

Resource state distillation via stabilizer channels

Christopher Popp^{1,*}, Tobias C. Sutter^{1,†} and Beatrix C. Hiesmayr^{2,‡}¹*University of Vienna, Faculty of Physics, Währingerstrasse 17, 1090 Vienna, Austria*²*IT:U Interdisciplinary Transformation University, Freistädter Strasse 400, 4040 Linz, Austria*

(Received 25 March 2026; accepted 11 June 2026; published 7 July 2026)

Quantum technologies rely on high-quality resource states, such as maximally entangled or private states, which are indispensable for quantum communication and cryptography. In practice, however, these states are inevitably degraded by noise. Distillation protocols aim to recover high-resource states from multiple imperfect copies, and while stabilizer-based methods have demonstrated high performance in entanglement purification, they have yet to be established for broader tasks such as secret-key distillation. This work introduces a unified framework for stabilizer-based resource distillation in systems of prime local dimension. By formulating stabilizer routines as quantum channels and deriving closed-form expressions for their output, we enable the application of stabilizer operations to general input states and diverse distillation objectives. We identify key invariances in resource measures—such as coherent and private information—and demonstrate how they can be leveraged to significantly reduce the numerical complexity of channel optimization. To illustrate the framework’s versatility, we introduce several protocols: gF-IMAX for general fidelity optimization, and (S)CI-IMAX and (S)PI-IMAX for optimizing (smooth) coherent and private information in both asymptotic and one-shot regimes. Our numerical results confirm that these protocols effectively tailor stabilizer channels to specific operational tasks, establishing them as a flexible tool for quantum resource distillation in highly noisy environments.

DOI: [10.1103/78nk-n9sm](https://doi.org/10.1103/78nk-n9sm)

I. INTRODUCTION

Quantum information processing relies fundamentally on the availability of suitable quantum resources [1]. Depending on the task, these resources may take the form of static objects such as quantum states or dynamic objects such as quantum channels [2]. Static resources include entangled states [3], private or secret-key states [4], and more exotic forms such as data-hiding [5] or -locking [6] states. Each of these enables specific operational advantages, from quantum communication to cryptographic security (see Ref. [2]). Realistic quantum systems are inevitably affected by noise and imperfections. The process of transforming many noisy states into fewer, highly resourceful ones is called distillation and plays a central role in quantum communication and cryptography [7].

Two prominent examples are entanglement distillation (also named entanglement purification) [8], which aims to produce maximally entangled states, and secret-key distillation [9,10], which generates states from which a secure classical key can be extracted. Both tasks can be studied in the asymptotic regime, where arbitrarily many copies of the input state are available, and in the resource-limited one-shot

regime [11], where only a single use of the distillation channel is permitted. Distillation protocols are implemented through local operations and classical communication (LOCC) in the bipartite setting, or local operations and public communication (LOPC) in the tripartite setting, including a potentially adversarial party. Their performance can be characterized by information-theoretic quantities that measure a state’s usefulness for a given task (see Ref. [2] for a comprehensive summary). Examples include the coherent information, the mutual and private information [7], and their “smoothed” one-shot counterparts, such as the smooth conditional max-entropy [12] and the hypothesis-testing mutual information [13]. These quantities provide lower bounds on the distillable entanglement or secret key and therefore serve as natural optimization targets [14–16]. Many of these quantities can be described in terms of generalized divergences and have properties [17] that make their computation tractable via semidefinite programming [18–21].

Among the many entanglement distillation protocols [8,22–27], the application of stabilizer codes [28,29] to distillation [30] has recently proven particularly powerful [31,32]. Leveraging a shared group structure of stabilizers and Bell states, an entanglement distillation protocol for bipartite qudits called FIMAX demonstrates high performance regarding both distillation efficiency and distillation effectiveness for highly mixed states. The corresponding work [31] shows that stabilizer operations can be tailored to maximize the increase of fidelity with the maximally entangled state iteratively. Moreover, the action of stabilizer operations on Bell-diagonal states admits a compact description of corresponding output states in terms of the input state, the chosen stabilizer, and the applied encoding.

*Contact author: christopher.popp@univie.ac.at

†Contact author: tobias.christoph.sutter@univie.ac.at

‡Contact author: beatrix.hiesmayr@univie.ac.at

This raises a natural question: can these stabilizer methods be generalized beyond fidelity optimization to enable resource distillation guided by arbitrary information measures, thereby producing states that are highly capable for a broad range of quantum processing tasks?

This work develops such a general framework for systems of prime local dimension. We begin in Sec. II by specifying the setting and notation. Section III develops the main results of this work that enable the stabilizer formalism for general distillation tasks. In particular, in Sec. III A, we formalize the stabilizer routine used for entanglement distillation as a quantum channel and extend it to the tripartite setting of cryptographic scenarios, allowing its application to general input states and various distillation tasks. We provide a complete Kraus representation in terms of stabilizer measurements and encodings. Section III B demonstrates how these results can be leveraged for general stabilizer-based resource state distillation by optimizing the stabilizer channels for distillation tasks that are characterized by certain information measures. Following the identification of operational simplifications based on invariances of the corresponding information measures in Sec. III C, we present several protocols to prove the principle of stabilizer-based resource state distillation in Sec. III D. These protocols include a generalization of FIMAX optimizing the fidelity for non-Bell-diagonal states, as well as applications to the (one-shot) entanglement and secret-key distillation by optimizing other information measures. We conclude our results in Sec. IV. Finally, Sec. V provides a concise summary of preliminary results and established methods used in this work.

II. SETTING AND NOTATION

In this section, we briefly introduce the notation relevant for formulating the tasks of stabilizer-based secret-key and entanglement distillation as a quantum channel. For a compact introduction to these methods, the reader is referred to Sec. V, providing more details on stabilizer-based operations in Sec. V A, the distillation tasks in Sec. V B, and associated information measures in Sec. V C.

We consider a setting of two parties Alice (A) and Bob (B) and the potential adversary third party, Eve (E). Let $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B \cong \mathbb{C}^d \otimes \mathbb{C}^d$ be the Hilbert space of bipartite quantum states with dimension of the subsystems d . We restrict d to be a prime number. In this case, $\mathbb{Z}_d := \mathbb{Z}/d\mathbb{Z}$, the quotient ring of integers with addition and multiplication modulo d , is a field. We denote complex conjugation by $(\star)$ and define it in the computational basis for operators. Let $\mathcal{H}_{AB}^{\otimes N} := \bigotimes_{n=1}^N \mathcal{H}_{AB} \cong \mathcal{H}_A^{\otimes N} \otimes \mathcal{H}_B^{\otimes N}$ be the Hilbert space of N -copy quantum states as shown in Fig. 1. $\mathcal{D}(\mathcal{H}_{AB})$ denotes the set of density operators on $\mathcal{H}_{AB}$. Pure states and their density matrix are written using the same symbol, e.g., $|\psi\rangle \in \mathcal{H} \leftrightarrow \psi = |\psi\rangle\langle\psi| \in \mathcal{D}(\mathcal{H})$. Alice and Bob hold N copies of the state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = d$, and aim to establish a target state depending on the distillation task. In the bipartite setting of entanglement distillation, the target is to produce maximally entangled states via LOCC (1), while in the tripartite setting of secret-key distillation, they try to create secret-key states via LOPC (2). We assume Alice and Bob to hold the state ρ_{AB} , while in case the task is secret-key

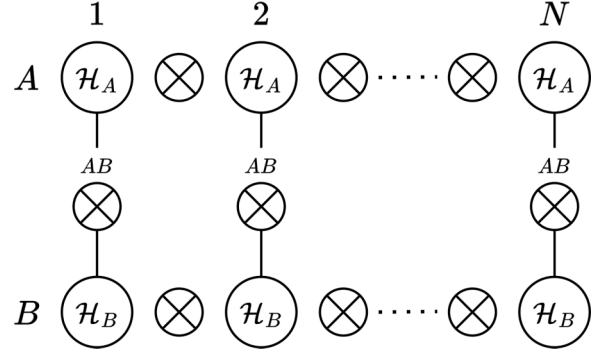


FIG. 1. Hilbert space $\mathcal{H}_{AB}^{\otimes N}$ of N copies of a bipartite system $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

distillation, the third party, Eve, is assumed to possess the purifying system $\mathcal{H}_E$ for the purification ϕ_{ABE} of the state ρ_{AB} , giving her a strong position as any extension of ρ_{AB} is related to ϕ_{ABE} by a local transformation on her system [2].

Any LOCC channel, i.e., completely positive trace-preserving map, used in the bipartite setting of entanglement distillation can be written as

$$\mathcal{L}_{AB} = \sum_z \mathcal{L}_A^z \otimes \mathcal{L}_B^z \quad (1)$$

and acts on the state ρ_{AB} . $\mathcal{L}_A^z$ and $\mathcal{L}_B^z$ are completely positive maps, such that the composite map is trace preserving. The corresponding tripartite LOPC channel, used in the setting of secret-key distillation, acts on the purification ϕ_{ABE} and reads

$$\mathcal{L}_{ABE} = \sum_z \mathcal{L}_A^z \otimes \mathcal{L}_B^z \otimes \mathbb{1}_E \otimes |z\rangle\langle z|_E, \quad (2)$$

considering that any classical communication between Alice and Bob is also known to Eve. Quantum states and channels are labeled by the parties that own the systems in the state. If it is not explicitly relevant, we omit specific labels for systems. For example, a state of the systems A_1 and A_2 , both in possession of Alice and formally written $\psi_{A_1 A_2}$, is written as ψ_A . Marginal states are labeled by a subset of systems, for example $\psi_{AE} := \text{Tr}_B[\psi_{ABE}]$. Since all considered quantum operations are local, we also label the channels with A, B, E , according to the parties that perform operations and omit system labels, if possible. For example, a channel mapping the systems B_1 and B_2 to E_1 , where B_1 and B_2 belong to Bob and E_1 to Eve, is denoted as $\mathcal{L}_{BE}$ if the specific systems and the channel direction are not relevant. Otherwise, we write explicitly $\mathcal{L}_{B_1 B_2 \rightarrow E_1}$. Moreover, if a channel, say $\mathcal{L}_{AB}$, corresponds only to a subset of the parties holding a state, say ψ_{ABE} , we identify $\mathcal{L}_{AB}(\psi_{ABE}) := \mathcal{L}_{AB} \otimes \text{id}_E(\psi_{ABE})$. Isometries are denoted by capital letters V , labeled as V_A if only the owner of the systems they act on is relevant, or as $V_{A_1 \rightarrow A_2}$ if the explicit systems the operator acts on are specified. Unitary operators are named by capital U .

III. RESULTS

A. The stabilizer routine as a quantum channel

In this section, we define the quantum channel corresponding to the stabilizer distillation routine, making it directly

available to any bipartite input state and allowing us to extend the distillation setting to a tripartite setting relevant for the distillation of secret-key states.

1. The stabilizer distillation routine

In Ref. [30], a protocol using stabilizer codes for entanglement distillation has been introduced, which has been generalized and analyzed in detail in Ref. [31]. If successful, the recurrently applied bipartite $[N, K]$ distillation protocol transforms N copies of a bipartite input state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB}^{\otimes N})$ into K copies of a highly entangled bipartite output state $\sigma_{AB}^{x,y} \in \mathcal{D}(\mathcal{H}_{AB}^{\otimes K})$ via LOCC. For a summary of the formalism for stabilizers and related results, see Sec. V A.

Given a stabilizer S with encodings $U(|x\rangle \otimes |k\rangle) = |u_{x,k}\rangle$ and $U^*(|y\rangle \otimes |l\rangle) = |u_{y,l}^*\rangle$, $x, y \in \mathcal{Z}_d^p$, $k, l \in \mathcal{Z}_d^{N-p}$, and corresponding projective stabilizer measurements $\mathcal{P}(x, y) : \mathcal{H}_{AB}^{\otimes N} \rightarrow \mathcal{Q}(x) \otimes \mathcal{Q}^*(y)$. One iteration of the protocol includes the following steps.

(1) Alice and Bob perform local stabilizer measurements with outcomes x, y .

(2) Bob sends Alice his measurement outcome y . Alice may declare failure of the protocol depending on x and y .

(3) Alice and Bob apply the inverse of stabilizer encodings U (Alice) and U^* (Bob) on $\mathcal{H}_A^{\otimes N}$ and $\mathcal{H}_B^{\otimes N}$.

The state after steps 1–3 can be written as

$$\begin{aligned} & \frac{(U \otimes U^*)^\dagger \mathcal{P}(x, y) \rho_{AB} \mathcal{P}(x, y) (U \otimes U^*)}{\mathbb{P}(x, y)} \\ &= |x\rangle\langle x| \otimes |y\rangle\langle y| \otimes \sigma_{AB}^{x,y}, \end{aligned} \quad (3)$$

where the first p qudits contain the measurement outcomes and $\sigma_{AB}^{x,y}$ is the output state to be used in the following iterations. Here, $\mathbb{P}(x, y) = \text{Tr}[\mathcal{P}(x, y) \rho_{AB}]$ corresponds to the probability of obtaining the measurement outcomes x, y .

2. The bipartite stabilizer channel

Since, by definition, the codewords $|u_{x,k}\rangle \otimes |u_{y,l}^*\rangle$ form a basis of the joint codespaces $\mathcal{Q}(x) \otimes \mathcal{Q}^*(y)$, we can write

$$\mathcal{P}_A(x) = \sum_{k \in \mathcal{Z}_d} |u_{x,k}\rangle\langle u_{x,k}|, \quad (4)$$

$$\mathcal{P}_B^*(y) = \sum_{l \in \mathcal{Z}_d} |u_{y,l}^*\rangle\langle u_{y,l}^*|, \quad (5)$$

$$\mathcal{P}(x, y) = \sum_{k, l \in \mathcal{Z}_d} |u_{x,k}\rangle\langle u_{x,k}| \otimes |u_{y,l}^*\rangle\langle u_{y,l}^*|. \quad (6)$$

Now consider the postmeasurement state for the input state $\rho_{AB} \in \mathcal{H}_{AB}^{\otimes N}$ and measurement outcomes $x, y \in \mathcal{Z}_d^p$, stored in the additional classical registers X (belonging to Alice) and Y (belonging to Bob), followed by the application of the inverse encoding according to steps 1–3 of the stabilizer distillation routine presented in Sec. III A 1:

$$\begin{aligned} \mathcal{L}_{AB}^{x,y}(\rho_{AB}) &:= |x, y\rangle\langle x, y|_X \otimes |y\rangle\langle y|_Y \\ &\otimes \frac{(U \otimes U^*)^\dagger \mathcal{P}(x, y) \rho_{AB} \mathcal{P}(x, y) (U \otimes U^*)}{\mathbb{P}(x, y)}. \end{aligned} \quad (7)$$

Considering all measurement outcomes, we define the bipartite stabilizer routine channel as

$$\begin{aligned} \mathcal{L}_{AB}(\rho_{AB}) &:= \sum_{x,y} |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes (U \otimes U^*)^\dagger \\ &\times \mathcal{P}(x, y) \rho_{AB} \mathcal{P}(x, y) (U \otimes U^*). \end{aligned} \quad (8)$$

Introducing the operators

$$M_A^x := \sum_k (|x\rangle \otimes |k\rangle)\langle u_{x,k}| = U^\dagger \mathcal{P}_A(x), \quad (M_A^x : \mathcal{H}_A^{\otimes N} \rightarrow \mathcal{H}_A^{\otimes N}), \quad (9)$$

$$M_B^{*y} := \sum_l (|y\rangle \otimes |l\rangle)\langle u_{y,l}^*| = (U^*)^\dagger \mathcal{P}_B^*(y), \quad (M_B^{*y} : \mathcal{H}_B^{\otimes N} \rightarrow \mathcal{H}_B^{\otimes N}), \quad (10)$$

$$K_{AB}^{x,y} := |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes M_A^x \otimes M_B^{*y}, \quad (K_{AB}^{x,y} : \mathcal{H}_{AB}^{\otimes N} \rightarrow \mathcal{H}_{XY} \otimes \mathcal{H}_{AB}^{\otimes N}), \quad (11)$$

we have

$$\mathcal{L}_{AB}(\rho_{AB}) = \sum_{x,y} |x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes (M_A^x \otimes M_B^{*y}) \rho_{AB} (M_A^{x\dagger} \otimes M_B^{*y\dagger}) = \sum_{x,y} K_{AB}^{x,y} \rho_{AB} K_{AB}^{x,y\dagger}. \quad (12)$$

Note that $\sum_{x,y} K_{AB}^{x,y\dagger} K_{AB}^{x,y} = \mathbb{1}_{AB}$. Hence, the $K_{AB}^{x,y}$ are Kraus operators for the quantum channel $\mathcal{L}_{AB}$. We call this channel the “bipartite stabilizer channel.”

For fixed measurement outcomes x, y , the output state $\sigma_{AB}^{x,y} := \mathcal{L}_{AB}^{x,y}(\rho_{AB})$ can be written in terms of $K_{AB}^{x,y}$ as follows:

$$\sigma_{AB}^{x,y} = \frac{K_{AB}^{x,y} \rho_{AB} K_{AB}^{x,y\dagger}}{\text{Tr}[K_{AB}^{x,y} \rho_{AB} K_{AB}^{x,y\dagger}]} = \frac{1}{\mathbb{P}(x, y)} K_{AB}^{x,y} \rho_{AB} K_{AB}^{x,y\dagger}. \quad (13)$$

3. The tripartite stabilizer channel

In the setting of quantum cryptography, e.g., for the distillation or distribution of secret keys, we consider a tripartite setting by including the adversary party “Eve” holding the system E . We assume that Eve holds a purification ϕ_{ABE} of

the state ρ_{AB} and that she can perform any local operation on her system. Additionally, public classical communication is assumed. So any classical information sent between Alice and Bob is also known to Eve, and an LOCC channel becomes an LOPC channel. In the following, we assume that all

measurement outcomes are communicated in public. Consider the purification based on the spectral decomposition of ρ_{AB} in terms of its eigenstates $\{|\Phi_m\rangle\}_{m \in \{0, \dots, r-1\}}$ with $r = \text{rank}(\rho_{AB})$ and nonzero eigenvalues λ_m :

$$\rho_{AB} = \sum_m \lambda_m |\Phi_m\rangle \langle \Phi_m|_{AB}, \quad (14)$$

$$\phi_{ABE} = |\phi\rangle \langle \phi|_{ABE} = \sum_{m,n} \sqrt{\lambda_m \lambda_n} |\Phi_m\rangle \langle \Phi_n|_{AB} \otimes |m\rangle \langle n|_E. \quad (15)$$

Here $\{|m\rangle\}_m$ is a basis of the purifying system with dimension r . The tripartite channel corresponding to the bipartite stabilizer distillation channel is defined as

$$\mathcal{L}_{ABE}(\phi_{ABE}) := \mathcal{L}_{AB} \otimes \text{id}_E(\phi_{ABE}) \quad (16)$$

$$= \sum_{x,y} K_{AB}^{x,y} \otimes \mathbb{1}_E \phi_{ABE} K_{AB}^{x,y\dagger} \otimes \mathbb{1}_E, \quad (17)$$

from which we read off the Kraus operators $\hat{K}_{x,y} = K_{AB}^{x,y} \otimes \mathbb{1}_E$. We call this channel the “tripartite stabilizer channel.”

Let $\{|\Omega(e)\rangle\}_{e \in \mathcal{Z}_d^N}$ be the N -copy Bell basis (see Definition 2) of $\mathcal{H}_{AB}^{\otimes N}$. Writing

$|\Phi_m\rangle \langle \Phi_n|_{AB} = \sum_{e,f} \beta_{e,f}^{m,n} |\Omega(e)\rangle \langle \Omega(f)|_{AB}$ in this basis, ϕ_{ABE} takes the form

$$\phi_{ABE} = \sum_{m,n=0}^{r-1} \sum_{e,f \in \mathcal{Z}_d^N} \sqrt{\lambda_m \lambda_n} \beta_{e,f}^{m,n} |\Omega(e)\rangle \langle \Omega(f)|_{AB} \otimes |m\rangle \langle n|_E \quad (18)$$

$$=: \sum_{\substack{m,n, \\ e,f}} \alpha_{e,f}^{m,n} |\Omega(e)\rangle \langle \Omega(f)|_{AB} \otimes |m\rangle \langle n|_E. \quad (19)$$

For a Bell-diagonal input state $\rho_{AB} = \sum_m p_m |\Omega(m)\rangle \langle \Omega(m)|$ this simplifies to

$$\phi_{ABE} = \sum_{m,n=0}^{r-1} \sqrt{p_m p_n} |\Omega(m)\rangle \langle \Omega(n)|_{AB} \otimes |m\rangle \langle n|_E. \quad (20)$$

In Ref. [31] it is demonstrated that the action of stabilizer operations on Bell states $|\Omega(e)\rangle$ can be specified by so-called action operators $T_x^{U,e}$, of dimension $d^{\otimes N-p}$ and characterized by (see Lemma 1)

$$U^\dagger W(e) U = \sum_{x \in \mathcal{Z}_d^p} |x+s\rangle \langle x| \otimes T_{x+s}^{U,e}. \quad (21)$$

Here, $s = s(e) \in \mathcal{Z}_d$ is the “syndrome” of e and depends on the stabilizer and the error e . The unitary operators T depend on the encoding U , the error e , and the measurement outcome x . Assuming the encoding U to be fixed, we omit the label and write simply T_x^e .

The forms of the operators $M_A^x = \sum_k (|x\rangle \otimes |k\rangle) \langle u_{x,k}|$ and $M_B^{*y} = \sum_l (|y\rangle \otimes |l\rangle) \langle u_{y,l}^*|$ (9) and (10) together with (21) now imply

$$M_A^x \otimes M_B^{*y} |\Omega(e)\rangle = (M_A^x \otimes M_B^{*y})(W(e) \otimes \mathbb{1})(U \otimes U^*) |\Omega_{0,0}\rangle^{\otimes N} \quad (22)$$

$$= (|x\rangle \langle x-s| \otimes T_x^e) \otimes (|y\rangle \langle y| \otimes \mathbb{1}) |\Omega_{0,0}\rangle^{\otimes N} \quad (23)$$

$$= \frac{1}{d^{p/2}} \delta_{x-y,s} (|x\rangle \otimes |y\rangle) \otimes (T_x^e \otimes \mathbb{1}) |\Omega_{0,0}\rangle^{\otimes N-p}. \quad (24)$$

One then finds for the output of the tripartite stabilizer distillation channel for the input of (18)

$$\begin{aligned} \mathcal{L}_{ABE}(\phi_{ABE}) &= \sum_{\substack{x,y, \\ m,n, \\ e,f \in \mathcal{E}(x-y)}} \alpha_{e,f}^{m,n} \frac{1}{d^p} |x, y\rangle \langle x, y|_{XYZ} \\ &\otimes [(T_x^e \otimes \mathbb{1}) \Omega_{0,0}^{\otimes N-p} (T_x^{f\dagger} \otimes \mathbb{1})]_{AB} \otimes |m\rangle \langle n|_E. \end{aligned} \quad (25)$$

For fixed measurement outcomes x, y , stored in the classical registers X, Y, Z of Alice, Bob, and Eve, the tripartite post-measurement output state of only the nonclassical systems A, B, E is

$$\tau_{ABE}^{x,y} = \langle x, y|_{XYZ} \otimes \mathbb{1}_{ABE} \left(\frac{\hat{K}_{x,y} \phi_{ABE} \hat{K}_{x,y}^\dagger}{\text{Tr}[\hat{K}_{x,y} \phi_{ABE} \hat{K}_{x,y}^\dagger]} \right) |x, y\rangle_{XYZ} \otimes \mathbb{1}_{ABE} \quad (26)$$

$$= \frac{1}{\mathbb{P}(x, y)} \sum_{\substack{m,n, \\ e,f \in \mathcal{E}(x-y)}} \alpha_{e,f}^{m,n} \frac{1}{d^p} [(T_x^e \otimes \mathbb{1}) \Omega_{0,0}^{\otimes N-p} (T_x^{f\dagger} \otimes \mathbb{1})]_{AB} \otimes |m\rangle \langle n|_E, \quad (27)$$

where we used the fact that the only trace-decreasing operation in $\mathcal{L}_{ABE}$ for fixed x, y is the bipartite stabilizer measurement via $\mathcal{P}(x, y)$ and that ϕ_{ABE} is the purification of ρ_{AB} , implying $\mathbb{P}(x, y) = \text{Tr}[\hat{K}_{x,y} \phi_{ABE} \hat{K}_{x,y}^\dagger]$.

B. Principle and relevant objects for stabilizer-based resource distillation

In this section we show how to optimize the stabilizer channels so that their bipartite and tripartite output states are highly potent for operational tasks like entanglement and secret-key distillation.

The capability of general quantum states for the entanglement and secret-key distillation tasks can be characterized or lower-bounded via generalized information quantities. We summarize methods of how to do so in Secs. VB and VC. The principle of stabilizer-based resource state distillation is as follows: depending on the distillation task, we choose an information quantity that measures the corresponding capability of a quantum state. Leveraging the precise output form of the stabilizer channels, we optimize the channel regarding the stabilizer, encoding, and measurement outcome such that the information measure for the channel output becomes maximized. This procedure can be iterated, effectively distill-

ing target resource states that are optimal for the operational task as measured by the chosen information quantity. In the following, we determine relevant states and information measures for entanglement and secret-key distillation and leverage their properties to simplify the optimization of the distillation channel.

1. Relevant states and measures for entanglement distillation

Tracing out the system E from the tripartite output state (26), the general bipartite output state (13) takes the specific form

$$\begin{aligned}\sigma_{AB}^{x,y} &= \frac{1}{\mathbb{P}(x,y)} K_{AB}^{x,y} \rho_{AB} K_{AB}^{x,y\dagger} \\ &= \frac{1}{\mathbb{P}(x,y)} \sum_{\substack{m \\ e,f \in \mathcal{E}(x-y)}} \alpha_{e,f}^{m,m} \frac{1}{d^p} [(T_x^e \otimes \mathbb{1}) \Omega_{0,0}^{\otimes N-p} (T_x^{f\dagger} \otimes \mathbb{1})]_{AB}.\end{aligned}\quad (28)$$

In the one-shot setting, we leverage Theorem 3 to determine the smooth max-relative entropy $H_{\max}^{\varepsilon}(\sigma_{AB}^{x,y})$ as an information

$$\chi_{ABE}^{x,y} := \mathcal{D}_A(\tau_{ABE}^{x,y}) = \frac{1}{\mathbb{P}(x,y)} \sum_{\substack{m,n \\ e,f \in \mathcal{E}(x-y), \\ i,k,l \in \mathbb{Z}_d^{N-p}}} \alpha_{e,f}^{m,n} \langle i | T_x^e | k \rangle \langle l | T_x^{f\dagger} | i \rangle \langle i | i \rangle_A \otimes | k \rangle \langle l |_B \otimes | m \rangle \langle n |_E. \quad (30)$$

To evaluate this state regarding its usefulness for secret-key generation, we consider the reduced bipartite states:

$$\chi_{AB}^{x,y} := \text{Tr}_E[\chi_{ABE}] = \frac{1}{\mathbb{P}(x,y)} \sum_{\substack{m \\ e,f \in \mathcal{E}(x-y), \\ i,k,l \in \mathbb{Z}_d}} \alpha_{e,f}^{m,m} \langle i | T_x^e | k \rangle \langle l | T_x^{f\dagger} | i \rangle \langle i | i \rangle_A \otimes | k \rangle \langle l |_B, \quad (31)$$

$$\chi_{AE}^{x,y} := \text{Tr}_B[\chi_{ABE}] = \frac{1}{\mathbb{P}(x,y)} \sum_{\substack{m,n \\ e,f \in \mathcal{E}(x-y), \\ i \in \mathbb{Z}_d}} \alpha_{e,f}^{m,n} \langle i | T_x^e T_x^{f\dagger} | i \rangle \langle i | i \rangle_A \otimes | m \rangle \langle n |_E. \quad (32)$$

In the one-shot setting, Theorem 5 implies that the difference of the hypothesis testing mutual information $I_H^{\varepsilon}(\chi_{AB}^{x,y})$ and the smooth max-mutual information $I_{\max}^{\varepsilon}(\chi_{AE}^{x,y})$ provides achievable rates for the one-shot secret-key distillation, given certain smoothing parameters ε and ϵ . Optimization of this difference by varying ε , ϵ , and the channel output $\tau_{ABE}^{x,y}$ (determining χ_{AB} and χ_{AE}) hence optimizes the resource for one-shot secret key distillation.

Likewise, in the asymptotic setting, the so-called private information $I(\chi_{ABE}) := I(\chi_{AB}) - I(\chi_{AE})$ provides an achievable rate according to Theorem 6 and serves as a quantity to be optimized via stabilizer channels.

C. Simplifications for local isometric and unitary invariance

In Ref. [17], it is shown that all considered divergence-based measures, as discussed above and defined in Sec. V, are invariant under local isometric or unitary transformations. We leverage this property in two ways. First, we show that a different choice of encoding for the stabilizer channel corresponds to a local unitary transformation of the output state.

measure to be optimized for distilling resource states with a high capability for entanglement distillation.

In the asymptotic setting, Theorem 4 implies that the coherent information $I_c^{A|B}(\sigma_{AB}^{x,y})$ is an achievable rate for entanglement distillation and therefore provides a suitable information measure for optimization.

2. Relevant states and measures for secret-key distillation

For the task of secret-key distillation, consider the output (26) of the tripartite stabilizer distillation channel, given the outcome x, y :

$$\begin{aligned}\tau_{ABE}^{x,y} &:= \frac{1}{\mathbb{P}(x,y)} \sum_{\substack{m,n \\ e,f \in \mathcal{E}(x-y)}} \alpha_{e,f}^{m,n} [(T_x^e \otimes \mathbb{1}_B) \\ &\quad \times \Omega_{0,0}^{\otimes N-p} (T_x^{f\dagger} \otimes \mathbb{1}_B)]_{AB} \otimes | m \rangle \langle n |_E.\end{aligned}\quad (29)$$

To draw a key from this state, Alice and Bob apply local measurements to their system, whose action is given by the local measurement or dephasing channels $\mathcal{D}_{A/B}(\cdot)$ in (48). Assume that Alice applies $\mathcal{D}_A$ to the output state:

Hence, given a certain information measure, the choice of encoding is irrelevant for finding the optimal stabilizer channel if the information measure is invariant. Second, we show that the tripartite purification of the bipartite stabilizer channel output is related to the output of the tripartite channel by a local isometric transformation. Given a local isometric invariant information measure in the tripartite distillation setting, the purification of the bipartite channel output can be considered instead of the tripartite channel output. This effectively reduces the dimension of the states to evaluate and therefore brings significant performance improvements for calculating the information measure for distillation.

1. Local unitary equivalence of encodings

We now show that a change of stabilizer encoding implies a unitary transformation of the bipartite output state, acting locally on the systems A and B . Following Proposition 6 of Ref. [31], given a stabilizer encoding U , for any other stabilizer encoding V , there exist unitary matrices Z_k , such that

$V = U (\sum_k |k\rangle\langle k| \otimes Z_k)$ and $T_x^{V,e} = Z_x^\dagger T_x^{U,e} Z_y$. This implies for the output state (28) using the encoding V

$$\begin{aligned}\sigma_{AB}^{x,y,V} &= \frac{1}{\mathbb{P}(x,y)} \sum_{e,f \in \mathcal{E}(x-y)} \alpha_{e,f}^{m,m} \frac{1}{d^p} (Z_x^\dagger T_x^{U,e} Z_y \otimes \mathbb{1}) \Omega_{0,0}^{\otimes N-p} (Z_x^\dagger T_x^{U,f} Z_y \otimes \mathbb{1})^\dagger \\ &= \frac{1}{\mathbb{P}(x,y)} \sum_{e,f \in \mathcal{E}(x-y)} \alpha_{e,f}^{m,m} \frac{1}{d^p} (Z_x^\dagger T_x^{U,e} \otimes Z_y^T) \Omega_{0,0}^{\otimes N-p} (Z_x^\dagger T_x^{U,f} \otimes Z_y^T)^\dagger \\ &= \frac{1}{\mathbb{P}(x,y)} \sum_{e,f \in \mathcal{E}(x-y)} \alpha_{e,f}^{m,m} \frac{1}{d^p} (Z_x^\dagger \otimes Z_y^T) (T_x^{U,e} \otimes \mathbb{1}) \Omega_{0,0}^{\otimes N-p} (T_x^{U,f} \otimes \mathbb{1})^\dagger (Z_x \otimes Z_y^*) \\ &= (Z_x^\dagger \otimes Z_y^T) \sigma_{AB}^{x,y,U} (Z_x \otimes Z_y^*). \tag{33}\end{aligned}$$

Note that the coefficients α only depend on the input state and that the probabilities $\mathcal{P}(x,y)$ only depend on the codespaces $\mathcal{Q}(x) \otimes \mathcal{Q}(y)$ and not on the choice of encoding, i.e., their basis. Also, for the second equation, we used the “transpose (T) trick,” holding for any matrix $M \in \mathbb{C}^{d_A \times d_B}$: $M \otimes \mathbb{1} |\Omega_{0,0}\rangle = \mathbb{1} \otimes M^T |\Omega_{0,0}\rangle$.

Equivalently, one finds for the tripartite channel output

$$\tau_{ABE}^{x,y,V} = (Z_x^\dagger \otimes Z_y^T)_{AB} \tau_{ABE}^{x,y,U} (Z_x \otimes Z_y^*)_{AB}. \tag{34}$$

Consequently, any information measure that is invariant under local unitary transformations is invariant under change of encodings for the stabilizer channel when measuring the channel output.

2. Local isometric equivalence of purifications

We now show that the tripartite purification $\psi_{ABE'}^{x,y}$ of the bipartite output state $\sigma_{AB}^{x,y}$ of the bipartite channel $\mathcal{L}_{AB}$ for a certain measurement outcome x,y is related to the post-measurement output state $\tau_{ABE}^{x,y}$ of the tripartite channel $\mathcal{L}_{ABE}$ applied to the purification ϕ_{ABE} of the input state ρ_{AB} .

By (8) and (16), the channel $\mathcal{L}_{ABE}$ consists of a projective measurement followed by a unitary transformation. Given the purification of the input state ϕ_{ABE} , applying $\mathcal{L}_{ABE}$ and projecting to the measurement outcomes x,y , the resulting state $\tau_{ABE}^{x,y}$ is also a pure state. We have for the purification $\psi_{ABE'}^{x,y}$ of the bipartite output state $\sigma_{AB}^{x,y}$ and the tripartite output state $\tau_{ABE}^{x,y}$

$$\text{Tr}_{E'}[\psi_{ABE'}^{x,y}] = \sigma_{AB}^{x,y} = \text{Tr}_E[\tau_{ABE}^{x,y}]. \tag{35}$$

Hence, both $\psi_{ABE'}^{x,y}$ and $\tau_{ABE}^{x,y}$ are purifications of $\sigma_{AB}^{x,y}$ and as such related by an isometry $V_{E' \rightarrow E}$ [2], mapping one purification system to the other:

$$\tau_{ABE}^{x,y} = V_{E' \rightarrow E} \psi_{ABE'}^{x,y} V_{E' \rightarrow E}^\dagger. \tag{36}$$

As the isometry only acts on the purifying system, also the locally dephased states satisfy this relation:

$$\begin{aligned}\chi_{ABE}^{x,y} &= \mathcal{D}_A(\tau_{ABE}^{x,y}) \\ &= \mathcal{D}_A(V_{E' \rightarrow E} \psi_{ABE'}^{x,y} V_{E' \rightarrow E}^\dagger) \\ &= V_{E' \rightarrow E} \mathcal{D}_A(\psi_{ABE'}^{x,y}) V_{E' \rightarrow E}^\dagger \\ &=: V_{E' \rightarrow E} \zeta_{ABE'}^{x,y} V_{E' \rightarrow E}^\dagger, \tag{37}\end{aligned}$$

where we defined the partially dephased state $\zeta_{ABE'}^{x,y} = \mathcal{D}_A(\psi_{ABE'}^{x,y})$ based on the purification $\psi_{ABE'}^{x,y}$. Consequently, the reduced states χ_{AB} (31) and χ_{AE} (32) satisfy

$$\chi_{AB}^{x,y} = \zeta_{AB}^{x,y}, \tag{38}$$

$$\chi_{AE}^{x,y} = V_{E' \rightarrow E} \zeta_{AE'}^{x,y} V_{E' \rightarrow E}^\dagger. \tag{39}$$

Note that because E' is a purification system for the d^{N-p} -dimensional output state $\sigma_{AB}^{x,y}$, E' can be chosen to be $d^{2(N-p)}$ -dimensional if $\sigma_{AB}^{x,y}$ has full rank. The system E used for the purification of the d^N -dimensional input state ρ_{AB} , however, needs to be d^{2N} -dimensional if ρ_{AB} has full rank. Hence, considering states based on E' has computational advantages, for the calculation of quantities that are invariant under isometric transformations on the purifying system. Since the Hilbert-space dimension grows exponentially with the number of qudits, this reduction lowers the computational complexity of stabilizer-based protocols—such as the SPI-IMAX protocol introduced below—by orders of magnitude, transforming otherwise intractable optimizations into feasible numerical tasks.

D. Defining stabilizer-based resource distillation protocols

In this section, we define specific protocols that demonstrate the principle of stabilizer-based resource distillation. We consider the operational tasks of entanglement distillation (see Sec. VB 1) and secret-key distillation (see Sec. VB 2) and define protocols that optimize corresponding information measures via stabilizer operations.

1. Entanglement distillation

The first example extends the recently introduced FIMAX protocol [31]. Using a specific “canonical encoding U_c ,” FIMAX requires Bell-diagonal states to increase the fidelity with the maximally entangled state $\mathcal{F}(\rho) := \langle \Omega_{0,0} | \rho | \Omega_{0,0} \rangle$. For two copies of the input state and prime dimension, FIMAX is proven to maximize the fidelity increase per iteration for Bell-diagonal states among stabilizer-based distillation protocols. Leveraging the general output of the bipartite stabilizer channel $\sigma_{AB}^{x,y}$, we define the “generalized fidelity increase maximizing (gF-IMAX)” protocol that is applicable for all two-copy input states in prime dimension.

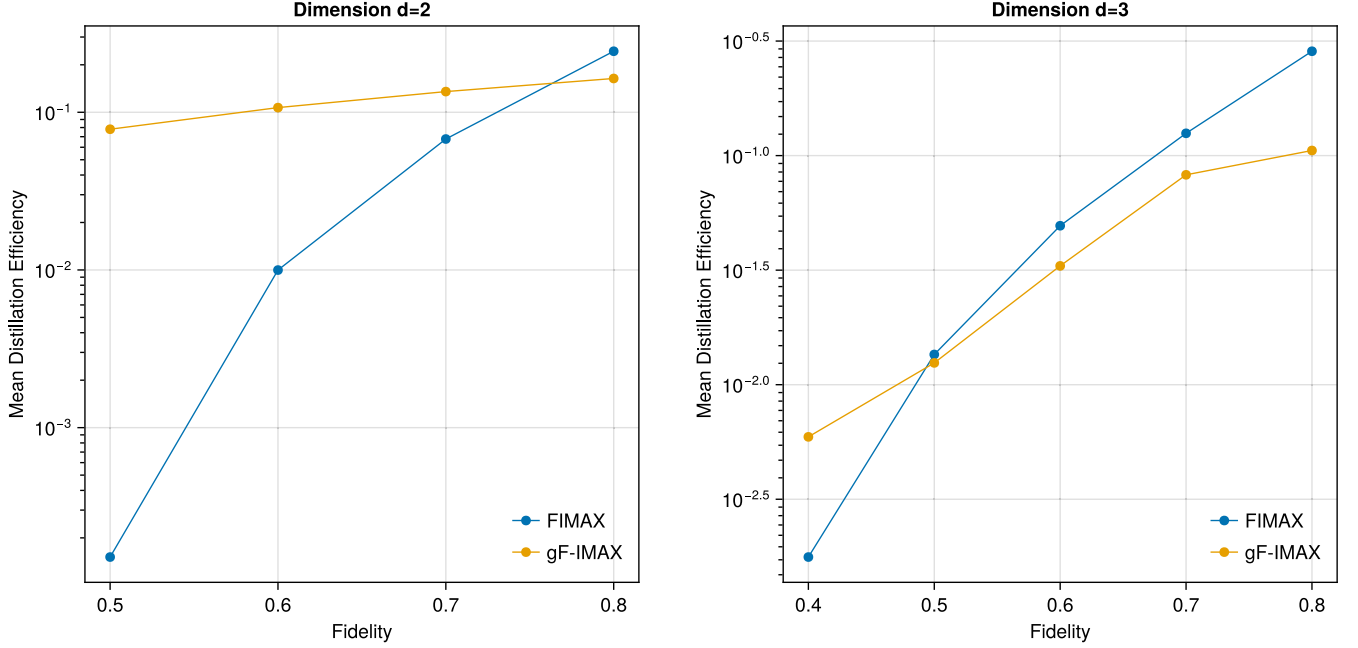


FIG. 2. Protocol comparison of mean distillation efficiencies to reach a target fidelity of 0.9 depending on the fidelity of pure states. Each data point represents the mean efficiency for a group of 1000 bipartite entangled input states with fidelities rounded to one digit for local dimensions $d = 2$ (left) and $d = 3$ (right). The efficiency is defined as the inverse of the required number of input states to produce one output state with fidelity larger than the target fidelity. To generate these results, we used the methods implemented in Ref. [33].

(a) *gF-IMAX protocol.* Let ρ_{AB} be any bipartite state shared between Alice and Bob with prime dimensions $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = d$ and let U_c be the canonical encoding (see Ref. [31]) for two copies of ρ_{AB} . The following steps are recurrently applied.

(1) For each stabilizer S , all measurement outcomes $x, y \in \mathcal{Z}_d$, and all $k, l \in \mathcal{Z}_d$, Alice computes $\mathcal{F}_{k,l}(\sigma_{AB}^{x,y}) = \langle \Omega_{k,l} | \sigma_{AB}^{x,y} | \Omega_{k,l} \rangle$ for the corresponding post-measurement stabilizer channel outputs $\sigma_{AB}^{x,y}$ as in (28).

(2) Alice determines the configuration $(S_{\max}, x_{\max}, y_{\max}, k_{\max}, l_{\max})$ that maximizes $\mathcal{F}_{k,l}(\sigma_{AB}^{x,y})$ and communicates it to Bob.

(3) Alice and Bob apply the stabilizer channel corresponding to $S_{\max}$ with the canonical encoding U_c and determine their outcomes x, y . If $x \neq x_{\max}$ or $y \neq y_{\max}$, they declare failure of the protocol.

(4) Alice applies the unitary Weyl-Heisenberg transformation $W_{k_{\max}, l_{\max}}^\dagger(\cdot) W_{k_{\max}, l_{\max}}$ (see Definition 1) locally to her output.

Although both increase the fidelity by using the stabilizer operations with the canonical encoding, there are relevant differences between gF-IMAX and FIMAX. First, unlike FIMAX for Bell-diagonal states, the canonical encoding does not imply a maximal increase of fidelity in each iteration among all stabilizers, encodings, and measurement outcomes. Depending on the input state, some other encoding may achieve better performance. Second, the condition for failure of FIMAX is given by the difference of measurement outcomes $s := x - y \neq s_{\max}$. This is because for Bell-diagonal states, the channel output only depends on the syndrome, i.e., the difference of measurement outcomes $s = x - y$, which

does not hold for general input states. gF-IMAX fails unless precisely $x = x_{\max}$ and $y = y_{\max}$, implying a higher probability of failure due to stricter postselection, and thus a negative impact on the protocol efficiency. On the other hand, to apply FIMAX to non-Bell-diagonal states, a twirl to Bell-diagonal form is required, generally inducing additional noise. As this is not the case for gF-IMAX, it may be more efficient for non-Bell-diagonal states. This is demonstrated in Fig. 2, where the efficiency of distilling states is shown in dependence on the input fidelity of random pure states. The performance of gF-IMAX exceeds FIMAX for certain low-fidelity regions, while FIMAX is superior for higher fidelities. For more general resource distillation protocols, we consider other quantities than the fidelity to optimize with stabilizer channels. Theorem 3 states that the negative smooth conditional max-entropy $(-H_{\max}^\epsilon)$ (Definition 18), also denoted as “smooth coherent information,” defines a lower bound on the one-shot distillable entanglement. We want to optimize this quantity via stabilizer operations. According to Ref. [17], $H_{\max}^\epsilon(\rho_{AB})$ is invariant under local unitary transformation of the bipartite state ρ_{AB} . Due to the results of Sec. III C 1, all channels for some stabilizer with different encodings U produce output states $\sigma_{AB}^{x,y,U}$ with equal smooth conditional max-entropy $H_{\max}^\epsilon(\sigma_{AB}^{x,y,U})$. To maximize the smooth coherent information $(-H_{\max}^\epsilon)$, it consequently suffices to consider different stabilizers with fixed arbitrary encodings. We define the “smooth coherent information increase maximizing (SCI-IMAX)” protocol as follows.

(b) *SCI-IMAX protocol.* Let ρ_{AB} be any bipartite state shared between Alice and Bob with prime local dimensions

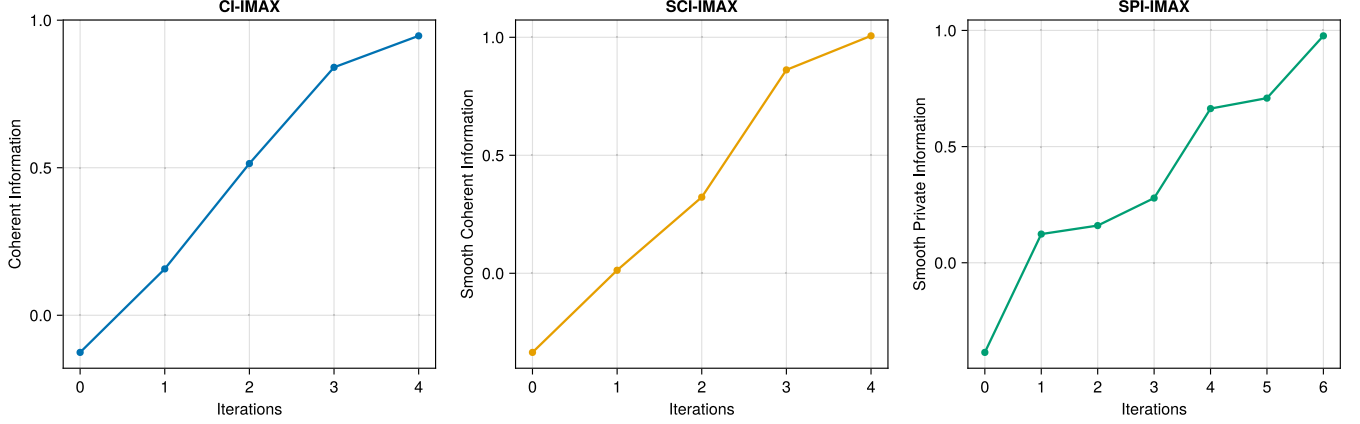


FIG. 3. Resource state distillation based on three optimization quantities for $d = 2$. Starting with the isotropic state $\rho(p) = p |\Omega_{0,0}\rangle\langle\Omega_{0,0}| + (1-p) \pi_{mm}$ for $p = 0.7$ and where π_{mm} is the maximally mixed state, different optimization quantities are iteratively increased. For the evaluation of the smooth coherent information ($-H_{\max}^{\epsilon}$) (used for SCI-IMAX) we use the semidefinite program (SDP) presented in Ref. [20]. For the smooth private information (used for SPI-IMAX), I_H^{ϵ} can also be evaluated by an SDP [2]. The smooth max-mutual information $I_{\max}^{\epsilon}$ is approximated by the SDP-based algorithm given in Ref. [21]. The smoothing parameters ϵ, ϵ are both set to 0.1. The protocols are iterated until the optimization quantity is larger than 90% of the maximally achievable value. For all protocols we use the implementation of Ref. [33].

$d_A = d_B$ and $\epsilon \in (0, 1)$. The following steps are recurrently applied.

(1) For each stabilizer S Alice and Bob fix an arbitrary encoding U_S .

(2) For all S and all measurement outcomes x, y , Alice computes $H_{\max}^{\epsilon}(\sigma_{AB}^{x,y})$ for the corresponding postmeasurement stabilizer channel outputs $\sigma_{AB}^{x,y}$ (28).

(3) Alice determines the configuration $(S_{\max}, x_{\max}, y_{\max})$ that maximizes $[-H_{\max}^{\epsilon}(\sigma_{AB}^{x,y})]$ and communicates it to Bob.

(4) Alice and Bob apply the stabilizer channel corresponding to $S_{\max}$ with the arbitrary encoding $U_{S_{\max}}$ and determine their outcomes x, y . If $x \neq x_{\max}$ or $y \neq y_{\max}$, they declare failure of the protocol.

According to Theorem 4, the coherent information $I_c^{(A)B}$ (Definition 16) provides a lower bound for the distillable entanglement in the asymptotic setting. This quantity is also invariant under local unitaries [17] and consequently under a change of encodings. We therefore define the “coherent information increase maximizing (CI-IMAX)” protocol.

(c) *CI-IMAX protocol.* Let ρ_{AB} be any bipartite state shared between Alice and Bob with prime local dimensions $d_A = d_B$. The following steps are recurrently applied.

(1) For each stabilizer S Alice and Bob fix an arbitrary encoding U_S .

(2) For all S and all measurement outcomes x, y , Alice calculates $I_c^{(A)B}(\sigma_{AB}^{x,y})$ for the corresponding postmeasurement channel outputs $\sigma_{AB}^{x,y}$ (28).

(3) Alice determines the configuration $(S_{\max}, x_{\max}, y_{\max})$ that maximizes $I_c^{(A)B}(\sigma_{AB}^{x,y})$ and communicates it to Bob.

(4) Alice and Bob apply the stabilizer channel corresponding to $S_{\max}$ with the arbitrary encoding $U_{S_{\max}}$ and determine their outcomes x, y . If $x \neq x_{\max}$ or $y \neq y_{\max}$, they declare failure of the protocol.

Figure 3 shows how the coherent information and the smooth coherent information are increased by applying

the corresponding protocols to an isotropic input state. For the numericals, the implementation of *BellDiagonalQudits.jl* [33] is used.

2. Secret-key distillation

Theorem 6 states that the hypothesis testing mutual information I_H^{ϵ} (Definition 17) and the smooth max-mutual information $I_{\max}^{\epsilon}$ (Definition 18) define a lower bound for the one-shot distillable secret key. More precisely, for parameters ϵ and ϵ , we consider $I_H^{\epsilon}(\chi_{AB}^{x,y}) - I_{\max}^{\epsilon}(\chi_{AE}^{x,y})$, where $\chi_{AB}^{x,y}$ (31) and $\chi_{AE}^{x,y}$ (32) are the dephased marginals of the tripartite stabilizer channel output. We also call this expression “smooth private information.” As shown in Ref. [17], I_H^{ϵ} is invariant under local isometric transformations, while $I_{\max}^{\epsilon}$ is invariant under unitary transformations in the first subsystem and isometric transformations in the second system. This implies, on the one hand, that the choice of stabilizer encoding is not relevant for maximizing these quantities. On the other hand, as shown in Sec. III C 2, when evaluating $I_{\max}^{\epsilon}$, we may consider the state $\zeta_{AE'}^{x,y}$ as in (39) instead of the higher dimensional $\chi_{AE}^{x,y}$ of (32). We define the “smooth private information increase maximizing (SPI-IMAX)” protocol as follows.

(a) *SPI-IMAX protocol.* Let ρ_{AB} be any bipartite state shared between Alice and Bob with prime local dimensions $d_A = d_B$ and $\epsilon, \epsilon \in (0, 1)$.

(1) For each stabilizer S , Alice and Bob fix an arbitrary encoding U_S .

(2) For all S and all measurement outcomes x, y , Alice calculates $I_H^{\epsilon}(\zeta_{AB}^{x,y}) - I_{\max}^{\epsilon}(\zeta_{AE}^{x,y})$ for the corresponding dephased tripartite postmeasurement channel outputs $\zeta_{AB}^{x,y}$ and $\zeta_{AE}^{x,y}$ as in (38) and (39).

(3) Alice determines the configuration $(S_{\max}, x_{\max}, y_{\max})$ that maximizes $I_H^{\epsilon}(\zeta_{AB}^{x,y}) - I_{\max}^{\epsilon}(\zeta_{AE}^{x,y})$ and communicates it to Bob.

(4) Alice and Bob apply the stabilizer channel corresponding to $S_{\max}$ with the arbitrary encoding $U_{S_{\max}}$ and determine their outcomes x, y . If $x \neq x_{\max}$ or $y \neq y_{\max}$, they declare failure of the protocol.

Figure 3 below includes this protocol for an isotropic input state.

(b) *PI-IMAX protocol.* The private information I_p (see comment below Theorem 6) provides a lower bound of the distillable secret key in the asymptotic setting. It is straightforward to define a similar protocol to the ones introduced above that maximizes the increase of private information among all stabilizer-based protocols. However, it turns out that such a protocol is equivalent to the bipartite CI-IMAX protocol that maximized the coherent information. To see this, we again use the results of Sec. III C. First, we have $I_p(\chi_{ABE}^{x,y}) = I_p(\zeta_{ABE'}^{x,y})$ with the states of (37)–(39). Considering that $\zeta_{ABE'}^{x,y} := \mathcal{D}_A(\psi_{ABE'}^{x,y})$ for the purification $\psi_{ABE'}^{x,y}$ of the bipartite output state $\sigma_{AB}^{x,y}$, the private information of the state satisfies $I_p(\zeta_{ABE'}^{x,y}) = I_c^{AB}(\sigma_{AB}^{x,y})$ (see Ref. [7]). Consequently, applying the bipartite protocol CI-IMAX of Sec. III D 1 also maximizes the increase of private information, and PI-IMAX is equivalent to CI-IMAX.

IV. CONCLUSION

In this work, we have formulated the stabilizer distillation routine—originally introduced in Ref. [30] and further developed in Ref. [31]—as a quantum channel. This perspective provides a unified framework for stabilizer-based methods, extending their application from bipartite entanglement distillation to tripartite secret-key distillation and general input states.

We derived explicit Kraus representations for both bipartite and tripartite stabilizer channels, parametrized by the choice of stabilizer and encoding. Leveraging the shared group structure of stabilizers and Bell states [31], we obtained closed-form expressions for the resulting output states. These expressions establish a general framework for stabilizer-based resource distillation: for any information-processing task characterized by a specific measure, one can evaluate that measure on the channel outputs and optimize the stabilizer channel to maximize the resource increase under iterative application. Key examples demonstrated here include the (smooth) coherent information for (one-shot) entanglement distillation and the (smooth) private information for (one-shot) secret-key distillation.

To ensure this optimization remains computationally tractable, we leveraged local invariances within the relevant information measures. Specifically, we demonstrated invariance under changes of stabilizer encodings and, in the tripartite setting, under the choice of the purification system. These invariances significantly reduce the numerical complexity of the optimization, effectively transforming otherwise intractable tasks into feasible numerical optimizations.

We provided several proofs of concept illustrating the versatility of stabilizer channels for resource-state distillation. First, we generalized the FIMAX protocol [31] to gF-IMAX, which optimizes fidelity for arbitrary input states. Initial numerical tests on random pure states indicate that gF-IMAX can outperform the standard FIMAX protocol in

specific regimes. Second, we introduced CI-IMAX and SCI-IMAX to optimize coherent information in the asymptotic and one-shot regimes, respectively. As coherent information lower-bounds the distillable entanglement, these protocols yield stabilizer channels that efficiently generate highly entangled states. Finally, we extended the framework to tripartite secret-key distillation. Noting that maximizing coherent information via CI-IMAX also maximizes the asymptotic private information, we developed the SPI-IMAX protocol to increase the smooth private information. Since this quantity provides lower bounds for one-shot secret-key rates, SPI-IMAX generates states highly optimized for one-shot cryptographic tasks. Numerical results for isotropic input states confirm that these protocols successfully identify effective operations to tailor resourceful states to specific quantum processing tasks.

Several directions for future research naturally follow. A systematic numerical comparison of the proposed protocols, particularly for highly mixed states, would clarify their relative efficiency and distillation effectiveness. This also includes analyzing the protocols' robustness with respect to initial states and imperfect operations. While the discussed entanglement distillation protocols exhibit high efficiency and effectiveness for very noisy states (see Fig. 2 and Ref. [32]), it is known (see Ref. [34]) that the dynamics of entangled two-qubit systems under recurrent operations can be very sensitive to initial conditions. Investigating how this sensitivity arises with the presented optimization of stabilizer-based methods is therefore valuable both from a practical and theoretical perspective. Furthermore, identifying bipartite N - P - T states that are undistillable via stabilizer-based protocols yet still possess private capacity could provide new insights into the distillability problem and the existence of N - P - T bound entanglement. Additionally, stabilizer-based methods may help uncover positive partial transpose states with nonzero distillable secret key, which would be instrumental in understanding bound entanglement [35] and the broader separability problem.

In summary, these contributions establish stabilizer channels as a versatile and optimizable tool for quantum resource distillation. By connecting stabilizer operations to the optimization of general quantum resources, this framework provides practical, high-performance protocols for both entanglement and secret-key distillation in one-shot and asymptotic regimes.

V. METHODS

In this section, we summarize the methods applied to generate the results presented in Sec. III.

A. Stabilizer distillation routine

First, we present the background of the stabilizer framework developed in Ref. [31].

Let $\mathbb{Z}_d \equiv \mathbb{Z}/d\mathbb{Z}$ be the quotient ring of integers with addition and multiplication modulo d , which is a field for prime d , and let $\omega \equiv \exp(\frac{2\pi i}{d})$. Complex conjugation ($\star$) is defined in the computational basis.

Definition 1 (Weyl(-Heisenberg) operators, Weyl(-Heisenberg) errors).

$$W_{k,l} := \sum_{j=0}^{d-1} \omega^{jk} |j\rangle \langle j+l|, k, l \in \mathbb{Z}_d, \quad (40)$$

$$\begin{aligned} \mathcal{E}_N &:= \{W(e) | e = (\vec{k}, \vec{l}) \in \mathbb{Z}_d^N \times \mathbb{Z}_d^N\} \\ &:= \left\{ \bigotimes_{n=1}^N W_{k_n, l_n} | k_n, l_n \in \mathbb{Z}_d \right\}. \end{aligned} \quad (41)$$

The Weyl-Heisenberg operators satisfy the Weyl relations, i.e.,

$$\begin{aligned} W_{k_1, l_1} W_{k_2, l_2} &= \omega^{l_1 k_2} W_{k_1+k_2, l_1+l_2}, \\ W_{k, l}^\dagger &= \omega^{kl} W_{-k, -l} = W_{k, l}^{-1}, \end{aligned} \quad (42)$$

implying that the set of Weyl errors $\mathcal{E}_N$ forms a group under multiplication, if we identify errors that are equal up to a phase, i.e., $W_{k_1, l_1} W_{k_2, l_2} \equiv W_{k_1+k_2, l_1+l_2}$. $E \in \mathcal{E}_N$ are called error operators. For $E = W(e)$, $e \equiv (\vec{k}, \vec{l}) \in \mathbb{Z}_d^N \times \mathbb{Z}_d^N$ are called error elements. The group structure of $\mathcal{E}_N$ induces a group structure via the Weyl relations (42) for error elements on $\mathbb{Z}_d^N \times \mathbb{Z}_d^N$ with addition modulo d .

Definition 2 (Bell states).

$$\begin{aligned} |\Omega_{k,l}\rangle &:= (W_{k,l} \otimes \mathbb{1}_d) |\Omega_{0,0}\rangle \\ &:= (W_{k,l} \otimes \mathbb{1}_d) \frac{1}{\sqrt{d}} \sum_i |i\rangle \otimes |i\rangle, i, k, l \in \mathbb{Z}_d, \quad (43) \\ |\Omega(e)\rangle &:= (W(e) \otimes \mathbb{1}_d^{\otimes N}) |\Omega_{0,0}\rangle^{\otimes N} \\ &= \bigotimes_{n=1}^N |\Omega_{k_n, l_n}\rangle, e \equiv (\vec{k}, \vec{l}) \in \mathbb{Z}_d^N \times \mathbb{Z}_d^N. \end{aligned} \quad (44)$$

Definition 3 (Stabilizer group, generating operators, generating elements). A stabilizer S is an Abelian subgroup of $\mathcal{E}_N$. If $\{W(g_1), \dots, W(g_p)\}$ forms a minimal generating set of S , each $W(g_j)$ is called a generating operator and we write $S = \langle W(g_1), \dots, W(g_p) \rangle$. Each $g_j \in \mathbb{Z}_d^N \times \mathbb{Z}_d^N$ is called a generating element. Given one choice of generating elements, the corresponding subgroup of $\mathbb{Z}_d^N \times \mathbb{Z}_d^N$, i.e., $G_S := \{g \in \mathbb{Z}_d^N \times \mathbb{Z}_d^N \mid W(g) \in S\}$, is also denoted as $G_S = \langle g_1, \dots, g_p \rangle$.

Let S be a stabilizer with generating elements $\{g_1, \dots, g_p\}$. For prime d , each generator $W(g) \neq \mathbb{1}_d^{\otimes N}$ has d distinct eigenvalues with equal multiplicity [31], allowing us to associate each of the d eigenspaces of a generator $W(g_j)$ with a number $x_j \in \mathbb{Z}_d$. We write $\mathcal{Q}(x)$ for the joint eigenspace of $\{W(g_j)\}_{j=1}^p$, such that for all $|\phi\rangle \in \mathcal{Q}(x)$ and $j \in \{1, \dots, p\}$, $x = (x_1, \dots, x_p) \in \mathbb{Z}_d^p$ and $\mathcal{Q}(x) \subset \mathcal{H}_A^{\otimes N}$, we have $W(g_j)|\phi\rangle = \omega_{x_j}|\phi\rangle$ with $x_j \in \mathbb{Z}_d$ and $\omega_{x_j} \in \mathbb{C}$.

Decomposing the Hilbert space into eigenspaces of the generators, $\mathcal{H}_A^{\otimes N} \cong \bigoplus_{x \in \mathbb{Z}_d^p} \mathcal{Q}(x)$, defines the codespaces $\mathcal{Q}(x)$ in $\mathcal{H}_A^{\otimes N}$. Given $p \leq N$ generators of a stabilizer in $\mathcal{E}_N$ for prime dimensions d , the codespaces have dimension $\dim[\mathcal{Q}(x)] = d^{N-p} \forall x \in \mathbb{Z}_d^p$ [31]. Let S^* be the stabilizer with complex conjugated elements of S and generating operators $W^*(g_j)$. $\mathcal{Q}^*(x) \subset \mathcal{H}_B^{\otimes N}$ is the joint eigenspace of $\{W^*(g_j)\}_{j=1}^p$,

such that for all $|\phi\rangle \in \mathcal{Q}^*(x)$ and $j \in \{1, \dots, p\}$, we have $W^*(g_j)|\phi\rangle = \omega_{x_j}^*|\phi\rangle$.

Definition 4 (Error coset). Let $S \subset \mathcal{E}_N$ be a stabilizer and let $G_S \subset \mathbb{Z}_d^N \times \mathbb{Z}_d^N$ be the corresponding subgroup of error elements, such that $S = \{W(g) \mid g \in G_S\}$. Given an error element $e \in \mathbb{Z}_d^N \times \mathbb{Z}_d^N$, the error coset is defined as $C(e) := e + G_S = \{e + h \mid h \in G_S\}$.

Definition 5 (Codeword). Let $\mathcal{H}_A^{\otimes N} \cong \bigoplus_{x \in \mathbb{Z}_d^p} \mathcal{Q}(x)$ be decomposed into d^{N-p} -dimensional codespaces of a stabilizer S . Let $\{|u_{x,k}\rangle\}_{x \in \mathbb{Z}_d^p, k \in \mathbb{Z}_d^{N-p}}$ be an orthonormal basis of $\mathcal{H}_A^{\otimes N}$ with $|u_{x,k}\rangle \in \mathcal{Q}(x)$, i.e., $W(g_j)|u_{x,k}\rangle = \omega_{x_j}|u_{x,k}\rangle$, $\forall k, j$. The vectors $|u_{x,k}\rangle \in \mathcal{H}_A^{\otimes N}$ are called codewords of S in $\mathcal{H}_A^{\otimes N}$. The codewords of the stabilizer with complex conjugated elements S^* in $\mathcal{H}_B^{\otimes N}$ are denoted by $|u_{x,k}^*\rangle \in \mathcal{H}_B^{\otimes N}$.

Definition 6 (Encoding). Let $\{|x\rangle\}_{x \in \mathbb{Z}_d^p}$ be the computational basis of $\mathcal{H}_A^{\otimes p}$ and $\{|k\rangle\}_{k \in \mathbb{Z}_d^{N-p}}$ be the computational basis of $\mathcal{H}_A^{\otimes N-p}$. A unitary operator U on $\mathcal{H}_A^{\otimes N} \cong \mathcal{H}_A^{\otimes p} \otimes \mathcal{H}_A^{\otimes N-p}$ is an encoding for a stabilizer S in $\mathcal{H}_A^{\otimes N}$ if $\forall x \in \mathbb{Z}_d^p, k \in \mathbb{Z}_d^{N-p}$: $U(|x\rangle \otimes |k\rangle)$ is a codeword of S in $\mathcal{H}_A^{\otimes N}$.

If $U : |x\rangle \otimes |k\rangle \mapsto |u_{x,k}\rangle \in \mathcal{H}_A^{\otimes N}$ is an encoding for S in $\mathcal{H}_A^{\otimes N}$, then $U^* : |x\rangle \otimes |k\rangle \mapsto |u_{x,k}^*\rangle \in \mathcal{H}_B^{\otimes N}$ is an encoding for S^* in $\mathcal{H}_B^{\otimes N}$.

Definition 7 (Stabilizer measurement). Let $\mathcal{P}_A(x) : \mathcal{H}_A^{\otimes N} \rightarrow \mathcal{Q}(x)$ be the projection to the codespace $\mathcal{Q}(x)$ and $\mathcal{P}_B^*(y) : \mathcal{H}_B^{\otimes N} \rightarrow \mathcal{Q}^*(y)$ be the projection to the codespace $\mathcal{Q}^*(y)$. The measurement corresponding to the PVM $\{\mathcal{P}(x, y) := \mathcal{P}_A(x) \otimes \mathcal{P}_B^*(y) \mid x, y \in \mathbb{Z}_d\}$ is called stabilizer measurement.

Definition 8 (Symplectic product decomposition). The symplectic product of two error elements, $e = (\vec{k}, \vec{l})$ and $f = (\vec{m}, \vec{n})$, is defined as $\langle e, f \rangle := \sum_{i=1}^{N-1} l_i m_i - k_i n_i$. It induces a decomposition of the set of errors according to its values $s = (s_1, \dots, s_p)$ with respect to a stabilizer with generating elements $\{g_1, \dots, g_p\} : \mathcal{E}_N \cong \bigoplus_s \mathcal{E}(s)$, with

$$\mathcal{E}(s) := \{e \in \mathbb{Z}_d^N \times \mathbb{Z}_d^N \mid \langle g_j, e \rangle = s_j \forall j = 1, \dots, p\}. \quad (45)$$

Reference [31] demonstrates that the properties of the stabilizer encodings U and U^* can be leveraged to show that the state after steps 1–3 can be written in terms of certain unitary operators, the so-called error action operators $T_x^{U,e}$ for the error e , the encoding U , and the local stabilizer measurement outcome x .

Lemma 1 ([31]). Let U be an encoding of a stabilizer S with generating elements $\{g_1, \dots, g_p\}$. For each codespace $\mathcal{Q}(x) \subset \mathcal{H}_A^{\otimes N}$ and for each $W(e) \in \mathcal{E}_N$ with $(\langle g_1, e \rangle, \dots, \langle g_p, e \rangle) = (s_1, \dots, s_p)$, there exist unitary “action” operators $T_x^{U,e} : \mathcal{H}_A^{\otimes N-p} \rightarrow \mathcal{H}_A^{\otimes N-p}$ satisfying $U^\dagger W(e) U = \sum_{x \in \mathbb{Z}_d^p} |x + s\rangle \langle x| \otimes T_{x+s}^{U,e}$.

Proposition 1 [31]. Let S be a stabilizer with p generating elements defining the symplectic partition of errors in $\mathcal{E}_N \cong \bigoplus_s \mathcal{E}(s)$ and U be an encoding. Let $\rho_{AB} = \sum_{e,f \in \mathcal{E}_N} \rho(e, f) |\Omega(e)\rangle \langle \Omega(f)|$ be a general input state in the Bell basis. After performing the stabilizer measurements with results x, y , applying $U^{-1} \otimes (U^*)^{-1}$ and discarding the first p

copies, the output state $\sigma_{AB}^{x,y} \in \bigotimes_{n=p+1}^N \mathcal{H}_A \otimes \mathcal{H}_B$ is

$$\sigma_{AB}^{x,y} = \frac{1}{\mathbb{P}(x,y)} \sum_{e,f \in \mathcal{E}(x-y)} \rho(e,f) (T_x^{U,e} \otimes \mathbb{1}) \times |\Omega_{0,0}\rangle \langle \Omega_{0,0}|^{\otimes N-p} (T_x^{U,f} \otimes \mathbb{1})^\dagger. \quad (46)$$

B. Entanglement and secret-key distillation tasks

In this section, we briefly review the tasks of entanglement distillation and secret-key distillation and define the distillable entanglement and distillable key in the asymptotic and one-shot setting.

1. Entanglement distillation

The goal of entanglement distillation is to (approximately) create maximally entangled states, which we define as follows.

Definition 9 (Maximally entangled state of Schmidt rank D). The state

$$\Psi_{AB} := \frac{1}{D} \sum_{i,j=0}^{D-1} |i\rangle \langle j|_A \otimes |i\rangle \langle j|_B$$

is called the maximally entangled state of Schmidt rank D .

Using the shared bipartite state ρ_{AB} , Alice and Bob apply a protocol $(D, \mathcal{L}_{AB})$, where the Schmidt rank D is the local dimension of the maximally entangled target state and $\mathcal{L}_{AB}$ is a LOCC channel as in (1), which they apply to ρ_{AB} . The entanglement distillation error is given by

$$p_{\mathcal{E}}^{\text{err}}(\mathcal{L}_{AB}, \rho_{AB}) := 1 - \mathcal{F}(\Psi_{AB}, \mathcal{L}_{AB}(\rho_{AB})), \quad (47)$$

where Ψ_{AB} is the maximally entangled state and $\mathcal{F}(\rho, \sigma) := (\text{Tr}[\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}])^2$ is the fidelity of two mixed states [36].

The distillable entanglement of a quantum state measures how useful it is for entanglement distillation. Contrary to the asymptotic setting, in which infinitely many copies of the input state can be used for the distillation task, in the one-shot setting the LOCC channel corresponding to the protocol can only be used once. In this setting the output of the channel will generally differ by some error from the maximally entangled target state.

Definition 10 (One-shot distillable entanglement). The one-shot distillable entanglement with distillation error $\varepsilon \in [0, 1]$ of a bipartite state ρ_{AB} is

$$\mathcal{E}_D^\varepsilon(\rho_{AB}) := \sup_{D, \mathcal{L}_{AB}} \{\log_2 D : p_{\mathcal{E}}^{\text{err}}(\mathcal{L}_{AB}, \rho_{AB}) \leq \varepsilon\},$$

where $(D, \mathcal{L}_{AB})$ is a protocol creating approximately maximally entangled states of size D using the LOCC channel $\mathcal{L}_{AB}$.

In the asymptotic setting, Alice and Bob are allowed to use an infinite number of copies of ρ_{AB} to create maximally entangled states. If a protocol uses a finite number n of copies of ρ_{AB} , it is equivalent to a protocol using the input state $\rho_{AB}^{\otimes n}$ once. This allows defining the distillable entanglement in the asymptotic setting as the maximum of so-called achievable rates for the creation of target states.

Definition 11 (Rate, distillable entanglement of a quantum state). Given a protocol $(n, D, \mathcal{L}_{AB})$ for a LOCC channel $\mathcal{L}_{AB}$ acting on n copies of a state, having $p_{\mathcal{E}}^{\text{err}}(\mathcal{L}_{AB}, \rho_{AB}^{\otimes n}) \leq \varepsilon$, the

rate of the protocol is $R(n, D) := \frac{\log_2 D}{n}$. Given a state ρ_{AB} , a rate is achievable, if for all $\varepsilon \in (0, 1]$, $\delta > 0$ and sufficiently large n , there exists a protocol $(n, 2^{n(R-\delta)}, \mathcal{L}_{AB})$ with $p_{\mathcal{E}}^{\text{err}}(\mathcal{L}_{AB}, \rho_{AB}^{\otimes n}) \leq \varepsilon$. The quantity

$$\mathcal{E}_D(\rho_{AB}) := \sup\{R : R \text{ is an achievable rate for } \rho_{AB}\}$$

is called the distillable entanglement of ρ_{AB} .

2. Secret-key distillation

The goal of secret-key distillation is to (approximately) create tripartite key states. By definition, those states are a resource to establish a cryptographic key between two parties, which is secret from any malicious third party. For this, consider the local measurement channel corresponding to any local system F or G and composite system FG , respectively:

$$\mathcal{D}_F(\cdot) := \sum_i |i\rangle \langle i|_F (\cdot) |i\rangle \langle i|_F, \mathcal{D}_{FG}(\cdot) := \mathcal{D}_F(\cdot) \otimes \mathcal{D}_G(\cdot). \quad (48)$$

Definition 12 (Secret-key state). A state γ_{ABE} is a tripartite secret-key state of size K if, after application of the measurement channel $\mathcal{D}_{AB}$, the state becomes a maximally correlated state of size K in the systems A and B ,

$$\hat{\Psi}_{AB} = \frac{1}{K} \sum_{i=0}^{K-1} |i\rangle \langle i|_A \otimes |i\rangle \langle i|_B,$$

that is in product with the state σ_E of the system E :

$$\mathcal{D}_{AB}(\gamma_{ABE}) = \mathcal{D}_{AB} \otimes \mathbb{1}_E(\gamma_{ABE}) = \hat{\Psi}_{AB} \otimes \sigma_E.$$

To create such states from a given bipartite state ρ_{AB} , Alice and Bob use a protocol $(K, \mathcal{L}_{ABE})$, where K is the size of the key system and $\mathcal{L}_{ABE}$ is a LOPC channel as in (2), which they apply to a purification ϕ_{ABE} of ρ_{AB} . The key distillation error is given by

$$p_{\mathcal{K}}^{\text{err}}(\mathcal{L}_{ABE}, \rho_{AB}) := \inf_{\gamma_{ABE}} \{1 - \mathcal{F}(\gamma_{ABE}, \mathcal{L}_{ABE}(\phi_{ABE}))\}, \quad (49)$$

where the optimization is with respect to all tripartite key states γ_{ABE} .

Given a quantum state, the distillable key of that state quantifies how useful it is for secret-key distillation. We consider both the asymptotic setting of infinite resources (see, e.g., Refs. [14,37]) and the resource-limited one-shot setting (see, e.g., Refs. [11,15]). While the former allows infinitely many copies of an input state to be used simultaneously for the channel, in the one-shot setting, the LOPC channel is only used once with a fixed number of input states. In this setting, secret-key states can generally only be approximately created, so we consider protocols with a finite distillation error (49).

Definition 13 (One-shot distillable key). The one-shot distillable key with distillation error $\varepsilon \in [0, 1]$ of a bipartite state ρ_{AB} is

$$\mathcal{K}_D^\varepsilon(\rho_{AB}) := \sup_{K, \mathcal{L}_{ABE}} \{\log_2 K : p_{\mathcal{K}}^{\text{err}}(\mathcal{L}_{ABE}, \rho_{AB}) \leq \varepsilon\},$$

where $(K, \mathcal{L}_{ABE})$ is a protocol creating approximately secret-key states of size K using the LOPC channel $\mathcal{L}_{ABE}$.

In the asymptotic setting, Alice and Bob may use any number of copies of ρ_{AB} to produce secret-key states. If a protocol

uses n copies of ρ_{AB} , it is equivalent to a one-shot protocol using the input state $\rho_{AB}^{\otimes n}$ and we can define accordingly.

Definition 14 (Rate, distillable key of a quantum state). Given a protocol $(n, K, \mathcal{L}_{ABE})$ for a LOPC channel $\mathcal{L}_{ABE}$ acting on n copies of a state, having $p_K^{\text{err}}(\mathcal{L}_{ABE}, \rho_{AB}^{\otimes n}) \leq \varepsilon$, the rate of the protocol is $R(n, K) := \frac{\log_2 K}{n}$. Given a state ρ_{AB} , a rate is achievable, if for all $\varepsilon \in (0, 1]$, $\delta > 0$ and sufficiently large n , there exists a protocol $(n, 2^{n(R-\delta)}, \mathcal{L}_{ABE})$ with $p_K^{\text{err}}(\mathcal{L}_{ABE}, \rho_{AB}^{\otimes n}) \leq \varepsilon$. The quantity

$$\mathcal{K}_D(\rho_{AB}) := \sup\{R : R \text{ is an achievable rate for } \rho_{AB}\}$$

is called the distillable key of ρ_{AB} .

C. Distillation bounds based on generalized information measures

Given a certain bipartite input state ρ_{AB} , it is generally not clear if there exists a LOCC channel that transforms it to an approximately maximally entangled state. The same holds for LOPC channels to create an approximately secret-key state. However, there exist lower bounds on the (one-shot) distillable entanglement and the (one-shot) distillable secret key. These bounds are based on information measures that can be defined via generalized divergences (see Ref. [2] for a comprehensive summary). In the one-shot setting, these are “smoothed,” i.e., the environment around a given quantum state for which the measure is to be evaluated is taken into account. Often, the sine distance [2] is used to define this smoothing environment.

Definition 15 (Smoothing environment). Using the sine distance $P(\rho, \sigma) := \sqrt{1 - \mathcal{F}(\rho, \sigma)}$, the smoothing environment $B^\varepsilon(\rho)$ around a state ρ is defined as

$$\begin{aligned} B^\varepsilon(\rho) &:= \{\tilde{\rho} \in \mathcal{D}(\mathcal{H}) : P(\rho, \tilde{\rho}) \leq \varepsilon\} \\ &= \{\tilde{\rho} : \mathcal{F}(\rho, \tilde{\rho}) \geq 1 - \varepsilon^2\}. \end{aligned} \quad (50)$$

Specifically, we consider the following generalized divergences and related information quantities that can be used to bound the distillable secret key from below.

Definition 16 (Quantum relative entropy, quantum mutual information, coherent information [38,39]).

$$D(\rho||\sigma) := \begin{cases} \text{Tr}[\rho(\log_2 \rho - \log_2 \sigma)] & \text{if } \text{supp}(\rho) \subseteq \text{supp}(\sigma) \\ +\infty & \text{else} \end{cases}, \quad (51)$$

$$I(\rho_{AB}) := D(\rho_{AB}||\rho_A \otimes \rho_B), \quad (52)$$

$$I_c^{A|B}(\rho_{AB}) := D(\rho_{AB}||\mathbb{1}_A \otimes \rho_B). \quad (53)$$

Definition 17 (Quantum hypothesis testing relative entropy, hypothesis testing mutual information [13,40,41]).

$$\begin{aligned} D_H^\varepsilon(\rho||\sigma) &:= -\log_2(\inf_{\Lambda} \{\text{Tr}[\Lambda\sigma] : 0 \leq \Lambda \leq \mathbb{1}, \text{Tr}[\Lambda\rho] \geq 1 - \varepsilon\}), \\ & \quad (54) \end{aligned}$$

$$I_H^\varepsilon(\rho_{AB}) := \inf_{\sigma_B} D_H^\varepsilon(\rho_{AB}||\rho_A \otimes \sigma_B), \quad (55)$$

where the optimization is over all quantum states σ_B .

Definition 18 (Max-relative entropy, smooth max-mutual information [42], smooth conditional max-entropy [12]).

$$D_{\max}(\rho||\sigma) := \begin{cases} \log_2 \|\sigma^{-\frac{1}{2}} \rho \sigma^{-\frac{1}{2}}\|_\infty & \text{if } \text{supp}(\rho) \subseteq \text{supp}(\sigma) \\ +\infty & \text{else} \end{cases} \quad (56)$$

$$I_{\max}^\varepsilon(\rho_{AB}) := \inf_{\tilde{\rho}_{AB} \in B^\varepsilon(\rho_{AB})} D_{\max}(\tilde{\rho}_{AB}||\rho_A \otimes \tilde{\rho}_B), \quad (57)$$

$$H_{\max}^\varepsilon(\rho_{AB}) := \inf_{\substack{\tilde{\rho}_{AE} \in B^\varepsilon(\rho_{AE}) \\ \sigma_E}} D_{\max}(\tilde{\rho}_{AE}||\mathbb{1}_A \otimes \sigma_E) \quad (58)$$

where σ_E is a quantum state, $\rho_{AE} := \text{Tr}_B[\phi_{ABE}]$ is defined via the purification ϕ_{ABE} of ρ_{AB} , and $B^\varepsilon(\rho_{AB})$ is as in Definition 15.

Note that the definition of $H_{\max}^\varepsilon$ of Definition 18 is based on the smooth conditional min-entropy $H_{\min}^\varepsilon$ and the duality $H_{\max}^\varepsilon(\rho_{AB}) = -H_{\min}^\varepsilon(\rho_{AE})$. Consult Refs. [2,11] for more details.

We are now in a position to state the lower bounds on the one-shot and asymptotic distillable entanglement and distillable key, motivating the information quantities under consideration in this work.

Theorem 3 (Lower bound for the one-shot distillable entanglement [2,16]). Let ρ_{AB} be a bipartite state. Let $\mathcal{L}$ be any LOCC channel with output $\mathcal{L}(\rho_{AB}) = \hat{\rho}_{AB}$, $\varepsilon \in (0, 1]$, and $\eta \in [0, \sqrt{\varepsilon}]$. It holds that

$$\mathcal{E}_D^\varepsilon(\rho_{AB}) \geq \sup_{\mathcal{L}} [-H_{\max}^{\sqrt{\varepsilon}-\eta}(\hat{\rho}_{AB}) + 4 \log_2(\eta)]. \quad (59)$$

Theorem 4 (Characterization of the distillable entanglement [2,14]). Let ρ_{AB} be a bipartite state. Let $\mathcal{L}^{(n)}$ be any LOCC channel acting on n copies of ρ_{AB} with output $\mathcal{L}^{(n)}(\rho_{AB}^{\otimes n}) = \hat{\rho}_{AB}$. It holds that

$$\mathcal{E}_D(\rho_{AB}) = \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{\mathcal{L}^{(n)}} I_c^{A|B}(\hat{\rho}_{AB}). \quad (60)$$

For secret-key distillation, the bounds are based on so-called classical-quantum-quantum states, having the form $\chi_{ABE} = \sum_i |i\rangle\langle i|_A \otimes \chi_{BE}^i$.

Theorem 5 (Lower bound for the one-shot distillable key [2,15]). Let ρ_{AB} be a bipartite state with purification ϕ_{ABE} . Let $\varepsilon \in (0, 1]$, $\mathcal{L}$ be any LOPC channel with classical-quantum-quantum output $\mathcal{L}(\phi_{ABE}) = \chi_{ABE}$ and $\varepsilon' = 1 - \sqrt{1 - \varepsilon}$. It holds that

$$\begin{aligned} \mathcal{K}_D^\varepsilon(\rho_{AB}) &\geq \sup_{\substack{\mathcal{L}, \\ \delta \in (0, \varepsilon'), \\ \eta \in (0, \varepsilon' - \delta), \\ \zeta \in (0, \delta)}} \left[I_H^{\varepsilon' - \delta - \eta}(\chi_{AB}) - I_{\max}^{\delta - \zeta}(\chi_{AE}) \right. \\ &\quad \left. - \log_2 \left(\frac{4(\varepsilon' - \delta)}{\eta^2} \right) - \log_2 \left(\frac{2}{\zeta^2} \right) \right]. \end{aligned} \quad (61)$$

Theorem 6 (Characterization of the distillable key [2,14]). Let ρ_{AB} be a bipartite state with purification ϕ_{ABE} . Let $\mathcal{L}^{(n)}$ be any LOPC channel acting on n copies of ϕ_{ABE} with classical-quantum-quantum output $\mathcal{L}^{(n)}(\phi_{ABE}^{\otimes n}) = \chi_{ABE}$. It holds that

$$\mathcal{K}_D(\rho_{AB}) = \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{\mathcal{L}^{(n)}} [I(\chi_{AB}) - I(\chi_{AE})]. \quad (62)$$

The quantity $I_p(\chi_{ABE}) := I(\chi_{AB}) - I(\chi_{AE})$ is also called private information.

ACKNOWLEDGMENTS

This research was funded in whole, or in part, by the Austrian Science Fund (FWF) (Grant No. 10.55776/P36102).

Conceptualization, C.P.; validation, C.P., T.C.S., and B.C.H.; formal analysis, C.P.; writing—original draft preparation, C.P.; writing—review and editing, C.P., T.C.S., and

B.C.H. All authors have read and agreed to the published version of the manuscript.

DATA AVAILABILITY

The data that support the findings of this article are not publicly available. The data are available from the authors upon reasonable request.

-
- [1] E. Chitambar and G. Gour, Quantum resource theories, *Rev. Mod. Phys.* **91**, 025001 (2019).
 - [2] S. Khatri and M. M. Wilde, Principles of quantum communication theory: A modern approach, [arXiv:2011.04672](#).
 - [3] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, *Rev. Mod. Phys.* **81**, 865 (2009).
 - [4] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, General paradigm for distilling classical key from quantum states, *IEEE Trans. Inf. Theory* **55**, 1898 (2009).
 - [5] D. P. DiVincenzo, D. W. Leung, and B. M. Terhal, Quantum data hiding, *IEEE Trans. Inf. Theory* **48**, 580 (2002).
 - [6] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, Locking classical correlations in quantum states, *Phys. Rev. Lett.* **92**, 067902 (2004).
 - [7] M. M. Wilde, *Quantum Information Theory* (Cambridge University, Cambridge, England, 2013).
 - [8] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Purification of noisy entanglement and faithful teleportation via noisy channels, *Phys. Rev. Lett.* **76**, 722 (1996).
 - [9] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
 - [10] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [11] M. Tomamichel, *Quantum Information Processing with Finite Resources: Mathematical Foundations*, Springer briefs in Mathematical Physics Vol. 5 (Springer, New York, 2016).
 - [12] R. Renner, Security of quantum key distribution, [arXiv:quant-ph/0512258](#).
 - [13] L. Wang and R. Renner, One-shot classical-quantum capacity and hypothesis testing, *Phys. Rev. Lett.* **108**, 200501 (2012).
 - [14] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, *Proc. R. Soc. A* **461**, 207 (2005).
 - [15] S. Khatri, E. Kaur, S. Guha, and M. M. Wilde, Second-order coding rates for key distillation in quantum key distribution, [arXiv:1910.03883](#).
 - [16] M. M. Wilde, M. Tomamichel, and M. Berta, Converse bounds for private communication over quantum channels, *IEEE Trans. Inf. Theory* **63**, 1792 (2017).
 - [17] C. Popp, T. C. Sutter, and B. C. Hiesmayr, Local invariance of divergence-based quantum information measures, *Entropy* **27**, 1051 (2025).
 - [18] P. Skrzypczyk and D. Cavalcanti, *Semidefinite Programming in Quantum Information Science* (Institute of Physics, University of Reading, Berkshire, 2023).
 - [19] A. Tavakoli, A. Pozas-Kerstjens, P. Brown, and M. Araújo, Semidefinite programming relaxations for quantum correlations, *Rev. Mod. Phys.* **96**, 045006 (2024).
 - [20] T. Nuradha and M. M. Wilde, Fidelity-based smooth min-relative entropy: Properties and applications, *IEEE Trans. Inf. Theory* **70**, 4170 (2024).
 - [21] C. Popp, T. C. Sutter, and B. C. Hiesmayr, Computation of the smooth max-mutual information via semidefinite programming, *Quantum Info. Proc.* **25**, 86 (2026).
 - [22] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Quantum privacy amplification and the security of quantum cryptography over noisy channels, *Phys. Rev. Lett.* **77**, 2818 (1996).
 - [23] M. Horodecki and P. Horodecki, Reduction criterion of separability and limits for a class of distillation protocols, *Phys. Rev. A* **59**, 4206 (1999).
 - [24] G. Alber, A. Delgado, N. Gisin, and I. Jex, Efficient bipartite quantum state purification in arbitrary dimensional Hilbert spaces, *J. Phys. A* **34**, 8821 (2001).
 - [25] J. Miguel-Ramiro and W. Dür, Efficient entanglement purification protocols for d -level systems, *Phys. Rev. A* **98**, 042309 (2018).
 - [26] J. Dehaene, M. Van den Nest, B. De Moor, and F. Verstraete, Local permutations of products of Bell states and entanglement distillation, *Phys. Rev. A* **67**, 022310 (2003).
 - [27] K. G. H. Vollbrecht and M. M. Wolf, Efficient distillation beyond qubits, *Phys. Rev. A* **67**, 012303 (2003).
 - [28] E. Rains, Nonbinary quantum codes, *IEEE Trans. Inf. Theory* **45**, 1827 (1999).
 - [29] A. Ashikhmin and E. Knill, Nonbinary quantum stabilizer codes, *IEEE Trans. Inf. Theory* **47**, 3065 (2001).
 - [30] R. Matsumoto, Conversion of a general quantum stabilizer code to an entanglement distillation protocol, *J. Phys. A* **36**, 8113 (2003).
 - [31] C. Popp, T. C. Sutter, and B. C. Hiesmayr, A novel stabilizer-based entanglement distillation protocol for qudits, *Quantum* **9**, 1945 (2025).
 - [32] C. Popp, T. C. Sutter, and B. C. Hiesmayr, Low-fidelity entanglement distillation with FIMAX, *Int. J. Quantum Inf.* **23**, 2550017 (2025).

- [33] C. Popp, BellDiagonalQudits: A package for entanglement analyses of mixed maximally entangled qudits, *J. Open Source Softw.* **8**, 4924 (2023).
- [34] T. Kiss, S. Vymětal, L. D. Tóth, A. Gábris, I. Jex, and G. Alber, Measurement-induced chaos with entangled states, *Phys. Rev. Lett.* **107**, 100501 (2011).
- [35] B. C. Hiesmayr, C. Popp, and T. C. Sutter, Bipartite bound entanglement, *Int. J. Quantum Inf.* **23**, 2530003 (2025).
- [36] A. Uhlmann, The “transition probability” in the state space of a $*$ -algebra, *Rep. Math. Phys.* **9**, 273 (1976).
- [37] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, in *Theory of Cryptography*, edited by S. P. Vadhan (Springer-Verlag, Berlin, 2007), pp. 456–478.
- [38] H. Umegaki, Conditional expectation in an operator algebra. IV. Entropy and information, *Kodai Math. J.* **14**, 59 (1962).
- [39] F. Hiai and D. Petz, The proper formula for relative entropy and its asymptotics in quantum probability, *Commun. Math. Phys.* **143**, 99 (1991).
- [40] M. Hayashi and H. Nagaoka, in *Proceedings IEEE International Symposium on Information Theory* (IEEE, New York, 2002), p. 71.
- [41] F. Buscemi and N. Datta, The quantum capacity of channels with arbitrarily correlated noise, *IEEE Trans. Inf. Theory* **56**, 1447 (2010).
- [42] N. Datta, Min- and max-relative entropies and a new entanglement monotone, *IEEE Trans. Inf. Theory* **55**, 2816 (2009).