estimation on the composite system $\mathcal{H}_A \otimes \mathcal{H}_B$ by using local measurements when the unknown state is given as a Bell diagonal state $\rho[P_{XZ}]$, which is defined in Eq. (17). Here, we consider only the case when d is a prime p and the arithmetics is performed in $\mathbb{F}_p$ in the following part. First, we prepare the relation

$$\mathbf{W}(x,z)\mathbf{W}(x',z') = \omega^{x'z-xz'}\mathbf{W}(x',z')\mathbf{W}(x,z). \tag{D1}$$

For k,l, we measure the marginal distribution P_{lX-kZ} as follows. We say that the following measurement is $M(lX-kZ)$. Alice measures $\mathbf{W}(k,l) = \mathbf{X}^k\mathbf{Z}^l$ and obtains the outcome ω^Y. Bob measures $(\mathbf{X}^k\mathbf{Z}^l)^T = \mathbf{Z}^l\mathbf{X}^{-k}$ and obtains the outcome $\omega^{\bar{Y}}$. We denote the eigenvector of $\mathbf{X}^k\mathbf{Z}^l$ with eigenvalue ω^j on system $\mathcal{H}_A$ by $|j\rangle_{\mathbf{X}^k\mathbf{Z}^l,A}$. We define $|j\rangle_{\mathbf{Z}^l\mathbf{X}^{-k},B}$ in the same way. We have

$$|\Phi\rangle = \sum_{j=0}^{p-1}\frac{1}{\sqrt{d}}|j\rangle_{\mathbf{X}^k\mathbf{Z}^l,A}|j\rangle_{\mathbf{Z}^l\mathbf{X}^{-k},B}, \tag{D2}$$

and Eq. (D1) implies that

$$\begin{aligned}
\mathbf{W}(k,l)\mathbf{W}(x,z)|j\rangle_{\mathbf{X}^k\mathbf{Z}^l,A} &= \omega^{xl-zk}\mathbf{W}(x,z)\mathbf{W}(l,k)|j\rangle_{\mathbf{X}^k\mathbf{Z}^l,A} \\
&= \omega^{xl-zk+j}\mathbf{W}(x,z)|j\rangle_{\mathbf{X}^k\mathbf{Z}^l,A}.
\end{aligned} \tag{D3}$$

That is, $\mathbf{W}(x,z)|j\rangle_{\mathbf{X}^k\mathbf{Z}^l,A}$ is a constant times of $|xl-zk+j\rangle_{\mathbf{X}^k\mathbf{Z}^l,A}$. Hence, when we measure operator $\mathbf{X}^k\mathbf{Z}^l$ for state $\mathbf{W}(x,z)|\Phi\rangle$, the outcome $\omega^{Y-\bar{Y}}$ is ω^{xl-zk}.

We consider that state $\rho[P_{XZ}]$ is generated by applying operator $\mathbf{W}(x,z)$ to state $|\Phi\rangle$ with probability $P_{X,Z}(x,z)$. When $\mathbf{W}(x,z)$ is applied, the outcome $\omega^{Y-\bar{Y}}$ is ω^{xl-zk}.

That is, $Y-\bar{Y}$ obeys the distribution P_{lX-kZ}. We define $E[\omega^{lX-kZ}] := \sum_{s=0}^{p-1} \omega^s P_{lX-kZ}(s)$. We define the equivalent relation $(x,z) \sim (x',z')$ in $\mathbb{F}_p^2$ as $(x,z)=(ax',az')$ with an element $a \in \mathbb{F}_p$. Since $P_{lX-kZ}(as) = P_{a(lX-kZ)}(s)$ and $(\mathbb{F}_p^2 \setminus \{0\})/\sim = \{[(1,0)],[(1,1)],\ldots,[(1,p-1)],[(0,1)]\}$, we can calculate $E[\omega^{lX-kZ}]$ only by measuring $P_X, P_{X+Z}, \ldots, P_{X+(p-1)Z}$, and P_Z, which requires $p+1$ types of measurements.

Lemma 5. *We have the relation*

$$P_{X,Z}(l,j) = \frac{1}{d^2}\sum_{b,z} \omega^{-jl+bl-jz} E[\omega^{(b-j)X+zZ}]. \tag{D4}$$

For $z \neq 0$, $E[\omega^{(b-j)X+zZ}]$ can be calculated from the distribution $P_{(b-j)X/z+Z}$, and $E[\omega^{(b-j)X}]$ can be calculated from the distribution P_X. Hence, from $p+1$ distributions $P_X, P_{X+Z}, \ldots, P_{X+(p-1)Z}$, and P_Z, we derive the distribution $P_{X,Z}$.

Proof of Lemma 5: To show Lemma 5, we consider the linear space $\mathcal{V}$ of complex functions on $\mathbb{F}_p^2$ and its dual space $\mathcal{V}^*$. We define $e_{(x,z)} \in \mathcal{V}^*$ as $e_{(x,z)}(f) := f(x,z) \in \mathbb{C}$ for $f \in \mathcal{V}$. Then, we define the following function $\mathcal{F}$ from $\mathcal{V}^*$ to $p \times p$ complex matrices:

$$\mathcal{F}[e_{(x,z)}] := (|x\rangle_{\mathbf{X}\ \mathbf{X}}\langle x|)(|z\rangle_{\mathbf{Z}\ \mathbf{Z}}\langle z|). \tag{D5}$$

We extend $E[\omega^{kX+lZ}]$ as an element of $\mathcal{V}^*$ as

$$E[\omega^{kX+lZ}](f) := \sum_{(x,z)} \omega^{kx+lz} f(x,z). \tag{D6}$$

Hence, it is sufficient to show that $\mathcal{F}$ is invertible and that the following relation holds:

$$(|l\rangle_{\mathbf{X}\ \mathbf{X}}\langle l|)(|j\rangle_{\mathbf{Z}\ \mathbf{Z}}\langle j|) = \frac{1}{p^2}\sum_{b,z} \omega^{-jl+bl-jz} \mathcal{F}[E[\omega^{(b-j)X+zZ}]]. \tag{D7}$$

We have

$$\begin{aligned}
\mathcal{F}[E[\omega^{lX-kZ}]] &= \sum_{j=0}^{d-1} \sum_{(x,z):lx-kz=j} \omega^j (|x\rangle_{\mathbf{X}\ \mathbf{X}}\langle x|)(|z\rangle_{\mathbf{Z}\ \mathbf{Z}}\langle z|) \\
&= \sum_{x,z} \omega^{lx-kz} (|x\rangle_{\mathbf{X}\ \mathbf{X}}\langle x|)(|z\rangle_{\mathbf{Z}\ \mathbf{Z}}\langle z|) \\
&= \left(\sum_x \omega^{lx} |x\rangle_{\mathbf{X}\ \mathbf{X}}\langle x|\right)\left(\sum_s \omega^{-kz} |z\rangle_{\mathbf{Z}\ \mathbf{Z}}\langle z|\right) \\
&= \mathbf{X}^l \mathbf{Z}^{-k}.
\end{aligned} \tag{D8}$$

Since the set $\{\mathbf{X}^l\mathbf{Z}^{-k}\}_{(l,k)}$ spans the set $d \times d$ matrices, the map $\mathcal{F}$ is invertible. In fact, we have

$$\begin{aligned}
&(|l\rangle_{\mathbf{X}\ \mathbf{X}}\langle l|)(|j\rangle_{\mathbf{Z}\ \mathbf{Z}}\langle j|) \\
&= \frac{\omega^{-jl}}{\sqrt{d}} |l\rangle_{\mathbf{X}\ \mathbf{Z}}\langle j| \\
&= \frac{\omega^{-jl}}{\sqrt{p}} \sum_{b=0}^{p-1} \frac{\omega^{bl}}{\sqrt{p}} |b\rangle_{\mathbf{Z}\ \mathbf{Z}}\langle j| \\
&= \frac{\omega^{-jl}}{p} \sum_{b=0}^{p-1} \omega^{bl} \frac{1}{p} \sum_{z=0}^{p-1} \omega^{-jz} \mathbf{X}^{b-j} \mathbf{Z}^z \\
&= \frac{1}{p^2} \sum_{b,z} \omega^{-jl+bl-jz} \mathcal{F}[E[\omega^{(b-j)X+zZ}]],
\end{aligned} \tag{D9}$$

which implies Eq. (D7). ■

2. Case with the general state

Even when ρ_{AB} is not a generalized Bell diagonal state, the resultant state $T(\tau_{AB})$ of discrete twirling (31) is a generalized Bell diagonal state.

When the state is given as the twirled state $T(\tau_{AB})$ and the measurement $M(lX-kZ)$ is applied, the probability with outcome y is

$$\begin{aligned}
&\sum_{j=0}^{p-1} {}_{\mathbf{X}^k\mathbf{Z}^l,A}\langle j+y|\, {}_{\mathbf{Z}^{-l}\mathbf{X}^k,B}\langle j| \frac{1}{d^2} \\
&\quad \times \left(\sum_{x,z} (\mathbf{W}(x,z)_A \otimes \mathbf{W}(x,z)_B^T)\tau_{AB}(\mathbf{W}(x,z)_A \right. \\
&\quad \left. \otimes\, \mathbf{W}(x,z)_B^T)^\dagger\right) |j+y\rangle_{\mathbf{X}^k\mathbf{Z}^l,A} |j\rangle_{\mathbf{Z}^{-l}\mathbf{X}^k,B} \\
&\quad = \sum_{j=0}^{p-1} \frac{1}{d^2} \sum_{x,z} {}_{\mathbf{X}^k\mathbf{Z}^l,A}\langle -xl+zk+j+y|\, {}_{\mathbf{Z}^{-l}\mathbf{X}^k,B} \\
&\quad \langle -xl+zk+j|\tau_{AB}|-xl+zk+j+y\rangle_{\mathbf{X}^k\mathbf{Z}^l,A}| \\
&\quad -xl+zk+j\rangle_{\mathbf{Z}^{-l}\mathbf{X}^k,B} \\
&\quad = \sum_{j=0}^{p-1} {}_{\mathbf{X}^k\mathbf{Z}^l,A}\langle j+y|\, {}_{\mathbf{Z}^{-l}\mathbf{X}^k,B}\langle j|\tau_{AB}|j+y\rangle_{\mathbf{X}^k\mathbf{Z}^l,A}|j\rangle_{\mathbf{Z}^{-l}\mathbf{X}^k,B}.
\end{aligned}$$

That is, the distribution of the outcome with input state (31) is the same as the distribution of the outcome with input state τ_{AB}. Hence, when input state (31) is given as $\rho[P_{XZ}]$, the distribution P_{lX-kZ} can be estimated by applying the measurement $M(lX-kZ)$ to state τ_{AB}.

Note that the twirling operation needs public communication about the choice (x,z). If they apply the twirling operation, Eve can perfectly recover the environment of the twirled state $T(\tau_{AB})$. Therefore, we can analyze the twirled state $T(\tau_{AB})$ for secrecy without applying it. To conclude, we show that we do not need to apply the twirling operation.

APPENDIX E: SEC. V PROOFS

This appendix gives the Sec. V proofs.

1. Proof of Theorem 1

For a CQ state $\rho_{L,E} = \sum_{l\in\mathcal{L}} |l\rangle\langle l| \otimes X_l$ and a function $f: \mathcal{L} \to \mathcal{M}'$, we define the CQ state $f(\rho_{L,E}) := \sum_{l\in\mathcal{L}} |f(l)\rangle\langle f(l)| \otimes X_l$. Recall the expression of $\bar{d}(M'; ES)$ in Eq. (34), where

$$\tau_{M'E|S=s} = \sum_{m'} \frac{1}{\mathsf{M}'} |m'\rangle\langle m'| \otimes \sum_{l\in f_s^{-1}(m')} \frac{1}{\mathsf{L}_2} W_E(l)$$
$$= f_s(W_E \times P_{\mathcal{L}}),$$
$$\tau_{E|S=s} = \mathrm{Tr}_{M'} \tau_{M'E|S=s} = W_E \circ P_{\mathcal{L}}.$$

Then, we introduce the privacy amplification lemma [82].

Lemma 6. *Let $\tau_{LE} \in \mathcal{D}(\mathcal{H}_L \otimes \mathcal{H}_E)$ be classical on L and $\{f_S\}: \mathcal{L} \to \mathcal{M}'$ be a UHF family. Then*

$$\mathbb{E}_S \| f_S(\tau_{LE}) - P_{\mathcal{M}'} \otimes \tau_E \|_1 \le 2^{(1-t)/(1+t)} 2^{[t/(1+t)](\log|\mathcal{M}'| - \tilde{H}^{\uparrow}_{1+t}(L|E)_\tau)}. \quad \text{(E1)}$$

Equation (46) follows immediately upon using the above lemma:

$$d(M'; ES) = \mathbb{E}_S \| \mathrm{id}_E \otimes f_S(W_E \times P_{\mathcal{L}}) - P_{\mathcal{M}'} \otimes W_E \circ P_{\mathcal{L}} \|_1$$
$$\le 2^{(1-t)/(1+t)} 2^{[t/(1+t)](\log \mathsf{M}' - \sup_{\sigma_E} \tilde{H}^{\uparrow}_{1+t}(L|E|W_E \times P_{\mathcal{L}}))}$$
$$= 2^{(1-t)/(1+t)} 2^{[t/(1+t)](-\log b + \tilde{I}^{\downarrow}_{1+t}(L;E|W_E \times P_{\mathcal{L}}))}. \quad \text{(E2)}$$

2. Proofs of Corollaries 1 and 2

The following lemma will be useful in the proofs.

Lemma 7. *For the n-fold channel W_B^n, the following inequalities hold for $t > -1$ and $t > -1/2$, respectively:*

$$\max_{Q_{X^n}} I^{\downarrow}_{1+t}(X^n; B^n | W_B^n \times Q_{X^n}) = n \max_{Q_X} I^{\downarrow}_{1+t}(X; E | W_B \times Q_X), \quad \text{(E3)}$$

$$\max_{Q_{X^n}} \tilde{I}^{\downarrow}_{1+t}(X^n; B^n | W_B^n \times Q_{X^n}) = n \max_{Q_X} \tilde{I}^{\downarrow}_{1+t}(X; B | W_B \times Q_X). \quad \text{(E4)}$$

Proof of Lemma 7: Equation (E3) for the Petz version was shown in Ref. [83], so we focus on Eq. (E4). Before continuing with the proof of Lemma 7, we state the following proposition. ■

Proposition 2 (Proposition 4.2 of Ref. [84]). For $t \ge -1/2$, we have

$$\sup_{Q_X} \tilde{I}^{\downarrow}_{1+t}(X; E | W \times Q_X) = \inf_{\sigma} \sup_{x\in\mathcal{X}} \tilde{D}_{1+t}(W(x)\|\sigma). \quad \text{(E5)}$$

Then, we define the quasi-entropy for convenience,

$$\Xi_{1+t}(\rho\|\sigma) := \mathrm{Tr}(\rho^{-t/2(1+t)}\sigma. \quad \text{(E6)}$$

For $t > -1/2$ and any probability distribution on $\mathcal{X}^n$, we have

$$\tilde{I}^{\downarrow}_{1+t}(X^n; E^n | W^{\otimes n} \times Q_{X^n})$$
$$= \inf_{\omega\in\mathcal{D}(\mathcal{H}_E^{\otimes n})} \frac{1}{t} \log \sum_{x^n\in\mathcal{X}^n} Q_{X^n}(x^n) \Xi_{1+t}(W^{\otimes n}(x^n)\|\omega) \quad \text{(E7)}$$
$$\le \inf_{\sigma\in\mathcal{D}(\mathcal{H}_E)} \frac{1}{t} \log \sum_{x^n\in\mathcal{X}^n} Q_{X^n}(x^n) \Xi_{1+t}(W^{\otimes n}(x^n)\|\sigma^{\otimes n})$$
$$= \inf_{\sigma\in\mathcal{D}(\mathcal{H}_E)} \frac{1}{t} \log \sum_{x^n\in\mathcal{X}^n} Q_{X^n}(x^n) \prod_{i=1}^{n} \Xi_{1+t}(W(x_i)\|\sigma) \quad \text{(E8)}$$
$$\le \inf_{\sigma\in\mathcal{D}(\mathcal{H}_E)} \sup_{x\in\mathcal{X}} \frac{1}{t} \log[\Xi_{1+t}(W(x)\|\sigma)]^n$$
$$= \inf_{\sigma\in\mathcal{D}(\mathcal{H}_E)} \sup_{x\in\mathcal{X}} n\tilde{D}_{1+t}(W(x_i)\|\sigma) \quad \text{(E9)}$$
$$= n \sup_{Q_X} \tilde{I}^{\downarrow}_{1+t}(X; E | W \times Q_X), \quad \text{(E10)}$$

where lines (E7) and (E9) follow from the definitions, line (E8) follows from the multiplicativity of Ξ_{1+t}, and line (E10) follows from Proposition 2.

By using Lemma 7, we have

$$\max_{Q_{X^n}} I_{1-t}(X^n; B^n | W_B^n \times Q_{X^n}) \ge \max_{Q_{X^n}} I^{\downarrow}_{1-t}(X^n; B^n | W_B^n \times Q_{X^n}) \quad \text{(E11)}$$
$$= n \max_{Q_X} I^{\downarrow}_{1-t}(X; B | W_B \times Q_X), \quad \text{(E12)}$$

where line (E11) follows by definition. Equation (49) is obtained by substituting the above inequality into Eq. (48). Hence, we obtain Corollary 1.

Combining Eqs. (7) and (E4), we obtain the bound

$$\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times P_{\mathcal{L}})\le n\max_{Q_X}\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times Q_X),\tag{E13}$$

where $P_{\mathcal{L}}$ is a distribution on $\mathcal{X}^n$ such that, for $x^n\in\mathcal{L}$, $P_{\mathcal{L}}(x^n)=1/|\mathcal{L}|$. Substituting Eq. (E13) into Eq. (46) yields Eq. (50). Hence, we obtain Corollary 2.

3. Proof of Theorem 2

For a given distribution Q_X on $\mathcal{X}$, we have

$$2^{t\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times Q_X)}=\inf_{\sigma\in\mathcal{D}(\mathcal{H}_E)}\sum_{x\in\mathcal{X}}Q_X(x)\Xi_{1+t}(W_E(x)\|\sigma).\tag{E14}$$

Given two distributions Q_X and $\bar{Q}_X$ and $0<\lambda<1$, we have

$$\begin{aligned}
&2^{t\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times(\lambda Q_X+(1-\lambda)\bar{Q}_X)}\\
&=\min_{\sigma\in\mathcal{D}(\mathcal{H}_E)}\Bigg(\sum_{x\in\mathcal{X}}(\lambda Q_X(x) \qquad\qquad (E15)\\
&\quad+(1-\lambda)\bar{Q}_X(x))\Xi_{1+t}(W_E(x)\|\sigma)\Bigg)\\
&\ge\lambda\min_{\sigma\in\mathcal{D}(\mathcal{H}_E)}\Bigg(\sum_{x\in\mathcal{X}}Q_X(x)\Xi_{1+t}(W_E(x)\|\sigma)\Bigg)\\
&\quad+(1-\lambda)\min_{\sigma\in\mathcal{D}(\mathcal{H}_E)}\Bigg(\sum_{x\in\mathcal{X}}\bar{Q}_X(x)\Xi_{1+t}(W_E(x)\|\sigma)\Bigg)\\
&=\lambda 2^{t\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times Q_X)}+(1-\lambda)2^{t\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times\bar{Q}_X)},
\end{aligned}\tag{E16}$$

which implies that the map $Q_X\mapsto 2^{t\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times Q_X)}$ is concave.

Given an element $x_0\in\mathcal{X}=G$, we define the distribution Q_{X,x_0} and the CQ channels W_{E,x_0} and $U_{x_0}(W_E)$ as $Q_{X,x_0}(x):=Q_X(x_0x)$, $W_{E,x_0}(x):=W_{E,x}(x_0x)$, $U_{x_0}\circ W_E)(x):=U_{x_0}W_E(x)U_{x_0}^{\dagger}$, respectively. Then, we have

$$\begin{aligned}
\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times Q_X)&=\tilde{I}^{\downarrow}_{1+t}(X;E|W_{E,x_0}\times Q_{X,x_0})\\
&=\tilde{I}^{\downarrow}_{1+t}(X;E|U_{x_0}\circ W_E\times Q_{X,x_0})\\
&=\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times Q_{X,x_0}),
\end{aligned}\tag{E17}$$

where the second equality follows from the unitary invariance of quasientropy and the last inequality follows from the symmetric condition $W_E(x)=U_x\rho_0U_x^{\dagger}$. Because of Eqs. (E16) and (E15), the uniform distribution $P_{\mathcal{X}}$ on $\mathcal{X}$ satisfies

$$\begin{aligned}
2^{t\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times Q_X)}&=\frac{1}{|\mathcal{X}|}\sum_{x_0\in\mathcal{X}}2^{t\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times Q_{X,x_0})}\\
&\le 2^{t\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times P_{\mathcal{X}})}.
\end{aligned}\tag{E18}$$

Thus, we have

$$\max_{P_X}\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times P_X)=\tilde{I}^{\downarrow}_{1+t}(X;E|W_E\times P_{\mathcal{X}}).\tag{E19}$$

Combining Eqs. (46) and (E18) implies Eq. (51).

4. Proof of Lemma 2

It is known that the capacity of the degraded wiretap channel is $\sup_{Q_X}I(X;\hat{B})_{Q_X}-I(X;\hat{E})_{Q_X}$ [42],[60, Eq. (9.75)]. Also, in this case, For $x_0\in\mathcal{X}$, we define the distribution Q_{X,x_0} as $Q_{X,x_0}(x):=Q_X(x_0x)$. Because of the symmetric condition, we find that

$$I(X;\hat{B})_{Q_X}-I(X;\hat{E})_{Q_X}=I(X;\hat{B})_{Q_{X,x_0}}-I(X;\hat{E})_{Q_{X,x_0}}.\tag{E20}$$

Since $\sum_{x_0\in\mathcal{X}}Q_{X,x_0}/|\mathcal{X}|=P_{\mathcal{X}}$ and the map $Q_X\mapsto I(X;\hat{B})_{Q_X}-I(X;\hat{E})_{Q_X}$ is known to be concave for degraded channels [60, Eq. (9.76)], we have

$$\begin{aligned}
&I(X;\hat{B})_{P_{\mathcal{X}}}-I(X;\hat{E})_{P_{\mathcal{X}}}\\
&\ge\sum_{x_0\in\mathcal{X}}\frac{1}{|\mathcal{X}|}(I(X;\hat{B})_{Q_{X,x_0}}-I(X;\hat{E})_{Q_{X,x_0}})\\
&=I(X;\hat{B})_{Q_X}-I(X;\hat{E})_{Q_X}.
\end{aligned}$$

Hence, $\sup_{Q_X}I(X;\hat{B})_{Q_X}-I(X;\hat{E})_{Q_X}=I(X;\hat{B})_{P_{\mathcal{X}}}-I(X;\hat{E})_{P_{\mathcal{X}}}$. This completes the proof of Lemma 2.

APPENDIX F: PROOF OF LEMMA 3

Recall the definition of C,

$$c=g_{s'}(m,y)=y+T(s')m.\tag{F1}$$

For fixed s',m, the map between y and c is bijective, so we have the function $y=y(m,s',c)$. Then, we evaluate $d(M;E'S'C)$ as

$$
\begin{aligned}
d(M;EAS'C) &= \min_{\sigma_{EAS'C}} \|\tau_{MEAS'C} - P_{\mathcal{M}} \otimes \sigma_{EAS'C}\|_1 \\
&\leq \min_{\{\sigma_{EA,Y=y,M=m}\}_{m,y}} \Bigg\| \sum_{s',m,y} P_{\mathcal{M}}(m)P_{\mathcal{S}'}(s')P_{\mathcal{Y}}(y)|m\rangle\langle m| \otimes \tau_{EA,Y=y,M=m} \otimes |s'\rangle\langle s'| \otimes |g_{s'}(m,y)\rangle\langle g_{s'}(m,y)| \\
&\quad - \left(\sum_m P_{\mathcal{M}}(m)|m\rangle\langle m|\right) \otimes \left(\sum_{s',m,y} P_{\mathcal{M}}(m)P_{\mathcal{S}'}(s')P_{\mathcal{Y}}(y)\sigma_{EA,Y=y,M=m} \otimes |s'\rangle\langle s'| \otimes |g_{s'}(m,y)\rangle\langle g_{s'}(m,y)|\right)\Bigg\|_1 \\
&= \min_{\{\sigma_{EA,Y=y,M=m}\}_{m,y}} \Bigg\| \sum_{s',m,c} P_{\mathcal{M}}(m)P_{\mathcal{S}'}(s')P_{\mathcal{Y}}(c)|m\rangle\langle m| \otimes \tau_{EA,Y=y(m,s',c),M=m} \otimes |s'\rangle\langle s'| \otimes |c\rangle\langle c| - \left(\sum_m P_{\mathcal{M}}(m)|m\rangle\langle m|\right) \\
&\quad \otimes \left(\sum_{s',m,c} P_{\mathcal{M}}(m)P_{\mathcal{S}'}(s')P_{\mathcal{Y}}(c)\sigma_{EA,Y=y(m,s',c),M=m} \otimes |s'\rangle\langle s'| \otimes |c\rangle\langle c|\right)\Bigg\|_1 \\
&= \min_{\{\sigma_{EA,Y=y,M=m}\}_{m,y}} \sum_{s',c} P_{\mathcal{S}'}(s')P_{\mathcal{Y}}(c) \Bigg\| \sum_m P_{\mathcal{M}}(m)|m\rangle\langle m| \otimes \tau_{EA,Y=y(m,s',c),M=m} - \left(\sum_m P_{\mathcal{M}}(m)|m\rangle\langle m|\right) \\
&\quad \otimes \left(\sum_m P_{\mathcal{M}}(m)\sigma_{EA,Y=y(m,s',c),M=m}\right)\Bigg\|_1 \\
&= \min_{\{\sigma_{EA,Y=y,M=m}\}_{m,y}} \sum_{s',y} P_{\mathcal{S}'}(s')P_{\mathcal{Y}}(y) \Bigg\| \sum_m P_{\mathcal{M}}(m)|m\rangle\langle m| \otimes \tau_{EA,Y=y,M=m} - \left(\sum_m P_{\mathcal{M}}(m)|m\rangle\langle m|\right) \\
&\quad \otimes \left(\sum_m P_{\mathcal{M}}(m)\sigma_{EA,Y=y,M=m}\right)\Bigg\|_1 \\
&= \min_{\{\sigma_{EA,Y=y,M=m}\}_{m,y}} \sum_{s'} P_{\mathcal{S}'}(s') \Bigg\| \sum_{m,y} P_{\mathcal{Y}}(y)P_{\mathcal{M}}(m)|m,y\rangle\langle m,y| \otimes \tau_{EA,Y=y,M=m} - \sum_y P_{\mathcal{Y}}(y)\left(\sum_m P_{\mathcal{M}}(m)|m,y\rangle\langle m,y|\right) \\
&\quad \otimes \left(\sum_m P_{\mathcal{M}}(m)\sigma_{EA,Y=y,M=m}\right)\Bigg\|_1 \\
&\leq \min_{\{\sigma_{EA,M=m}\}_m} \sum_{s'} P_{\mathcal{S}'}(s') \Bigg\| \sum_{m,y} P_{\mathcal{Y}}(y)P_{\mathcal{M}}(m)|m,y\rangle\langle m,y| \otimes \tau_{EA,Y=y,M=m} - \sum_y P_{\mathcal{Y}}(y)\left(\sum_m P_{\mathcal{M}}(m)|m,y\rangle\langle m,y|\right) \\
&\quad \otimes \left(\sum_m P_{\mathcal{M}}(m)\sigma_{EA,M=m}\right)\Bigg\|_1 \\
&= \min_{\{\sigma_{EA,M=m}\}_m} \sum_{s'} P_{\mathcal{S}'}(s') \Bigg\| \sum_{m,y} P_{\mathcal{Y}}(y)P_{\mathcal{M}}(m)|m,y\rangle\langle m,y| \otimes \tau_{EA,Y=y,M=m} - \left(\sum_{m,y} P_{\mathcal{M}}(m)P_{\mathcal{Y}}(y)|m,y\rangle\langle m,y|\right) \\
&\quad \otimes \left(\sum_m P_{\mathcal{M}}(m)\sigma_{EA,M=m}\right)\Bigg\|_1 \\
&= \min_{\sigma_{EA}} \sum_{s'} P_{\mathcal{S}'}(s') \Bigg\| \sum_{m,y} P_{\mathcal{Y}}(y)P_{\mathcal{M}}(m)|m,y\rangle\langle m,y| \otimes \tau_{EA,Y=y,M=m} - \left(\sum_{m,y} P_{\mathcal{M}}(m)P_{\mathcal{Y}}(y)|m,y\rangle\langle m,y|\right) \otimes \sigma_{EA}\Bigg\|_1 \\
&= d(M';EA).
\end{aligned}
$$

Then, we obtain Eq. (61).

APPENDIX G: PROOF OF LEMMA 4

Define

$$\omega_{XAE} = W_E \times P_{\mathcal{X}} = \sum_{x\in\mathcal{X}} \frac{1}{|\mathcal{X}|}|x\rangle\langle x| \otimes U_x \tau_{AE} U_x^\dagger. \tag{G1}$$

By definition,

$$\tilde{I}_{1+t}^{\downarrow}(X;AE|\omega_{XAE}) = \min_{\sigma_{AE}} \frac{1}{t} \log \Xi_{1+t}(\omega_{XAE}\|\omega_X \otimes \sigma_{AE}). \tag{G2}$$

Note that ω_{XAE} is invariant under group operation $\{U_x\}_{x\in\mathcal{X}}$ and quasientropy $\Xi_{1+t}(\cdot\|\cdot)$ [see Eq. (E6) for a definition] is invariant under the unitary operation. Thus, the minimizer σ_{AE} is also invariant under group operation $\{U_x\}_{x\in\mathcal{X}}$, which means that it takes the form $\sigma_{AE} = I_A/d_A$. Then we have

$$\begin{aligned}
&\tilde{I}_{1+t}^{\downarrow}(X;AE|\omega_{XAE})\\
&= \min_{\sigma_E} \frac{1}{t} \log \Xi_{1+t}\left(\omega_{XAE}\|\omega_X \otimes \frac{I_A}{d_A} \otimes \sigma_E\right)\\
&= \min_{\sigma_E} \frac{1}{t} \log \frac{d_A^s}{|\mathcal{X}|} \sum_x \Xi_{1+t}(U_x\tau_{AE}U_x^\dagger\|\sigma_E)\\
&= \log d_A - \tilde{H}_{1+t}^{\uparrow}(A|E|\tau_{AE}).
\end{aligned} \tag{G3}$$

APPENDIX H: PROOF OF THEOREM 4

Recall that an achievable rate for the wire-tap channel requires that $\epsilon(W_B) = \Pr[M \neq \hat{M}]$ and $\bar{d}(M;E)$ go to zero asymptotically. An achievable rate for the PDC protocol requires that ϵ_C, ϵ_E and ϵ_B go to zero asymptotically. We prove Theorem 4 by showing the conversion between these conditions.

Protocol 4 gives a conversion from a specific wire-tap code to a PDC protocol. However, this type of conversion can be made for any wire-tap code. Since the consumed length for covering variable Y is negligible in comparison with n, we have the "$\leq$" relation in Eq. (74).

Conversely, the asymptotic setting of the PDC model requires the following. Alice transmits her message with asymptotically zero error under n times use of the channel W_B. Also, when Eve receives her information via n times use of the channel W_E, Eve obtains no information about Alice's message.

Now, we consider a PDC protocol P_n that is ϵ_C complete, ϵ_E secure, and ϵ_B reliable with a message $M \in \mathcal{M}$ and a random variable $S \in \mathcal{S}$ to be sent via the public channel. We have a conditional distribution $P_{G^n|M,S}$ such that Alice chooses an element $(g_1,\ldots,g_n) \in G^n$ subject to $P_{G^n|M,S}$ and applies $U_{g_1} \otimes \cdots \otimes U_{g_n}$ dependently of S and M. Also, we denote the decoder Π^S dependently of S.

In the following, we consider the case when the channel from Alice to Bob is $\Lambda_A^{\otimes n}$. We denote the recovered message by Bob by $\hat{M}$. Then, we have

$$\begin{aligned}
\Pr[M \neq \hat{M}] &= \Pr[M \neq \hat{M}, \mathrm{Ab}^c] + \Pr[M \neq \hat{M}, \mathrm{Ab}]\\
&\leq \Pr[\mathrm{Ab}^c\,|M \neq \hat{M}] + \Pr[\mathrm{Ab}]\\
&\leq \epsilon_B + \epsilon_C,
\end{aligned} \tag{H1}$$

Also, there exists a distribution Q_S of S such that

$$\|P_{S,M} - P_M \times Q_S\|_1 \leq \epsilon_E, \tag{H2}$$

which implies that

$$\|P_S - Q_S\|_1 \leq \epsilon_E. \tag{H3}$$

Thus, we have

$$\|P_{S,M} - P_M \times P_S\|_1 \leq 2\epsilon_E. \tag{H4}$$

Hence, we have

$$\begin{aligned}
&\sum_{s\in\mathcal{S}} P_S(s)(P(M \neq \hat{M}|S=s) + \|P_{M|S=s} - P_M\|_1)\\
&\quad \leq 2\epsilon_E + \epsilon_B + \epsilon_C.
\end{aligned} \tag{H5}$$

When $S = s$ and the distribution $P_{M|S=s}$ is replaced by P_M, we denote the decoding error probability by $\Pr[M \neq \hat{M}|S=s][P_M]$. Then, we have

$$\begin{aligned}
&\Pr[M \neq \hat{M}|S=s][P_M]\\
&\quad \leq \Pr[M \neq \hat{M}|S=s][P_{M|S=s}] + \|P_{M|S=s} - P_M\|_1\\
&\quad = \Pr[M \neq \hat{M}|S=s] + \|P_{M|S=s} - P_M\|_1.
\end{aligned} \tag{H6}$$

That is, we have

$$\sum_{s\in\mathcal{S}} P_S(s) \Pr[M \neq \hat{M}|S=s][P_M] \leq 2\epsilon_E + \epsilon_B + \epsilon_C. \tag{H7}$$

In the following, we consider the case when Eve intercepts the transmitted state. There exists a state σ_{SE} such that

$$\|\rho_{MSE} - P_M \otimes \sigma_{SE}\| \leq \epsilon_E. \tag{H8}$$

For the same reason as used above in Eq. (H4), we have

$$\|\rho_{MSE} - P_M \otimes \rho_{SE}\| \le 2\epsilon_E. \tag{H9}$$

We define the joint state $\bar{\rho}_{MSE}$ as

$$\bar{\rho}_{MSE} := \sum_{s\in\mathcal{S}, m\in\mathcal{M}} P_M(m) P_S(s) |m,s\rangle\langle m,s| \otimes \rho_{E|M=m,S=s}. \tag{H10}$$

Then, we have

$$\begin{aligned}
&\|\bar{\rho}_{MSE} - P_M \otimes \rho_{SE}\|_1 \\
&\quad\le \|\bar{\rho}_{MSE} - \rho_{MSE}\|_1 + \|\rho_{MSE} - P_M \otimes \rho_{SE}\|_1 \\
&\quad\le \|P_{S,M} - P_M \times P_S\|_1 + \|\rho_{MSE} - P_M \otimes \rho_{SE}\|_1 \\
&\quad\le 4\epsilon_E.
\end{aligned} \tag{H11}$$

That is,

$$\sum_{s\in\mathcal{S}} P_S(s) \|\bar{\rho}_{ME|S=s} - P_M \otimes \rho_{E|S=s}\|_1 \le 4\epsilon_E. \tag{H12}$$

Because of Eqs. (H7) and (H12) and the Markov inequality, there exists $s_0 \in \mathcal{S}$ such that

$$P(M \neq \hat{M}|S = s_0)[P_M] \le 3(2\epsilon_E + \epsilon_B + \epsilon_C), \tag{H13}$$

$$\|\bar{\rho}_{ME|S=s_0} - P_M \otimes \rho_{E|S=s_0}\|_1 \le 12\epsilon_E. \tag{H14}$$

Similarly as above for Eq. (H4), we have

$$\|\bar{\rho}_{ME|S=s_0} - P_M \otimes \bar{\rho}_{E|S=s_0}\|_1 \le 24\epsilon_E. \tag{H15}$$

Now, as our wire-tap encoder, we choose $P_{G^n|M=m,S=s_0}$ for each message $m \in \mathcal{M}$. We choose Π^{s_0} as our wire-tap decoder. The decoding error probability of this wire-tap code is evaluated by Eq. (H13), and the information leakage of this wire-tap code is evaluated by Eq. (H15). Hence, we have the "$\ge$" relation in Eq. (74).

[1] Charles H. Bennett and Stephen J. Wiesner, Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States, Phys. Rev. Lett. **69**, 2881 (1992).

[2] Tohya Hiroshima, Optimal dense coding with mixed state entanglement, J. Phys. A: Math. Gen. **34**, 6907 (2001).

[3] Michal Horodecki, Pawel Horodecki, Ryszard Horodecki, Debbie Leung, and Barbara Terhal, Classical capacity of a noiseless quantum channel assisted by noisy entanglement, P Soc Photo-Opt Ins **1**, 70 (2001).

[4] Xiao Shu Liu, Gui Lu Long, Dian Min Tong, and Feng Li, General scheme for superdense coding between multiparties, Phys. Rev. A **65**, 022304 (2002).

[5] Eyuri Wakakuwa, Superdense coding in resource theory of asymmetry, arXiv preprint arXiv:2002.01603 (2020).

[6] Kun Wang and Masahito Hayashi, Permutation enhances classical communication assisted by entangled states, IEEE Trans. Inf. Theory **67**, 3905 (2021).

[7] Masahito Hayashi and Kun Wang, Dense coding with locality restriction for decoder: Quantum encoders vs. super-quantum encoders, arXiv preprint arXiv:2109.12518 (2021).

[8] Fu-Guo Deng, Gui Lu Long, and Xiao Shu Liu, Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block, Phys. Rev. A **68**, 042317 (2003).

[9] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Phys. Rev. Lett. **76**, 722 (1996).

[10] Charles H. Bennett, Herbert J. Bernstein, Sandu Popescu, and Benjamin Schumacher, Concentrating partial entanglement by local operations, Phys. Rev. A **53**, 2046 (1996).

[11] Keiji Matsumoto and Masahito Hayashi, Universal distortion-free entanglement concentration, Phys. Rev. A **75**, 062338 (2007).

[12] Yu-Bo Sheng and Fu-Guo Deng, One-step deterministic polarization-entanglement purification using spatial entanglement, Phys. Rev. A **82**, 044305 (2010).

[13] Hoi-Kwong Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[14] Xiao-Min Hu, Cen-Xiao Huang, Yu-Bo Sheng, Lan Zhou, Bi-Heng Liu, Yu Guo, Chao Zhang, Wen-Bo Xing, Yun-Feng Huang, Chuan-Feng Li, and Guang-Can Guo, Long-Distance Entanglement Purification for Quantum Communication, Phys. Rev. Lett. **126**, 010503 (2021).

[15] Cen-Xiao Huang, Xiao-Min Hu, Bi-Heng Liu, Lan Zhou, Yu-Bo Sheng, Chuan-Feng Li, and Guang-Can Guo, Experimental one-step deterministic polarization entanglement purification, Sci. Bull. **67**, 593 (2022).

[16] Gui Lu Long and Xiao Shu Liu, An efficient high capacity quantum key distribution scheme, arXiv preprint arXiv:0012056 (2000).

[17] Gui-Lu Long and Xiao Shu Liu, Theoretically efficient high-capacity quantum-key-distribution scheme, Phys. Rev. A **65**, 032302 (2002).

[18] Fu-Guo Deng and Gui Lu Long, Secure direct communication with a quantum one-time pad, Phys. Rev. A **69**, 052319 (2004).

[19] Gilad Gour, Iman Marvian, and Robert W. Spekkens, Measuring the quality of a quantum reference frame: The relative entropy of frameness, Phys. Rev. A **80**, 012307 (2009).

[20] Eyuri Wakakuwa, Symmetrizing cost of quantum states, Phys. Rev. A **95**, 032328 (2017).

[21] Iman Marvian and Robert W. Spekkens, Asymmetry properties of pure quantum states, Phys. Rev. A **90**, 014102 (2014).

[22] Borzu Toloui, Gilad Gour, and Barry C. Sanders, Constructing monotones for quantum phase references in totally dephasing channels, Phys. Rev. A **84**, 022322 (2011).

[23] Marco Piani, Marco Cianciaruso, Thomas R. Bromley, Carmine Napoli, Nathaniel Johnston, and Gerardo Adesso,

Robustness of asymmetry and coherence of quantum states, Phys. Rev. A **93**, 042107 (2016).

[24] Ryuji Takagi, Skew informations from an operational view via resource theory of asymmetry, Sci. Rep. **9**, 14562 (2019).

[25] Kamil Korzekwa, Zbigniew Puchała, Marco Tomamichel, and Karol Życzkowski, Encoding classical information into quantum resources, IEEE Trans. Inf. Theory (2022).

[26] N. Cai, A. Winter, and R. W. Yeung, Quantum privacy and quantum wiretap channels, Probl. Peredachi Inf. **40**, 318 (2004).

[27] Igor Devetak, The private classical capacity and quantum capacity of a quantum channel, IEEE Trans. Inf. Theory **51**, 44 (2005).

[28] Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal, Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem, IEEE Trans. Inf. Theory **48**, 2637 (2002).

[29] Charles H. Bennett, Igor Devetak, Aram W. Harrow, Peter W. Shor, and Andreas Winter, The quantum reverse Shannon theorem and resource tradeoffs for simulating quantum channels, IEEE Trans. Inf. Theory **60**, 2926 (2014).

[30] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[31] Masahito Hayashi and Toyohiro Tsurumaru, Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths, New J. Phys. **14**, 093014 (2012).

[32] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, Simple and tight device-independent security proofs, SIAM J. Comput. **48**, 181 (2019).

[33] Marco Tomamichel and Anthony Leverrier, A largely self-contained and complete security proof for quantum key distribution, Quantum **1**, 14 (2017).

[34] Chi-Hang Fred Fung, Xiongfeng Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, Phys. Rev. A **81**, 012318 (2010).

[35] Benjamin Schumacher and Michael D. Westmoreland, Quantum mutual information and the one-time pad, Phys. Rev. A **74**, 042305 (2006).

[36] Ruoyang Qi, Zhen Sun, Zaisheng Lin, Penghao Niu, Wentao Hao, Liyuan Song, Qin Huang, Jiancun Gao, Liguo Yin, and Gui-Lu Long, Implementation and security analysis of practical quantum secure direct communication, Light: Sci. Appl. **8**, 22 (2019).

[37] Jiawei Wu, Zaisheng Lin, Liuguo Yin, and Gui-Lu Long, Security of quantum secure direct communication based on Wyner's wiretap channel theory, Quantum Eng. **1**, e26 (2019).

[38] Kunal Sharma, Eyuri Wakakuwa, and Mark M. Wilde, Conditional Quantum One-Time Pad, Phys. Rev. Lett. **124**, 050503 (2020).

[39] Siddhartha Das, Bipartite quantum interactions: Entangling and information processing abilities, arXiv preprint arXiv:1901.05895 (2000).

[40] Zhen Sun, Liyuan Song, Qin Huang, Liuguo Yin, Guilu Long, Jianhua Lu, and Lajos Hanzo, Toward practical quantum secure direct communication: A quantum-memory-free protocol and code design, IEEE Trans. Commun. **68**, 5778 (2020).

[41] Zhen Sun, Ruoyang Qi, Zaisheng Lin, Liuguo Yin, Guilu Long, and Jianhua Lu, in *2018 IEEE Globecom Workshops (GC Wkshps)* (2018), p. 1.

[42] Igor Devetak and Peter W. Shor, The capacity of a quantum channel for simultaneous transmission of classical and quantum information, Commun. Math. Phys. **256**, 287 (2005).

[43] Masahito Hayashi, Quantum wiretap channel with non-uniform random number and its exponent and equivocation rate of leaked information, IEEE Trans. Inf. Theory **61**, 5595 (2015).

[44] Aaron D. Wyner, The wire-tap channel, Bell Syst. Tech. J. **54**, 1355 (1975).

[45] Imre Csiszár and János Körner, Broadcast channels with confidential messages, IEEE Trans. Inf. Theory **24**, 339 (1978).

[46] Imre Csiszár, Almost independence and secrecy capacity, Probl. Peredachi Inf. **32**, 40 (1996).

[47] Haoyu Qi, Kunal Sharma, and Mark M. Wilde, Entanglement-assisted private communication over quantum broadcast channels, J. Phys. A: Math. Theor. **51**, 374001 (2018).

[48] Stefan Bäuml, Siddhartha Das, and Mark M. Wilde, Fundamental Limits on the Capacities of Bipartite Quantum Interactions, Phys. Rev. Lett. **121**, 250504 (2018).

[49] Siddhartha Das, Stefan Bäuml, and Mark M. Wilde, Entanglement and secret-key-agreement capacities of bipartite quantum interactions and read-only memory devices, Phys. Rev. A **101**, 012344 (2020).

[50] Chuan Wang, Fu-Guo Deng, Yan-Song Li, Xiao-Shu Liu, and Gui Lu Long, Quantum secure direct communication with high-dimension quantum superdense coding, Phys. Rev. A **71**, 044305 (2005).

[51] Masahito Hayashi, Exponential decreasing rate of leaked information in universal random privacy amplification, IEEE Trans. Inf. Theory **57**, 3989 (2011).

[52] Ángeles Vázquez-Castro and Masahito Hayashi, Physical layer security for RF satellite channels in the finite-length regime, IEEE Trans. Inf. Forensics Security **14**, 981 (2019).

[53] Masahito Hayashi and Ángeles Vázquez-Castro, Two-way physical layer security protocol for Gaussian channels, IEEE Trans. Commun. **68**, 3068 (2020).

[54] Masahito Hayashi, Secret communication method and secret communication device thereof, U.S. patent US8239 680B2, (Aug. 2012).

[55] Jacob Cohen, Chapter 3 - the significance of a product moment rs. In Jacob Cohen, editor, *Statistical Power Analysis for the Behavioral Sciences*. (Academic Press, 1977).

[56] Dénes Petz, Quasi-entropies for finite quantum systems, Rep. Math. Phys. **23**, 57 (1986).

[57] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel, On quantum Rényi entropies: A new generalization and some properties, J. Math. Phys. **54**, 122203 (2013).

[58] Mark M. Wilde, Andreas Winter, and Dong Yang, Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy, Commun. Math. Phys. **331**, 593 (2014).

[59] Huzihiro Araki, On an inequality of Lieb and Thirring, Lett. Math. Phys. **19**, 167 (1990).
[60] Masahito Hayashi, *Quantum Information Theory: Mathematical Foundation.* (Springer, Berlin Heidelberg, 2016).
[61] Igor Devetak and Andreas Winter, Distillation of secret key and entanglement from quantum states, Proc. Roy. Soc. A Math. Phys. Eng. Sci. **461**, 207 (2005).
[62] Masahito Hayashi, *A Group Theoretic Approach to Quantum Information.* (Springer, Berlin, 2017).
[63] Mitsuru Hamada, Teleportation and entanglement distillation in the presence of correlation among bipartite mixed states, Phys. Rev. A **68**, 012301 (2003).
[64] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, Mixed-state entanglement and quantum error correction, Phys. Rev. A **54**, 3824 (1996).
[65] Masahito Hayashi and Ryutaroh Matsumoto, in *2010 IEEE International Symposium on Information Theory* (2010), p. 2538.
[66] Andrew Thangaraj, Souvik Dihidar, A. R. Calderbank, Steven W. McLaughlin, and Jean-Marc Merolla, Applications of LDPC codes to the wiretap channel, IEEE Trans. Inf. Theory **53**, 2933 (2007).
[67] Hessam Mahdavifar and Alexander Vardy, Achieving the secrecy capacity of wiretap channels using polar codes, IEEE Trans. Inf. Theory **57**, 6428 (2011).
[68] Demijan Klinc, Jeongseok Ha, Steven W. McLaughlin, João Barros, and Byung-Jae Kwak, LDPC codes for the Gaussian wiretap channel, IEEE Trans. Inf. Forensics Security **6**, 532 (2011).
[69] Masahito Hayashi, Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding, Phys. Rev. A **76**, 062301 (2007).
[70] Masahito Hayashi, Quantum-inspired secure wireless communication protocol under spatial and local Gaussian noise assumptions, ArXiv e-prints arXiv:1604.00635 (2016).
[71] Masahito Hayashi and Toyohiro Tsurumaru, More efficient privacy amplification with less random seeds via dual universal hash function, IEEE Trans. Inf. Theory **62**, 2213 (2016).
[72] Erdal Arikan, Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels, IEEE Trans. Inf. Theory **55**, 3051 (2009).
[73] Eren Şaşoğlu, Emre Telatar, and Erdal Arikan, in *2009 IEEE Information Theory Workshop* (2009), p. 144.
[74] Ryuhei Mori and Toshiyuki Tanaka, in *2010 IEEE International Symposium on Information Theory* (2010), p. 894.
[75] Ryuhei Mori and Toshiyuki Tanaka, Source and channel polarization over finite fields and Reed–Solomon matrices, IEEE Trans. Inf. Theory **60**, 2720 (2014).
[76] Wei Zhang, Dong-Sheng Ding, Yu-Bo Sheng, Lan Zhou, Bao-Sen Shi, and Guang-Can Guo, Quantum Secure Direct Communication with Quantum Memory, Phys. Rev. Lett. **118**, 220501 (2017).
[77] Feng Zhu, Wei Zhang, Yubo Sheng, and Yidong Huang, Experimental long-distance quantum secure direct communication, Sci. Bull. **62**, 1519 (2017).
[78] Zhantong Qi, Yuanhua Li, Yiwen Huang, Juan Feng, Yuanlin Zheng, and Xianfeng Chen, A 15-user quantum secure direct communication network, Light: Sci. Appl. **10**, 183 (2021).
[79] Bi-Xue Wang, Ming-Jie Tao, Qing Ai, Tao Xin, Neill Lambert, Dong Ruan, Yuan-Chung Cheng, Franco Nori, Fu-Guo Deng, and Gui-Lu Long, Efficient quantum simulation of photosynthetic light harvesting, Npj Quantum Inf. **4**, 52 (2018).
[80] Lan Zhou and Yu-Bo Sheng, One-step device-independent quantum secure direct communication, Sci. China Phys. Mech. Astron. **65**, 250311 (2022).
[81] Yu-Bo Sheng, Lan Zhou, and Gui-Lu Long, One-step quantum secure direct communication, Sci. Bull. **67**, 367 (2022).
[82] Frédéric Dupuis, Privacy amplification and decoupling without smoothing, *ArXiv e-prints* arxiv:2105.05342 (2021).
[83] Tomohiro Ogawa and Hiroshi Nagaoka, Strong converse to the quantum channel coding theorem, IEEE Trans. Inf. Theory **45**, 2486 (1999).
[84] Milán Mosonyi and Tomohiro Ogawa, Strong converse exponent for classical-quantum channel coding, Commun. Math. Phys. **355**, 373 (2017).