

Threshold (Q, P) distillation of multipartite quantum correlationsShashank Gupta^{1,2,3,*}, William John Munro¹, and Carlos Cid^{1,4}¹*Okinawa Institute of Science and Technology Graduate University, Okinawa 904-0495, Japan*²*QuNu Labs Pvt. Ltd., M. G. Road, Bengaluru 560025, Karnataka, India*³*Indian Institute of Technology Indore, Khandwa Road, Simrol, Indore 453552, Madhya Pradesh, India*⁴*Simula UiB, Bergen, Norway*

(Received 17 September 2024; revised 21 August 2025; accepted 5 January 2026; published 10 February 2026)

We introduce a threshold quantum distillation protocol that enables the extraction of perfect quantum correlations from multiple imperfect copies of a multipartite quantum state using only a subset of the parties ($Q < P$) in the network. In particular, we show that for high-dimensional Greenberger–Horne–Zeilinger states, entanglement can be distilled by local filtering operations applied by just a single party, independent of the total number of parties in the network. In contrast, for the W states, at least $P - 1$ parties are required for successful distillation, highlighting a strong connection between distillability and separability. We provide explicit protocols for threshold entanglement distillation and threshold steering distillation (TSD), and establish a direct link between the two: Any assemblage that can be distilled via TSD necessarily corresponds to a distillable entangled state. Our framework introduces a scalable and experimentally viable approach to distillation in quantum networks, with potential applications in distributed quantum computing, communication, and cryptography.

DOI: [10.1103/6zdc-j51g](https://doi.org/10.1103/6zdc-j51g)

Introduction. The idea of a threshold is a fundamental technique in classical cryptography to provide privacy, security, and fault tolerance [1]. A well-celebrated protocol underpinning the threshold concept is the Shamir (Q, P) secret-sharing scheme, where any Q out of P parties can collaborate to recover a hidden secret [2]. Several protocols have adopted threshold features to improve secure multiparty computation, signatures, and database management in classical cryptography [3–8]. Here for the first time, we extend this idea in the quantum domain for the distillation task by using only a subset of the parties ($Q < P$). Quantum cryptography can only exist if the underlying quantum resource is above a specific value [9–12]. To achieve this, the distillation of the quantum resources is fundamental [13–16], leading to the proposal of several distillation or quantum privacy amplification protocols. In bipartite systems, distillation protocols for quantum entanglement [17–22], EPR (Einstein-Podolsky-Rosen) steering [23–25], and Bell nonlocality [26–31] are well established. Quantum entanglement represents nonseparable correlations in composite quantum systems, and steering is the semi-device-independent manifestation of the same. Recent research has addressed a long-standing issue in two-qubit systems by closing the Werner gap in quantum steering [32]. Subsequent work has underscored the practical challenges and future directions of EPR steering [33], underscoring its

potential in quantum technologies [34,35]. In the context of multipartite systems, distillation protocols have been proposed for genuine entanglement [36,37], genuine steering [38], and Bell nonlocality [39–42]. However, most of these proposed distillation protocols are not practically efficient as they require the participation of all parties involved, either directly or indirectly, to extract ideal quantum resources. Additionally, the relationship between different distillation protocols is not clearly defined. We propose a more efficient distillation protocol that requires the participation of fewer parties to achieve the desired outcome. Furthermore, we establish a strong connection between the distillation of steering and entanglement. This proposal aims to enhance the practicality and understanding of quantum resource extraction in multipartite systems.

Perfect quantum correlation. These represent an extremal point in a given polytope, which is the most desirable in any quantum information processing task [43]. However, environmental interactions and experimental imperfections restrict one from realizing the perfect quantum correlation, thus degrading the performance of the implemented task. Distillation addresses this problem by concentrating on imperfect correlations [18]. This Letter focuses on distilling the underlying state or assemblage rather than specific correlation. Once we distill the state, we distill the correlation as well.

Threshold quantum distillation (N, d, P, Q) . Consider a quantum network constituted by P spatially separated parties (see Fig. 1). Let the parties share N copies of quantum states (or assemblage in case of quantum steering) $\rho \in \mathcal{B}(\otimes_{i=1}^P \mathcal{H}_i^d)$, where d is the dimension of each subsystem. Here, $\mathcal{B}$ is the set of all density matrices in the Hilbert space $\otimes_{i=1}^P \mathcal{H}_i^d$. In general, the dimension of each subsystem might be different, but for simplicity, we consider it to be the same. The objective of

*Contact author: shashankg687@gmail.com

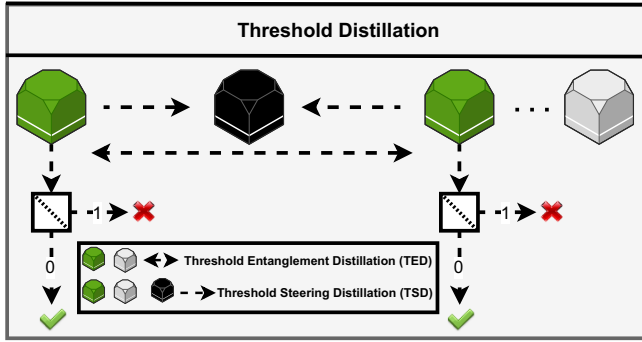


FIG. 1. Threshold distillation framework. Here, the green colored parties (Q) participate in the distillation protocol by applying local filtering operations. If the subsystem undergoes operation 0, the protocol is successful; otherwise, it fails. Nonparticipating parties, marked in gray ($P - Q$), act as ideal parties. Uncharacterized parties (S), marked in black, may also be present, forming an asymmetric network under quantum steering. Classical communication is two-way (double-sided dashed arrow) between characterized parties and one-way (single-sided dashed arrow) from characterized to uncharacterized parties. Q , $P - Q$, and two-way communication define threshold entanglement distillation, while Q , $P - Q$, S , and one-way communication define threshold steering distillation.

threshold quantum distillation is to extract fewer copies of the perfect quantum states (or assemblages) using a smaller number Q ($Q < P$) of parties and free operations only. The free operations are defined with respect to the distillable resource. For example, local operation and classical communication (LOCC) is used for entanglement, while one-way LOCC is used for quantum steering.

Performance metrics. The performance is measured using the fidelity. The metric is state (assemblage) fidelity for entanglement (steering), respectively, with respect to the perfect state or assemblage. Let ρ^{dist} be the state after the application of the threshold distillation protocol, and ρ^{perf} the perfect state in the same Hilbert space. The state fidelity between them is $\mathcal{F}_s(\rho^{\text{dist}}, \rho^{\text{perf}}) := \max_{\text{perf}} [\text{Tr}(\sqrt{\sqrt{\rho^{\text{dist}}} \rho^{\text{perf}} \sqrt{\rho^{\text{dist}}}})]^2$. Similarly, let $\{\sigma_{a_i|x_i}^{\text{dist}}\}$ be the assemblage after the application of the threshold steering distillation protocol, while $\{\sigma_{a_i|x_i}^{\text{perf}}\}$ be the assemblage of the same dimension with perfect steerability. The assemblage fidelity between them is $\mathcal{F}_a(\{\sigma_{a_i|x_i}^{\text{dist}}\}, \{\sigma_{a_i|x_i}^{\text{perf}}\}) := \min_{x_i} \sum_{a_i} [\text{Tr}(\sqrt{\sqrt{\sigma_{a_i|x_i}^{\text{dist}}} \sigma_{a_i|x_i}^{\text{perf}} \sqrt{\sigma_{a_i|x_i}^{\text{dist}}}})]^2$. Note that the minimization is required over the measurement settings of the uncharacterized parties [23].

Threshold entanglement distillation protocol (N, d, P, Q). In a quantum network consisting of (P) parties sharing imperfect entanglement, the threshold entanglement distillation (TED) concept is that a smaller number of parties (Q), called participating parties, perform local filtering operations to distill the perfect entanglement with some success probability. The nonparticipating parties ($P - Q$) perform no actions (see Fig. 1). We start with $N \geq 2$ copies of initial partially entangled states ρ^{ini} . Each of the Q parties performs dichotomic POVM (Positive Operator-Valued-Measure) $\mathcal{G}^i := \{G_0^i, G_1^i\}$, satisfying $G_{o_i^i}^i \geq 0 \forall o_i^i \in \{0, 1\}$ and $G_0^i + G_1^i = 1$ on the u th copy of the initial state with ($u \in \{1, 2, \dots, N - 1\}$). Here, G_0^i

implies success, while G_1^i means failure for a given run. If any Q parties obtain $o_i^u = 1 \forall u$, then the parties set $o_i^N = 0$ for the last copy without performing POVMs; otherwise, set $o_i^N = 1$ for the last copy. This will ensure that even if the distillation protocol fails, the network retains at least one copy with the initial correlation.

Next, the Q parties send the string $o_i := \{o_i^1, o_i^2, o_i^3, \dots, o_i^N\}$ to all the parties in the network through the classical channel. Finally, all the parties discard the u th copies for which any $o_i^u = 1$. The remaining copies of the states give the protocol output. For the filtering operation, we use the following notation: $K_{o_i^i}^i = \sqrt{G_{o_i^i}^i}$ such that $G_{o_i^i}^i = K_{o_i^i}^{i\dagger} K_{o_i^i}^i$. In the above protocol, the state of the u th copy after the application of the local filtering operations by the participating parties is

$$\rho_u^{\text{dist}} = \frac{\otimes_Q K_{o_i^i}^Q \otimes_{P-Q} \mathcal{I}^{P-Q} \cdot \rho_u^{\text{ini}} \cdot \otimes_Q K_{o_i^i}^{Q\dagger} \otimes_{P-Q} \mathcal{I}^{P-Q}}{\text{Tr}[\otimes_Q K_{o_i^i}^Q \otimes_{P-Q} \mathcal{I}^{P-Q} \cdot \rho_u^{\text{ini}} \cdot \otimes_Q K_{o_i^i}^{Q\dagger} \otimes_{P-Q} \mathcal{I}^{P-Q}]}$$

The success probability for the u th copy (P_s^u) is given by $\text{Tr}[\otimes_Q K_{o_i^i}^Q \otimes_{P-Q} \mathcal{I}^{P-Q} \cdot \rho_u^{\text{ini}} \cdot \otimes_Q K_{o_i^i}^{Q\dagger} \otimes_{P-Q} \mathcal{I}^{P-Q}]$. The action of the local filtering operation is independent of each copy, so the failure probability (at least one Q party gets outcome 1 for the u th copy where $u \in \{1, 2, \dots, N - 1\}$) is $(1 - P_s^u)^{N-1}$. This implies that the overall success probability of the threshold distillation protocol (P_s) is $1 - (1 - P_s^u)^{N-1}$. Now, the final state (ρ^{dist}) after the distillation protocol can be written as a convex combination of the perfect state with probability P_s and the initial state with probability $1 - P_s$. This state is used to determine the state fidelity postdistillation.

Threshold steering distillation protocol (N, d, S, P, Q). In a network with uncharacterized (S) and characterized ($P - S$) parties sharing entanglement, measurements by uncharacterized parties can influence the outcomes for characterized parties, leading to quantum steering. Threshold steering distillation (TSD) involves some characterized parties acting as the participating parties (Q), applying local filtering operations on their part of the assemblage (unnormalized conditional states left on the characterized parties' subsystem after uncharacterized parties' measurements). The operation performed by the characterized parties in the steering scenario is one-way LOCC (see Fig. 1). The TSD protocol is similar to TED protocol but the description is in terms of the assemblage instead of the underlying state.

The state of the u th copy of the assemblage after the application of the local filtering operations by the participating characterized parties (Q , where $Q < P - S < P$) is

$$\sigma_{a_i|x_i}^{\text{dist}} = \frac{\otimes_Q K_{o_i^i}^Q \otimes_{P-Q} \mathcal{I}^{P-Q} \cdot \sigma_{a_i|x_i}^{\text{ini}} \cdot \otimes_Q K_{o_i^i}^{Q\dagger} \otimes_{P-Q} \mathcal{I}^{P-Q}}{\text{Tr}[\otimes_Q K_{o_i^i}^Q \otimes_{P-Q} \mathcal{I}^{P-Q} \cdot \rho_{\text{ch}}^{\text{ini}} \cdot \otimes_Q K_{o_i^i}^{Q\dagger} \otimes_{P-Q} \mathcal{I}^{P-Q}]}$$

Here, $\rho_{\text{ch}}^{\text{ini}}$ is the conditional state on the characterized parties subsystems, i.e. $\rho_{\text{ch}}^{\text{ini}} = \text{Tr}_{\text{unch}} \rho^{\text{ini}}$. The success probability of the TSD protocol for the u th copy (P_s^u) is $\text{Tr}[\otimes_Q K_{o_i^i}^Q \otimes_{P-Q} \mathcal{I}^{P-Q} \cdot \rho_{\text{ch}}^{\text{ini}} \cdot \otimes_Q K_{o_i^i}^{Q\dagger} \otimes_{P-Q} \mathcal{I}^{P-Q}]$. Using the above threshold distillation protocols, we have the following results for the quantum state/assemblage.

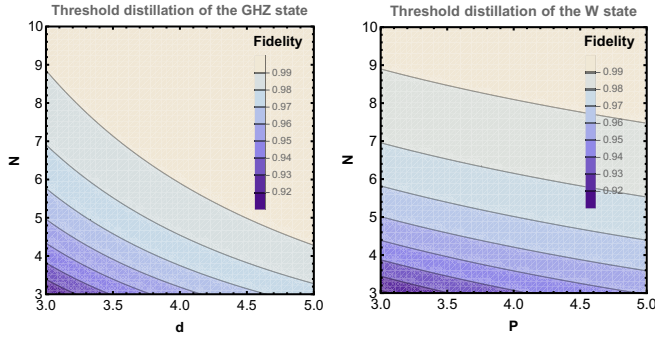


FIG. 2. Performance of the threshold distillation of the Greenberger-Horne-Zeilinger (GHZ) state (1) on the left and W state (3) on the right. The fidelity (2) is plotted concerning the number of copies N and the dimension d of the subsystem for a fixed value of the first state parameter ($\alpha_0 = 1/\sqrt{10}$) and the fixed difference (0.5) between d and $(\sum \alpha_i)^2$. Similarly, the fidelity (4) is plotted as a function of the number of copies N and the number of the parties P for a fixed value of the success probability ($P_s^u = 0.3$) and the fixed difference (0.5) between P and $(\sum \beta_i)^2$.

Theorem 1 (TED of the GHZ states). In a quantum network sharing multipartite high-dimensional GHZ states of the form

$$|\rho_{\text{GHZ}}^{\text{ini}}\rangle = \sum_{i=0}^{d-1} \alpha_i |\otimes_{j=0}^{P-1} i_j\rangle_d, \quad (1)$$

quantum entanglement can be distilled using a TED protocol ($N, d, P, 1 \leq Q \leq P-1$) with the success probability per copy ($P_s^u = d\alpha_0^2$) and the state fidelity

$$\mathcal{F}_s(\rho^{\text{dist}}, \rho_{\text{GHZ}}^{\alpha_i = \frac{1}{\sqrt{d}}}) = \left[1 - \frac{1}{d} (1 - P_s^u)^{N-1} \left(d - \left(\sum_{i=0}^{d-1} \alpha_i \right)^2 \right) \right], \quad (2)$$

which are independent of the number of parties in the network (P) and the number of participating parties (Q).

Using the local filtering operations by the Q parties ($1 \leq Q \leq P-1$) on the initial state (1) and postselecting the state when all the Q parties get the outcome zero yields the expression of the fidelity (2). It is a threshold distillation as the final fidelity (2) is same irrespective of whether $Q = 1, 2$, or $P-1$. For the expression of Krauss operators for a specific Q , detailed proof, and toy examples, see the Supplemental Material (I) [44]. The fidelity improves remarkably with increasing N and d (see Fig. 2). The fidelity is greater than 0.99% over 50% of the region. It asymptotically approaches 1. In experiments, the yield of high-fidelity states is also extremely important. We define the yield as the number of output states with improved fidelity with respect to the initial state. We found that for the N copies of the GHZ state with the initial fidelity of 0.7/0.8/0.9, $N/2$ copies are created with final fidelity of 0.91, 0.96, and 0.99 and success probability of 0.7/0.8/0.9, respectively. Similarly, $N/3$ copies are created with final fidelity of 0.973, 0.992, and 0.999 with success probability of 0.7/0.8/0.9, respectively, per copy.

Consider the assemblage derived from the GHZ state (1) by the action of uncharacterized parties ($1 \leq S \leq P-1$) in two

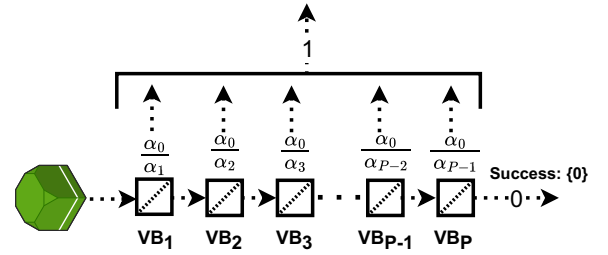


FIG. 3. Realization of a single-party Krauss operator for the TED (TSD) of the GHZ state (1) (assemblage) using cascaded variable reflectivity beam splitters (VBs). The output coefficient is tuned as per the ratio of the state parameters concerning the first parameter (α_0). The concept experiment follows from the recent experiment [23,46].

mutually unbiased bases (MUBs) [45]. These assemblages are imperfectly steerable due to the underlying state's imperfections. Only characterized parties can perform local filtering to distill the assemblage, making threshold distillation a natural fit in a realistic network.

Theorem 2 (TSD of the GHZ assemblages). In a quantum network sharing multipartite high-dimensional assemblages derived from the GHZ state (1) on the application of MUBs by uncharacterized parties, quantum steering can be distilled using a TSD protocol ($N, d, 1 \leq S \leq P-2, P, 1 \leq Q \leq P-S-1$) with the assemblage fidelity same as the state fidelity ($\mathcal{F}_s(\rho^{\text{dist}}, \rho_{\text{GHZ}}^{\alpha_i = \frac{1}{\sqrt{d}}})$) (2).

In a steering scenario ($1 \leq S \leq P-2$), some characterized parties ($P-S$) can act as participating parties ($1 \leq Q \leq P-S-1$). These parties use the same Krauss operators as in TED to distill the assemblage. They perform local filtering and postselect the assemblage when all Q parties get outcome zero. The assemblage fidelity is derived using the distilled and perfect assemblages corresponding to the GHZ state ($\forall \alpha_i = 1/\sqrt{d}$), minimizing over the characterized parties' input measurements. Note that $S = P-1$ is a valid steering scenario, allowing steering distillation with the only characterized party left, but it is not a valid TSD as all remaining characterized parties are being used. See the Supplemental Material (III) [44] for detailed proof and examples.

The GHZ state becomes separable when one party performs a projective measurement, making its entanglement tunable by a single party. We have identified the Krauss operator for a single party to distill GHZ-type entanglement and steering. We propose a concept experiment to realize the Krauss operator of the single party to distill GHZ state (1) [23] (see Fig. 3). The Krauss operator can be realized using a cascade of tunable beam splitters to tune their output coefficient as per the ratio of the state parameter concerning the first state parameter. Further tuning and postselection can be done using other passive optical components.

Corollary 1. A TED (TSD) is possible with at least one party when the shared state (assemblage) in the quantum network is a multipartite high-dimensional nonmaximally entangled GHZ state (assemblage), implying that GHZ state (assemblage) distillation and separability are strongly connected.

We know that quantum steering is a stronger correlation than entanglement [47]. This means a steerable state is always entangled. This implies that a steering distillation protocol can also distill entanglement.

Corollary 2. The existence of the TSD protocol in the quantum network sharing the assemblage derived from the GHZ state of the form (1) always indicates the existence of TED. The uncharacterized parties in the TSD can be nonparticipating parties in TED.

The above result holds as the number of nonparticipating parties in the entanglement scenario can be greater than or equal to the number of uncharacterized parties in the steering scenario for the GHZ state (1), i.e., $(P - Q \geq S)$.

Corollary 3. For a quantum network sharing a rank-2 mixed GHZ state with orthogonal constituent pure GHZ state, quantum entanglement (steering) can be distilled with success probability per copy $(P_{s(r=2)}^u = d\alpha_0^2)$ and state fidelity

$$\mathcal{F}_s(\rho_{\text{GHZ}}^{\text{dist}(r=2)}, \rho_{\text{GHZ}}^{\alpha_i=\frac{1}{\sqrt{d}}}) = \left[p - \frac{2p-1}{d} (1 - P_{s(r=2)}^u)^{N-1} \left(d - \left(\sum_{i=0}^{d-1} \alpha_i \right)^2 \right) \right],$$

when the corresponding state parameters are same and dimension of the subsystem is even to ensure orthogonality [48]. Here, “ p ” is the mixing parameter.

For details and results on higher rank mixed states, see the Supplemental Material (II) [44]. Next, we consider the W state under the action of threshold distillation.

Theorem 3 (TED of the W states). In a quantum network sharing multipartite W states of the form

$$|\rho_W^{\text{init}}\rangle = \sum_{i=0}^{P-1} \beta_i |\cdots 0_{i-1} 1_i 0_{i+1} \cdots\rangle, \quad (3)$$

quantum entanglement can be distilled using a TED protocol $(N, d = 2, P, Q = P - 1)$ with the success probability per copy $(P_s^u = P \frac{\prod_{i=0}^{P-1} \beta_i^2}{\beta_{P-1}^2})$ and state fidelity

$$\mathcal{F}_s(\rho^{\text{dist}}, \rho_W^{\beta_i=\frac{1}{\sqrt{P}}}) = \left[1 - \frac{1}{P} (1 - P_s^u)^{N-1} \left(P - \left(\sum_{i=0}^{P-1} \beta_i \right)^2 \right) \right]. \quad (4)$$

Using the local filtering operations by the participating parties $(Q = P - 1)$ on the initial state (3) and postselecting the state when all the Q parties get the outcome zero yields the expression of fidelity (4). See the Supplemental Material (IV) [44] for details. The fidelity improves remarkably with increments in the number of copies (N) and the number of parties (P) (see Fig. 2), and it asymptotically approaches 1.

Consider the assemblage derived from the W state (3) by the first party’s action in the computational and Hadamard bases. These assemblages are imperfect due to the underlying state’s imperfections. All characterized parties (in total $P - 1$) perform local filtering to distill the assemblage. Thus, in a

realistic network with characterized and uncharacterized parties sharing the W state, only steering distillation is possible, not threshold distillation, as at least $P - 1$ parties are needed. Distillation for other steering scenarios $(S > 1)$ is not feasible unless constraints are placed on the state parameters.

Theorem 4 (steering distillation of the W assemblages). For a quantum network sharing multipartite assemblages derived from the W state (3) on the action of MUBs by uncharacterized parties, quantum steering can be distilled using an steering distillation (SD) protocol $(N, d = 2, S = 1, P, Q = P - 1)$ with the assemblage fidelity same as the state fidelity $(\mathcal{F}_s(\rho^{\text{dist}}, \rho_W^{\beta_i=\frac{1}{\sqrt{P}}}))$ (4).

In the one-sided device-independent (1SDI) steering scenario $(S = 1)$, all the $P - 1$ characterized parties use the same Krauss operators as in the case of TED to distill the assemblage. The participating parties perform local filtering operations on their part of the assemblage and postselect the assemblage when all the Q parties get the outcome zero. The expression of the assemblage fidelity is then determined using distilled assemblage and the perfect assemblage $(\forall \beta_i = 1/\sqrt{P})$, where a minimization over the input measurements of the first party is done to determine the correct assemblage fidelity. See the Supplemental Material (V) [44] for details.

The W state (3) remains entangled up to the last bipartite configuration, meaning its genuine entanglement is tunable by the collaboration of all parties (except one due to normalization). We have identified the Krauss operator for $P - 1$ parties to distill W -type entanglement and steering.

Corollary 4. A TED (SD) is possible with at least $P - 1$ parties when the shared state (assemblage) in the quantum network is a multipartite nonmaximally entangled W state (assemblage), implying that W state (assemblage) distillation and separability are strongly connected.

It is well understood that the quantum steering correlation surpasses those of entanglement, as stated in Ref. [47]. Consequently, a steering state is invariably entangled. Therefore, if a protocol for distilling steering is established, it will invariably result in the distillation of entanglement as well.

Corollary 5. The existence of the SD in the quantum network sharing the assemblage derived from the W state of the form (3) always indicates the existence of TED. Uncharacterized parties in the SD can be nonparticipating parties in TED. The number of participating parties can be reduced by putting constraints on the state parameters (equality of some state parameters).

The corollary holds because the number of nonparticipating parties in the entanglement scenario is equal to the number of uncharacterized parties in the steering scenario for the W state (3), i.e., $(P - Q = S)$.

Conclusion. In the proposed threshold distillation protocol, fewer parties are needed to achieve quantum distillation. For an imperfect GHZ state, only one party is sufficient to distill the perfect GHZ state among multiple parties and subsystems. This means steerable correlations are distillable in all steering scenarios, from 1SDI to $(P - 1)$ -sided device-independent $[(P - 1)\text{SDI}]$, where P is the number of parties [threshold steering distillation is possible up to $(P - 2)\text{SDI}$]. For an imperfect W state, at least $(P - 1)$ parties are needed to

distill the perfect W state shared among multiple parties. This implies that steerable correlations are distillable only in a 1SDI scenario. Threshold distillation is possible even for the mixed GHZ and W states. The proposed Krauss operators can be realized using tunable beam splitters and other linear optical elements [23]. Extensive toy examples in the Supplemental Material [44] support these findings. The threshold concept is

worth exploring for a broader range of states, communication scenarios, and cryptographic settings.

Acknowledgment. W.J.M. was supported in part by the JSPS KAKENHI Grant No. 21H04880.

Data availability. data that supports the findings of this article is available from the corresponding author upon reasonable requests.

-
- [1] Y. Desmedt, Threshold cryptography, *Encyclopedia of Cryptography and Security* (Springer, Boston, MA, 2011), pp. 1288–1293.
 - [2] A. Shamir, How to share a secret, *Commun. ACM* **22**, 612 (1979).
 - [3] A. De Santis, Y. Desmedt, Y. Frankel, and M. Yung, How to share a function securely, in *Proceedings of the 26th Annual ACM Symposium on Theory of Computing, STOC'94* (ACM Press, New York, 1994).
 - [4] D. Bogdanov, M. Niitsoo, T. Toft, and J. Willemson, High-performance secure multi-party computation for data mining applications, *Int. J. Inf. Secur.* **11**, 403 (2012).
 - [5] R. Cramer, I. B. Damgård, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing* (Cambridge University Press, Cambridge, 2015).
 - [6] D. Evans, V. Kolesnikov, and M. Rosulek, A pragmatic introduction to secure multi-party computation, *Found. Trends Privacy Secur.* **2**, 70 (2018).
 - [7] D. W. Archer, D. Bogdanov, Y. Lindell, L. Kamm, K. Nielsen, J. I. Pagter, N. P. Smart, and R. N. Wright, From keys to databases—Real-world applications of secure multi-party computation, *Comput. J.* **61**, 1749 (2018).
 - [8] L. Kamm, D. Bogdanov, E. Brito, and A. Ostrak, Blueprints for deploying privacy enhancing technologies in e-government, in *Privacy and Identity Management. Sharing in a Digital World*, edited by F. Bieker, S. de Conca, N. Gruschka, M. Jensen, and I. Schiering (Springer Nature, Switzerland, 2024), pp. 3–19.
 - [9] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum repeaters: The role of imperfect local operations in quantum communication, *Phys. Rev. Lett.* **81**, 5932 (1998).
 - [10] E. T. Campbell, M. G. Genoni, and J. Eisert, Continuous-variable entanglement distillation and noncommutative central limit theorems, *Phys. Rev. A* **87**, 042330 (2013).
 - [11] E. Y.-Z. Tan, C. C.-W. Lim, and R. Renner, Advantage distillation for device-independent quantum key distribution, *Phys. Rev. Lett.* **124**, 020502 (2020).
 - [12] N. Rengaswamy, N. Raveendran, A. Raina, and B. Vasić, Entanglement purification with quantum LDPC codes and iterative decoding, *Quantum* **8**, 1233 (2024).
 - [13] X.-Q. Sun, T. Nebabu, X. Han, M. O. Flynn, and X.-L. Qi, Entanglement features of random neural network quantum states, *Phys. Rev. B* **106**, 115138 (2022).
 - [14] H. Yan, Y. Zhong, H.-S. Chang, A. Bienfait, M.-H. Chou, C. R. Conner, E. Dumur, J. Grebel, R. G. Povey, and A. N. Cleland, Entanglement purification and protection in a superconducting quantum network, *Phys. Rev. Lett.* **128**, 080504 (2022).
 - [15] S. Wei, B. Jing, X. Zhang, J. Liao, C. Yuan, B. Fan, C. Lyu, D. Zhou, Y. Wang, G. Deng, H. Song, D. Oblak, G. Guo, and Q. Zhou, Towards real-world quantum networks: A review, *Laser Photonics Rev.* **16**, 2100219 (2022).
 - [16] J. Miguel-Ramiro, A. Pirker, and W. Dür, Optimized quantum networks, *Quantum* **7**, 919 (2023).
 - [17] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Concentrating partial entanglement by local operations, *Phys. Rev. A* **53**, 2046 (1996).
 - [18] 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).
 - [19] M. Horodecki, P. Horodecki, and R. Horodecki, Mixed-state entanglement and distillation: Is there a “bound” entanglement in nature? *Phys. Rev. Lett.* **80**, 5239 (1998).
 - [20] M. Horodecki, P. Horodecki, and R. Horodecki, General teleportation channel, singlet fraction, and quasidistillation, *Phys. Rev. A* **60**, 1888 (1999).
 - [21] P. Horodecki, M. Horodecki, and R. Horodecki, Bound entanglement can be activated, *Phys. Rev. Lett.* **82**, 1056 (1999).
 - [22] P. Horodecki and R. Horodecki, Distillation and bound entanglement, *Quantum Inf. Comput.* **1**, 45 (2001).
 - [23] R. V. Nery, M. M. Taddei, P. Sahium, S. P. Walborn, L. Aolita, and G. H. Aguilar, Distillation of quantum steering, *Phys. Rev. Lett.* **124**, 120402 (2020).
 - [24] Y. Liu, K. Zheng, H. Kang, D. Han, M. Wang, L. Zhang, X. Su, and K. Peng, Distillation of Gaussian Einstein-Podolsky-Rosen steering with noiseless linear amplification, *npj Quantum Inf.* **8**, 38 (2022).
 - [25] Z.-Y. Hao, Y. Wang, J.-K. Li, Y. Xiang, Q.-Y. He, Z.-H. Liu, M. Yang, K. Sun, J.-S. Xu, C.-F. Li, and G.-C. Guo, Filtering one-way Einstein-Podolsky-Rosen steering, *Phys. Rev. A* **109**, 022411 (2024).
 - [26] M. Forster, S. Winkler, and S. Wolf, Distilling nonlocality, *Phys. Rev. Lett.* **102**, 120401 (2009).
 - [27] M. Forster, Bounds for nonlocality distillation protocols, *Phys. Rev. A* **83**, 062114 (2011).
 - [28] P. Høyer and J. Rashid, Optimal protocols for nonlocality distillation, *Phys. Rev. A* **82**, 042118 (2010).
 - [29] N. Brunner, D. Cavalcanti, A. Salles, and P. Skrzypczyk, Bound nonlocality and activation, *Phys. Rev. Lett.* **106**, 020402 (2011).
 - [30] K.-S. Wu and L.-Y. Hsu, Hybrid nonlocality distillation, *Phys. Lett. A* **377**, 1323 (2013).
 - [31] P. Høyer and J. Rashid, Quantum nonlocal boxes exhibit stronger distillability, *Mod. Phys. Lett. A* **28**, 1330012 (2013).
 - [32] Y. Zhang and E. Chitambar, Exact steering bound for two-qubit Werner states, *Phys. Rev. Lett.* **132**, 250201 (2024).
 - [33] Y. Xiang, S. Cheng, Q. Gong, Z. Ficek, and Q. He, Quantum steering: Practical challenges and future directions, *PRX Quantum* **3**, 030102 (2022).

- [34] K.-Y. Lee, J.-D. Lin, A. Miranowicz, F. Nori, H.-Y. Ku, and Y.-N. Chen, Steering-enhanced quantum metrology using superpositions of noisy phase shifts, *Phys. Rev. Res.* **5**, 013103 (2023).
- [35] Y. Li, Y. Xiang, X.-D. Yu, H. C. Nguyen, O. Gühne, and Q. He, Randomness certification from multipartite quantum steering for arbitrary dimensional systems, *Phys. Rev. Lett.* **132**, 080201 (2024).
- [36] Y.-S. Huang, H.-B. Xing, M. Yang, Q. Yang, W. Song, and Z.-L. Cao, Distillation of multipartite entanglement by local filtering operations, *Phys. Rev. A* **89**, 062320 (2014).
- [37] B. Fortescue and H.-K. Lo, Random-party entanglement distillation in multiparty states, *Phys. Rev. A* **78**, 012348 (2008).
- [38] S. Gupta, D. Das, and A. S. Majumdar, Distillation of genuine tripartite Einstein-Podolsky-Rosen steering, *Phys. Rev. A* **104**, 022409 (2021).
- [39] L.-Y. Hsu and K.-S. Wu, Multipartite nonlocality distillation, *Phys. Rev. A* **82**, 052102 (2010).
- [40] X.-J. Ye, D.-L. Deng, and J.-L. Chen, Nonlocal distillation based on multisetting Bell inequality, *Phys. Rev. A* **86**, 062103 (2012).
- [41] H. Ebbe and S. Wolf, Distillation of multi-party non-locality with and without partial communication, *2013 IEEE International Symposium on Information Theory* (IEEE, New Jersey, 2013), pp. 739–743.
- [42] G.-Z. Pan, C. Li, M. Yang, G. Zhang, and Z.-L. Cao, Nonlocality distillation for high-dimensional correlated boxes, *Quantum Inf. Process.* **14**, 1321 (2015).
- [43] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, *Rev. Mod. Phys.* **86**, 419 (2014).
- [44] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/6zdc-j51g> for the proof of theorems and toy examples.
- [45] S. Designolle, V. Srivastav, R. Uola, N. H. Valencia, W. McCutcheon, M. Malik, and N. Brunner, Genuine high-dimensional quantum steering, *Phys. Rev. Lett.* **126**, 200404 (2021).
- [46] D. Martínez, E. S. Gómez, J. Cariñe, L. Pereira, A. Delgado, S. P. Walborn, A. Tavakoli, and G. Lima, Certification of a non-projective qudit measurement using multipoint beam splitters, *Nat. Phys.* **19**, 190 (2022).
- [47] S. J. Jones, H. M. Wiseman, and A. C. Doherty, Entanglement, Einstein-Podolsky-Rosen correlations, Bell nonlocality, and steering, *Phys. Rev. A* **76**, 052116 (2007).
- [48] C. Zhang, Y. Long, Z. Sun, Q. Li, and Q. Huang, Three-party quantum private computation of cardinalities of set intersection and union based on GHZ states, *Sci. Rep.* **10**, 22246 (2020).