

Highly-entangled, highly-doped states that are efficiently cross-device verifiable

Janek Denzler,¹ Santiago Varona²,[✉] Tommaso Guaita¹,[✉] and Jose Carrasco^{1,*}

¹*Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, 14195 Berlin, Germany*

²*Instituto de Física Teórica, UAM-CSIC, Universidad Autónoma de Madrid, Cantoblanco, 28049 Madrid, Spain*



(Received 28 January 2025; revised 7 April 2025; accepted 2 June 2025; published 27 June 2025)

In this paper, we introduce a class of highly entangled real quantum states that cannot be approximated by circuits with log-many non-Clifford gates and prove that Bell sampling enables efficient cross-device verification (or distributed inner product estimation) for these states. That is, two remote parties can estimate the inner product $\text{tr}(\rho\sigma)$, each having black-box access to copies of a state ρ (or respectively σ) in this class. This is significant because it is clear that this task can be achieved in those cases (such as low entanglement or low non-Clifford gate count) where one can independently learn efficient classical descriptions of each state using established techniques and share the description to compute the overlap. Instead, our results demonstrate that this is possible even in more complex scenarios where these “learn and share” methods are insufficient. Our proposal is scalable, as it just requires a number of two-copy Bell measurements and single-copy Pauli measurements that grows polynomially with both the number of qubits and the desired inverse error, and can be implemented in the near term. Moreover, the required number of samples can be efficiently experimentally determined by the parties in advance, and our findings are robust against preparation errors. We anticipate that these results could have applications in quantum cryptography and verification.

DOI: [10.1103/b6rb-yr6c](https://doi.org/10.1103/b6rb-yr6c)

I. INTRODUCTION

As quantum computing advances, ensuring the reliability of implemented quantum states remains a key challenge [1]. This includes verifying the similarity of states prepared across different devices. Standard benchmarking techniques, such as quantum-state tomography [2] and direct-fidelity estimation [3,4], rely on first classically learning and sharing state descriptions to then assess the states’ similarity. However, these “learn and share” methods are inherently limited to states that can be efficiently represented classically, such as those with low entanglement [5] or requiring only a few non-Clifford gates to prepare [6,7]. At the same time, other solutions based on interactive proofs and post-quantum cryptography (e.g., Refs. [8–10]) require resources that are far from being reached in the near future.

In this work, we explore how two parties can assess the similarity of their quantum states efficiently in practically relevant scenarios, without requiring to reveal an efficient description of their structure (see Fig. 1). This is also relevant outside the benchmarking field and for applications in a fault-tolerant setting. Indeed, it would allow secure quantum verification, where parties can confirm that they hold the same quantum state without revealing its content.

Cross-device verification [11–13] requires estimating the overlap between states prepared on different platforms. The Hadamard test enables this via quantum communication, and recent works [14–16] have also explored the prospect of inner-product estimation with limited quantum communication. While this is a valid strategy, it is often impractical, particularly for devices based on different technologies or located at distant places. Instead, doing this just by local measurements combined with classical communication (LOCC) leads to the problem of distributed inner-product estimation (DIPE). Existing DIPE methods, such as those based on randomized measurements and classical shadows, avoid explicit-state learning but face exponential complexity for generic states [11,17].

A promising alternative is cross-device verification via Pauli sampling [18], which also estimates this overlap without learning-state descriptions. Crucially, Pauli sampling tailors the measurement schedule to the input states, making it efficient for certain families of states, depending on properties of their Pauli distribution. We demonstrate that via Pauli sampling, DIPE is efficient in cases where traditional “learn and share” strategies fail. Specifically, we introduce a class of highly entangled, highly doped real quantum states that are inaccessible to classical learning techniques. Our findings show that LOCC-based DIPE is feasible even when tomography is impractical, enabling verification in challenging quantum computing scenarios. Therefore, our approach is a step towards confidential and efficient verification, allowing parties to estimate state overlaps without revealing enough information for reconstruction. This is a crucial advancement both for benchmarking applications and for the development of secure quantum communication and cryptographic protocols.

*Contact author: jose.carrasco@fu-berlin.de

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article’s title, journal citation, and DOI.

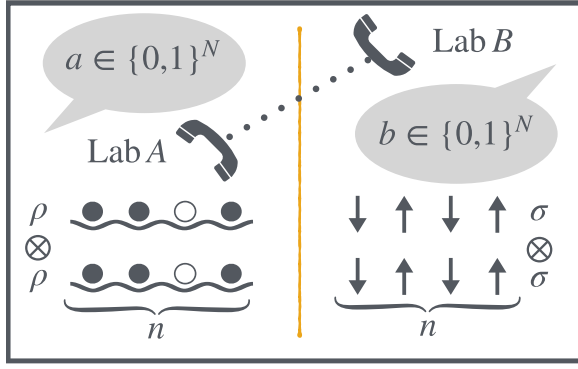


FIG. 1. Two distant quantum devices potentially operating on different platforms want to estimate the inner product $\text{tr}(\rho\sigma)$ using only LOCC. The parties exchange N bits of information a, b , which allows to construct an estimator for the inner product. The protocol is efficient if it is sufficient to choose N polynomial in the system size n . For low-entangled or low-doping states, a, b can be just compact classical descriptions that allow the reconstruction of ρ, σ . In this work we ask: is it possible to do efficient cross-device verification for states without sharing classical descriptions, i.e., with highly entangled and highly doped states?

One limitation is that our method requires states to be real. However, we show that it remains effective under realistic noise conditions: if a state is close to a real target-pure state in trace norm, the protocol still yields accurate overlap estimates. This robustness ensures practicality despite experimental imperfections, such as small nonreal gate errors. Additionally, for near-pure real states, remote parties can predict the number of samples needed to achieve a desired accuracy, enabling efficient and reliable verification. In conclusion, our work bridges the gap between efficiency and confidentiality in cross-device verification, providing a scalable solution for efficient and secure quantum-state validation in both near-term and fault-tolerant quantum technologies.

II. THE rDIPE ALGORITHM AND ITS COMPLEXITY

In Ref. [18], an algorithm for the distributed estimation of the inner product $\text{tr}(\rho\sigma)$ between two pure quantum states was introduced, which only relies on performing one- and two-copy measurements of either state. We use a version of this algorithm that also works for mixed states, assuming that $\text{tr}\rho^2, \text{tr}\sigma^2 > 1/2$. For completeness we provide it in Appendix A (see Algorithm 1).

In order to properly discuss the protocol's efficiency, let us introduce some notation. Given a quantum state ρ , we denote its Pauli distribution by p_ρ and its Bell distribution by q_ρ . That is

$$p_\rho(\mathbf{a}) = \frac{\langle P_{\mathbf{a}} \rangle_\rho^2}{2^n \text{tr} \rho^2}, \quad q_\rho(\mathbf{a}) = \langle \Phi_{\mathbf{a}} | \rho \otimes \rho | \Phi_{\mathbf{a}} \rangle,$$

for $\mathbf{a} \in \{0, 1, 2, 3\}^n$, where $P_{\mathbf{a}} = P_{a_1} \otimes \dots \otimes P_{a_n}$ are n -qubit Pauli operators and $|\Phi_{\mathbf{a}}\rangle = (\mathbb{I} \otimes P_{\mathbf{a}})|\Phi_0\rangle$ are the Bell states, with $|\Phi_0\rangle = 1/\sqrt{2^n} \sum_{z \in \{0,1\}^n} |z_1, \dots, z_n\rangle \otimes |z_1, \dots, z_n\rangle$. Notice that if ρ is pure and has real amplitudes then $p_\rho = q_\rho$ [19]. Then, we denote by F_ρ the cumulative-distribution function (CDF) of the random variable $\langle P_{\mathbf{a}} \rangle_\rho^2$ when $\mathbf{a}$ is sampled

according to p_ρ , that is

$$F_\rho(\epsilon) = \sum_{\mathbf{a}} p_\rho(\mathbf{a}) \theta(\epsilon - \langle P_{\mathbf{a}} \rangle_\rho^2), \quad (1)$$

where $\theta(t)$ is the indicator function for the set $\{t \geq 0\}$. Finally, we will consider sequences of states indexed by the number of qubits and denote these as $\{\rho\} \equiv \{\rho_n\}_n$.

The protocol rDIPE, presented in detail in Appendix A, outputs an approximation $f(\rho, \sigma, N_1, N_2)$ of the quantity

$$c(\rho, \sigma) := \text{tr}(\rho\sigma) / \sqrt{\text{tr} \rho^2 \text{tr} \sigma^2}, \quad (2)$$

computed by using N_1 copies of $\rho^{\otimes 2}$ and $\sigma^{\otimes 2}$ and $N_1 N_2$ copies of ρ and σ (see Algorithm 1 in Appendix A for a precise definition of this estimator f). In other words, it evaluates the cosine of the angle between ρ and σ , as determined by the inner product $\text{tr}(\rho\sigma)$. We say that rDIPE is efficient on inputs $\{\rho\}, \{\sigma\}$ if the following holds [20]:

Definition 1 (Efficiency of rDIPE). For two sequences $\{\rho\}, \{\sigma\}$, we say that rDIPE is efficient on inputs $\{\rho\}, \{\sigma\}$ if there exist integers $N_1, N_2 = \text{poly}(n, 1/\epsilon, \delta)$ such that for all $n, \epsilon, \delta > 0$

$$\mathbb{P}[|f(\rho_n, \sigma_n, N_1, N_2) - c(\rho_n, \sigma_n)| > \epsilon] < e^{-\delta}. \quad (3)$$

In order to make statements about the efficiency of rDIPE on specific states, we will use a technical result proven in Ref. [18] which expresses how well the quantity $c(\rho, \sigma)$ of Eq. (2) can be approximated by the output $f(\rho, \sigma, N_1, N_2)$ of the protocol, by relating this to properties of the states' CDFs and Bell distributions. The proof of this statement applies with minor modifications also to our case of mixed states, showing that for any $\epsilon_1 > 0$ and $\epsilon_2 > 0$

$$\begin{aligned} \mathbb{P}[|f(\rho, \sigma, N_1, N_2) - c(\rho, \sigma)| > 4\epsilon_1 + 4\sqrt{\epsilon_2} + 2F(\epsilon_2) + 6\Delta] \\ < 4 \exp(-2\epsilon_1^2 N_1) + 4N_1 \exp(-\epsilon_2^2 N_2/2), \end{aligned} \quad (4)$$

where $F = (F_\rho + F_\sigma)/2$ and Δ expresses the total variation (TV) distance between the Pauli distribution $p_{\text{mix}} = (p_\rho + p_\sigma)/2$ and the Bell distribution $q_{\text{mix}} = (q_\rho + q_\sigma)/2$, that is $\Delta = \text{TV}(p_{\text{mix}}, q_{\text{mix}})$.

III. THE CW FAMILY OF STATES

We now present our main results. That is, we introduce the following class of states, for which rDIPE is efficient, that are, however, not efficiently learnable with MPS or stabilizer-based methods. In the following, we will denote by $\text{rCl}(n)$ the real Clifford group on n qubits (see Ref. [21] for a detailed definition and summary of main properties).

Definition 2. Let $n > 0$ denote the number of qubits. We define the class $\text{CW}(n)$ as the family of states of the form $C|W_n\rangle$, where C is a real Clifford unitary on n qubits, and $|W_n\rangle$ is the n -qubit W state. Specifically,

$$\text{CW}(n) = \{|\psi\rangle : |\psi\rangle = C|W_n\rangle, C \in \text{rCl}(n)\},$$

where $|W_n\rangle = \sum_{|z|=1} c_z |z_1, \dots, z_n\rangle$ with $c_z = 1/\sqrt{n}$, and the sum extends over all $z \in \{0, 1\}^n$ such that $\sum_i z_i = 1$.

It is worth noting that our results are also valid if we replace the W state of the previous definition by a Dicke state with a constant number of excitations, or by any other nonpermutationally invariant superposition of computational basis states

with constant Hamming weight like, e.g., those of Ref. [22]. More generally, the same is true for states of the form $C \sum_{z \in S} c_z |z_1, \dots, z_n\rangle$, where C is a (highly entangling) real Clifford gate, and we take, for instance, $c_z \propto \pm 1/\sqrt{\text{poly}(n)}$ for possibly different polynomials and the sum $z \in S$ running over any $S \subset \{0, 1\}^n$ with cardinality $|S| = \text{poly}(n)$. However, for the purposes of this work, we shall favor the simplicity of Definition 2.

In the following, when dealing with sequences of states we will write $\{\rho\} \in \text{CW}$ if $\rho_n \in \text{CW}(n)$ for all n . First of all, we observe that rDIPE is efficient on inputs in CW.

Proposition 1. For all inputs $\{\rho\}, \{\sigma\} \in \text{CW}$, rDIPE is efficient in the sense of Definition 1.

Proof. To see this, for all $n, \epsilon > 0$ consider ϵ_1, ϵ_2 given by $\epsilon_1 = \epsilon/8$ and $\epsilon_2 = \min\{(\epsilon/8)^2, 3/n^2\}$. The main property of the states in CW that we will use here is that their CDF $F(\epsilon)$ vanishes when ϵ is inverse-polynomially small. This is proven in Appendix C [see specifically Eq. (C6)]. In particular, this fact allows us to conclude that $F_{\rho_n}(\epsilon_2) = F_{\sigma_n}(\epsilon_2) = 0$, since $\epsilon_2 \leq 3/n^2 < 4/n^2$.

It follows that $4\epsilon_1 + 4\sqrt{\epsilon_2} + 2F(\epsilon_2) \leq \epsilon$, which in turn implies

$$\begin{aligned} \mathbb{P}\{|f(\rho_n, \sigma_n, N_1, N_2) - c(\rho_n, \sigma_n)| > \epsilon\} \\ \leq \mathbb{P}\{|f(\rho_n, \sigma_n, N_1, N_2) - c(\rho_n, \sigma_n)| > 4\epsilon_1 + 4\sqrt{\epsilon_2} \\ + 2F(\epsilon_2)\} < 4 \exp(-2\epsilon_1^2 N_1) + 4N_1 \exp(-\epsilon_2^2 N_2/2), \end{aligned} \quad (5)$$

where in the last step we have used Eq. (4), considering that ρ_n, σ_n have real amplitudes which implies $\Delta = 0$. This shows that there are $N_1, N_2 = \text{poly}(n, 1/\epsilon, \delta)$ such that Eq. (3) holds for $\{\rho\}, \{\sigma\} \in \text{CW}$. ■

Next, we show that the class CW contains highly entangled states that cannot be efficiently approximated by matrix product states (MPS). This is summarized by the following proposition:

Proposition 2. There exists at least one family of states $\{\rho\} \in \text{CW}$ such that

$$S_2(\text{tr}_{n/2} \rho_n) \geq cn, \quad (6)$$

for some constant c . Here, $\text{tr}_{n/2} \rho_n$ is the reduced state obtained by tracing out the first half of the system's qubits and S_2 is the second Rényi entropy. According to well-known results (see, for example, Ref. [5]), this implies that $\{\rho\}$ cannot be approximated to arbitrary precision by a family of MPS with bond-dimension polynomial in n .

Proof. To prove this statement, we first show that the average entanglement entropy of the states in the class $\text{CW}(n)$ grows linearly in n , in particular

$$\mathbb{E}[S_2(\text{tr}_{n/2} C|W_n\rangle\langle W_n|C^\dagger)] \geq cn. \quad (7)$$

Here, $\mathbb{E}$ denotes the average over the unitary C according to the Haar measure of the real Clifford group $\text{rCl}(n)$.

To see this, notice that using standard techniques we can rewrite the left-hand side of the expression above as

$$\begin{aligned} \mathbb{E}[-\log \text{tr}(\text{SWAP}_{n/2} (C|W_n\rangle\langle W_n|C^\dagger)^{\otimes 2})] \\ \geq -\log \text{tr}[\text{SWAP}_{n/2} \mathbb{E}(C^{\otimes 2}(|W_n\rangle\langle W_n|)^{\otimes 2}(C^\dagger)^{\otimes 2})] \\ \geq -\log \text{tr}\left[\text{SWAP}_{n/2} \frac{1}{2^{2n}}(k P_{\text{sym}} + 2^{n-k'}|\Phi_0\rangle\langle\Phi_0|)\right], \end{aligned} \quad (8)$$

where $\text{SWAP}_{n/2}$ is the operator that swaps the first $n/2$ qubits of the first factor of the tensor product with the first $n/2$ qubits of the second factor. In the last step we have used Haar integration techniques to evaluate the average value of the quantity involving $C^{\otimes 2}$, using that the real Clifford group is an orthogonal 2-design [21]. More details on this calculation are presented in Appendix B (see Theorem B1, Lemma B1, and following discussion). In particular, we have that $P_{\text{sym}} = (\mathbb{I} + \text{SWAP}_n)/2$ and k, k' are constants. Here, SWAP_n swaps the entire first factor of the tensor product with the second. By straightforward computation we find $\text{tr}(\text{SWAP}_{n/2} P_{\text{sym}}) = 2^{3n/2}$ and $\text{tr}(\text{SWAP}_{n/2} |\Phi_0\rangle\langle\Phi_0|) = 1$, which implies that Eq. (8) is equal to $-\log(k 2^{-n/2} + k' 2^{-n}) \geq cn$.

Since, according to Eq. (7), the states' $\text{CW}(n)$ on average have an entanglement entropy of at least cn , there must exist at least one state in $\text{CW}(n)$ whose entanglement entropy is larger or equal to this average value. By setting ρ_n equal to such state for all n , we construct a family $\{\rho\}$ that satisfies Eq. (6). ■

A final property of the states in $\text{CW}(n)$ is that they cannot be approximated by quantum circuits with just few non-Clifford gates. Precisely, states prepared by Clifford circuits supplemented by at most tT gates (known in the literature as t -doped states [6,7]) can only be good approximations to states in $\text{CW}(n)$ if t grows linearly in n . This is summarized in the following proposition [23]:

Proposition 3. Let ρ' be a t -doped state on n qubits. If $\|\rho - \rho'\|_{\text{tr}} < 1/4$ for some $\rho \in \text{CW}(n)$, then $t > n/4$.

Proof. We show the contrapositive: t -doped states with $t \leq n/4$ are at least $1/4$ far in trace distance from $\text{CW}(n)$. A simple counting argument suffices: on the one hand, arbitrary t -doped states ρ' on n qubits have at least 2^{n-t} stabilizers, as the application of a single T gate reduces the number of stabilizer generators by at most one [6]. On the other hand, we can upper bound the number of Paulis with high expectation value for states ρ in $\text{CW}(n)$, as we discuss in Appendix C. Concretely, for $t \leq n/4$, we find that

$$\begin{aligned} |\{\mathbf{a} : |\langle P_{\mathbf{a}} \rangle_\rho| > 3/4\}| &< 2^{3n/4}, \\ |\{\mathbf{a} : |\langle P_{\mathbf{a}} \rangle_{\rho'}| = 1\}| &\geq 2^{n-t} \geq 2^{3n/4}, \end{aligned}$$

where we have used bound Eq. (C8) in Appendix C to obtain the first inequality. Therefore, there exists at least one Pauli operator P with $|\langle P \rangle_\rho - \langle P \rangle_{\rho'}| \geq 1/4$, and thus $\|\rho - \rho'\|_{\text{tr}} \geq 1/4$, as claimed. ■

We have constructed a (generalizable) class of states denoted CW, see Definition 2. Proposition 2 shows that this class contains sequences of highly-entangled states, for which MPS learning algorithms are known to fail [5]. In fact, as a consequence of Markov's inequality, a large fraction of sequences will have this property. Furthermore, due to Proposition 3, the states in CW cannot be well approximated by $(\log n)$ -doped states, for which efficient learning algorithms also exist [6,7]. Nonetheless, Algorithm 1 is efficient on states in CW, as specified by Proposition 1.

IV. ROBUSTNESS

In any realistic experimental setting, state preparation is subject to noise. Even if the protocol rDIPE is efficient on

inputs $\{\rho\}, \{\sigma\}$, it is *a priori* unclear how the protocol will behave on noisy inputs $\{\rho'\}, \{\sigma'\}$. In particular, we want that small state-preparation errors still allow for efficiently estimating $\text{tr}(\rho'\sigma')$, rendering the protocol practically meaningful. This is complicated by the fact that general noise channels will not preserve the realness of our target states, even if these are ideally prepared by real gates only [24,25]. Note here that an arbitrary noise channel can always be mapped to a realness-preserving Pauli channel by randomized compilation [26], even though our proposal does not rely on this technique. However, independently of this, in Appendix D we show that rDIPE is robust on inputs $\{\rho\}, \{\sigma\} \in \text{CW}$, in the following precise sense.

Given two sequences $\{\rho\}, \{\sigma\} \in \text{CW}$, there exists $k > 0$ and integers $N_1, N_2 = \text{poly}(n, 1/\tau, \delta)$ such that for all $n, \tau, \delta > 0$

$$\mathbb{P}\{|f(\rho'_n, \sigma'_n, N_1, N_2) - c(\rho'_n, \sigma'_n)| > k\tau\} < e^{-\delta}, \quad (9)$$

for all other sequences $\{\rho'\}, \{\sigma'\}$ such that $\sup_n \|\rho_n - \rho'_n\|_{\text{tr}} \leq \tau$ and analogously for σ . That is, even if we run rDIPE on not necessarily real inputs $\{\rho'\}, \{\sigma'\}$ that are within trace norm τ of the real pure states $\{\rho\}, \{\sigma\} \in \text{CW}$, where the protocol is efficient, we are still able to estimate the quantity $c(\rho', \sigma')$ of Eq. (2) with polynomial resources, but up to an error linear in τ .

To round off this section on the robustness of our protocol, let us note that the practical impossibility of preparing two exact copies $\rho \otimes \rho$ or $\sigma \otimes \sigma$ for Bell sampling can be treated in an analogous way. Indeed, any possibly entangled state $\tilde{\rho}$ with $\|\tilde{\rho} - \rho \otimes \rho\| < \tau$ allows for sampling from q_ρ , up to an error at most τ in TV distance.

V. ESTIMATION OF REQUIRED RESOURCES

A further appealing aspect of the presented protocol is that, given arbitrary real states (not necessarily known to be efficient), the remote parties can experimentally determine the number of samples required for distributed inner-product estimation as follows: First, collect N samples $\{\mathbf{a}_1, \dots, \mathbf{a}_N\}$ from the Pauli distribution of the n -qubit pure state ρ . This can be achieved by measuring in the Bell basis, as for real states $q_\rho(\mathbf{a}) = p_\rho(\mathbf{a})$. Then, for each sample, construct an estimate of $\langle P_{\mathbf{a}_i} \rangle_\rho^2$ using K further measurements. Let us call this estimate $\alpha_i^2(K)$. Consider now the previously introduced CDF Eq. (1) and its empirical estimator

$$F_{\rho, N, K}(x) = \frac{1}{N} \sum_{i=1}^N \theta(x - \alpha_i^2(K)). \quad (10)$$

Using the Dvoretzky–Kiefer–Wolfowitz [27,28] and Hoeffding inequalities, one can show that there are $N = \text{poly}(\delta, 1/\epsilon)$ and $K = \text{poly}(\delta, 1/x, \log(1/\epsilon))$ such that, if $F_{\rho, N, K}(2x) \leq \epsilon/2$ then

$$\mathbb{P}(F_\rho(x) > \epsilon) < e^{-\delta}.$$

This means that, by looking at $F_{\rho, N, K}$ with this choice of N, K , we can find a sufficiently small ϵ_2 such that with high probability $2F_\rho(\epsilon_2) + 4\sqrt{\epsilon_2} \leq \epsilon/2$. Consider now ϵ_2 as a function of $n, 1/\epsilon$. Then, similarly to Eq. (5), it follows that if $1/\epsilon_2 = \text{poly}(n, 1/\epsilon)$ the protocol is efficient. One can see that this is equivalent to the solution of $F_{\rho, N, K}(x) = \epsilon$ being

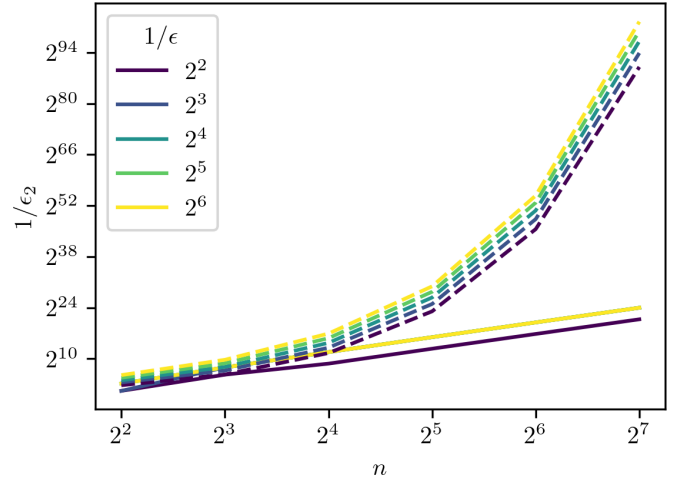


FIG. 2. Here we plot $1/\epsilon_2$ in terms of n for different values of $1/\epsilon$ and for two families of states where the protocol is efficient (solid) and inefficient (dashed). To illustrate the measurement protocol we consider states that have an efficient MPS representation and thus can be simulated, however the same behavior of the solid lines is also expected for other families of states with extensive entanglement entropy (see Definition 2, the remark afterwards, and Proposition 2). Precisely, we compute ϵ_2 as the solution of $F_{\rho, N, K}(\epsilon_2) = \epsilon$ [see discussion after Eq. (10)]. The solid lines correspond to the Dicke state with two excitations, whereas the dashed ones correspond to a translationally invariant random MPS of bond dimension 2 where the entries of each tensor are independent, identically distributed (iid) according to the standard normal distribution. We take $N = 5 \times 10^4$ and K effectively infinite (as for MPS $\langle P \rangle_\rho^2$ can be computed exactly).

$x = 1/\text{poly}(n, 1/\epsilon)$. We illustrate this approach in Fig. 2 for two different families of states.

VI. CONCLUSIONS

In our work, we construct explicit examples of states without compact-classical description (in the form of MPS or t -doped states) for which the distributed estimation of inner products is efficient via Pauli sampling. We would like to finish by commenting on the practical utility of our work and its limitations.

For our proposal to be implemented, each party needs to be able to approximately prepare a two-copy pure (and real) quantum state, a theoretical primitive that has been shown to be of interest in different contexts (see, e.g., Ref. [29] and references therein). We stress that each such two-copy state has to be prepared within the same laboratory, something that has actually been demonstrated in practice in different settings like photonic systems [30], trapped-ions [31], or atomic arrays [32,33], and even for logical quantum states [34]. Nonetheless, it is admittedly true that being able to prepare such a high-purity, two-copy state is experimentally challenging and already indicates a high quality of the quantum devices involved. However, we think that our proposal can still be practically useful in scenarios where the parties use different quantum implementations, or they cannot natively implement the same gate sets. For instance, our proposal can be used to efficiently check whether two sequences of different apparatus

do indeed produce similar wave functions (even if an efficient description of the underlying wave function is not available).

Our results further show that the amount of classical information that needs to be exchanged to estimate the inner product between certain quantum states via LOCC can be smaller than the amount of information needed to characterize the quantum states themselves. While our work primarily serves as a proof of concept, we hope that further investigation may generalize these findings to a broader class of states, potentially unlocking new applications in quantum cryptography and verification.

ACKNOWLEDGMENTS

We would like to thank R. Ruiz for pointing out Ref. [22] and useful discussions. T.G. was supported by the German Federal Ministry for Education and Research (BMBF) under the project FermiQP. J.C. acknowledges financial support from BerlinQuantum, BMBF (DAQC, MUNIQ-Atoms), and the project Munich Quantum Valley (K8). J.D. acknowledges financial support from BMBF (DAQC). S.V. acknowledges support from Grant No. PID2021-127726NB-I00 (MCIU/AEI/FEDER, UE), from the Grant IFT Centro de Excelencia Severo Ochoa CEX2020-001007-S, funded by Grant No. MCIN/AEI/10.13039/501100011033, and from the CSIC Research Platform on Quantum Technologies PTI-001.

DATA AVAILABILITY

To reproduce Fig. 2 one can use any standard technique to sample from the output distribution of MPS states, like for instance TenPy [35]. The particular implementation used in this work can be shared upon request.

APPENDIX A: THE rDIPE ALGORITHM

The protocol for real distributed inner-product estimation (rDIPE) which we analyze in this work is a particular instance of the so-called symmetric protocol of Ref. [18], adapted to mixed states with $\text{tr } \rho^2, \text{tr } \sigma^2 > 1/2$. It can be summarized as follows:

ALGORITHM 1. rDIPE

Input: N_1 copies of the unknown states $\rho \otimes \rho$ and $\sigma \otimes \sigma$, and $N_1 N_2$ copies of the states ρ and σ .

Output: $f(\rho, \sigma, N_1, N_2)$, an estimate of $c(\rho, \sigma)$.

- 1: Alice and Bob sample N_1 times from the distribution $q_{\text{mix}} = (q_\rho + q_\sigma)/2$ to obtain $\{\mathbf{a}_1, \dots, \mathbf{a}_{N_1}\}$. That is, each $\mathbf{a}_i$ is the outcome of a Bell measurement in either $\rho \otimes \rho$ or $\sigma \otimes \sigma$ with equal probability.
- 2: **for all** $i \in \{1, 2, \dots, N_1\}$ **do**
- 3: **Alice:** using N_2 single-copy measurements, construct $\alpha_i(N_2)$, an estimate of the expectation value $\langle P_{\mathbf{a}_i} \rangle_\rho$.
- 4: **Bob:** using N_2 single-copy measurements, construct $\beta_i(N_2)$, an estimate of the expectation value $\langle P_{\mathbf{a}_i} \rangle_\sigma$.
- 5: **end for**
- 6: **Return**

$$f(\rho, \sigma, N_1, N_2) = \frac{1}{N_1} \sum_{i=1}^{N_1} \frac{2[\alpha_i(N_2)][\beta_i(N_2)]}{[\alpha_i(N_2)]^2 \sqrt{B/A} + [\beta_i(N_2)]^2 \sqrt{A/B}},$$

where A and B are estimates of $\text{tr } \rho^2$ and $\text{tr } \sigma^2$.

In this work, to simplify derivations, we assume that A and B are exactly equal to the purities $\text{tr } \rho^2, \text{tr } \sigma^2$. In practice, one would need to estimate them using N_3 additional measurement shots. This will lead to a further error term on the final inner-product estimation, which can, however, be bounded with similar techniques to the other terms and can be made arbitrarily small by choosing a suitable N_3 .

APPENDIX B: ON HAAR INTEGRATION OVER THE REAL CLIFFORD SUBGROUP

Here we provide the details omitted in the proof of Proposition 2. To evaluate twirls with respect to the real Clifford subgroup, we make use of the following well-known result (see Ref. [36] and references therein for a recent review on related techniques):

Theorem B1 (Commutant theorem). Let G be a compact group with Haar measure μ_G and $\{U(g)\}_{g \in G}$ a (finite-dimensional) unitary representation of G on $(\mathcal{H}, \langle \cdot, \cdot \rangle)$. The k -fold twirl

$$\Phi_G^k : X \mapsto \int_G U(g)^{\otimes k} X U(g)^{\dagger \otimes k} d\mu_G(g)$$

is an orthogonal projector (with respect to the Hilbert-Schmidt inner product) onto the commutant of $\{U(g)^{\otimes k}\}_{g \in G}$.

As the real Clifford group rCl is an orthogonal 2-design [21], the expectation value appearing in Eqs. (7) and (8) in the proof of Proposition 2 coincides with a twofold twirl over the orthogonal group $G = O(2^n)$. To use the previous Theorem, we need the following characterization of the commutant of $O(2^n) \otimes O(2^n)$ (see Ref. [37] for details):

Lemma B1. An orthonormal basis of the commutant of $O(2^n) \otimes O(2^n)$, with respect to the Hilbert-Schmidt inner product, is given by

$$\frac{1}{d_{\text{sym}}^{1/2}} P_{\text{sym}} = \frac{1}{2 d_{\text{sym}}^{1/2}} (\mathbb{I} + \text{SWAP}_n),$$

$$\frac{1}{d_{\text{asym}}^{1/2}} P_{\text{asym}} = \frac{1}{2 d_{\text{asym}}^{1/2}} (\mathbb{I} - \text{SWAP}_n),$$

$$\bar{B} = \frac{1}{(1 - 1/d_{\text{sym}})^{1/2}} \left(|\Phi_0\rangle\langle\Phi_0| - \frac{1}{d_{\text{sym}}} P_{\text{sym}} \right),$$

where P_{sym} and P_{asym} are projectors onto the symmetric and antisymmetric subspaces with dimensions d_{sym} and d_{asym} , respectively.

To complete the chain of inequalities [Eq. (8)] in the proof of Proposition 2, we project $|W_n\rangle\langle W_n|^{\otimes 2}$ onto each orthogonal component separately. Due to swap invariance, the projection onto P_{asym} vanishes, leaving us with a linear combination of P_{sym} and $|\Phi_0\rangle\langle\Phi_0|$. Note that $d_{\text{sym}} = 2^n(2^n + 1)/2$.

APPENDIX C: CDF OF STATES IN CW

In this section, we prove several properties of the CDF of states in CW, which we use throughout the Letter. They allow us to complete the proof of Proposition 3 and analyze the efficiency and robustness of our protocol. We start with two Lemmas on the continuity of Pauli distributions and the

corresponding CDFs that will be needed for the following discussion.

Lemma C1. Let ρ, σ be quantum states with Pauli distributions p_ρ, p_σ . Then,

$$\sum_{\mathbf{a}} |(\text{tr } \rho^2) p_\rho(\mathbf{a}) - (\text{tr } \sigma^2) p_\sigma(\mathbf{a})| \leq 2 \|\rho - \sigma\|_{\text{tr}}, \quad (\text{C1})$$

$$\max\{\text{tr } \rho^2, \text{tr } \sigma^2\} \text{TV}(p_\rho, p_\sigma) \leq 2 \|\rho - \sigma\|_{\text{tr}}. \quad (\text{C2})$$

Proof. We start by proving Eq. (C1). To this end, we will use the identity $\sum_{\mathbf{a}} \langle P_{\mathbf{a}} \rangle_A^2 = 2^n \text{tr } A^2$, where A is any Hermitian n -qubit operator. We upper bound

$$\begin{aligned} \sum_{\mathbf{a}} |\langle P_{\mathbf{a}} \rangle_\rho^2 - \langle P_{\mathbf{a}} \rangle_\sigma^2| &= \sum_{\mathbf{a}} |\langle P_{\mathbf{a}} \rangle_{\rho+\sigma}| \cdot |\langle P_{\mathbf{a}} \rangle_{\rho-\sigma}| \\ &\leq \sqrt{\sum_{\mathbf{a}} \langle P_{\mathbf{a}} \rangle_{\rho+\sigma}^2} \cdot \sqrt{\sum_{\mathbf{b}} \langle P_{\mathbf{b}} \rangle_{\rho-\sigma}^2} \\ &= 2^n \sqrt{\text{tr}(\rho + \sigma)^2} \cdot \sqrt{\text{tr}(\rho - \sigma)^2} \\ &\leq 2 \cdot 2^n \|\rho - \sigma\|_{\text{tr}}, \end{aligned}$$

where we have used the Cauchy-Schwarz and Hölder inequalities. Noting that $(\text{tr } \rho^2) p_\rho(\mathbf{a}) = \langle P_{\mathbf{a}} \rangle_\rho^2 / 2^n$, this shows Eq. (C1) from which follows Eq. (C2) after applying the triangle inequality. Indeed, assume without loss of generality that $\text{tr } \rho^2 \geq \text{tr } \sigma^2$, and write

$$\begin{aligned} \text{TV}(p_\rho, p_\sigma) &\leq \frac{1}{2} \sum_{\mathbf{a}} \frac{|(\text{tr } \rho^2) p_\rho(\mathbf{a}) - (\text{tr } \sigma^2) p_\sigma(\mathbf{a})|}{\text{tr } \rho^2} \\ &\quad + \frac{1}{2} \sum_{\mathbf{a}} \frac{|(\text{tr } \sigma^2) p_\sigma(\mathbf{a}) - (\text{tr } \rho^2) p_\sigma(\mathbf{a})|}{\text{tr } \rho^2}. \end{aligned}$$

Using Eq. (C1) to bound the first term of the previous inequality, and using the fact that $|\text{tr } \rho^2 - \text{tr } \sigma^2| \leq 2 \|\rho - \sigma\|_{\text{tr}}$, Eq. (C2) follows. ■

Lemma C2. Let ρ, ρ' be quantum states with CDFs $F_\rho, F_{\rho'}$. Then, for all ϵ

$$F_{\rho'}(\epsilon) \leq F_\rho(2\epsilon) + \frac{4\|\rho - \rho'\|_{\text{tr}}}{\text{tr } \rho'^2}.$$

Proof. We consider the following subsets of Pauli strings:

$$\mathcal{A} = \{\mathbf{a} : \langle P_{\mathbf{a}} \rangle_{\rho'}^2 \leq \epsilon\},$$

$$\mathcal{B} = \{\mathbf{a} : \langle P_{\mathbf{a}} \rangle_\rho^2 \leq 2\epsilon\}.$$

We further write $F_{\rho'}(\epsilon) = \sum_{\mathbf{a} \in \mathcal{A}} p_{\rho'}(\mathbf{a})$, and split the sum into two parts:

$$F_{\rho'}(\epsilon) = \sum_{\mathbf{a} \in \mathcal{A} \cap \mathcal{B}} p_{\rho'}(\mathbf{a}) + \sum_{\mathbf{a} \in \mathcal{A} \cap \bar{\mathcal{B}}} p_{\rho'}(\mathbf{a}), \quad (\text{C3})$$

where $\bar{\mathcal{B}}$ is the complement of $\mathcal{B}$. Next, we upper bound both contributions separately. For one,

$$\sum_{\mathbf{a} \in \mathcal{A} \cap \mathcal{B}} p_{\rho'}(\mathbf{a}) \leq \sum_{\mathbf{a} \in \mathcal{B}} p_{\rho'}(\mathbf{a}) \leq F_\rho(2\epsilon) + \text{TV}(p_\rho, p_{\rho'}), \quad (\text{C4})$$

by the definition of the TV distance. Secondly,

$$\begin{aligned} \sum_{\mathbf{a} \in \mathcal{A} \cap \bar{\mathcal{B}}} p_{\rho'}(\mathbf{a}) &\leq \sum_{\mathbf{a} \in \mathcal{A} \cap \bar{\mathcal{B}}} \frac{\langle P_{\mathbf{a}} \rangle_\rho^2 - \langle P_{\mathbf{a}} \rangle_{\rho'}^2}{2^n \text{tr } \rho'^2} \\ &= \sum_{\mathbf{a} \in \mathcal{A} \cap \bar{\mathcal{B}}} \frac{(\text{tr } \rho^2) p_\rho(\mathbf{a}) - (\text{tr } \rho'^2) p_{\rho'}(\mathbf{a})}{\text{tr } \rho'^2}, \end{aligned} \quad (\text{C5})$$

since $\langle P_{\mathbf{a}} \rangle_\rho^2 \geq 2 \langle P_{\mathbf{a}} \rangle_{\rho'}^2$ whenever $\mathbf{a} \in \mathcal{A} \cap \bar{\mathcal{B}}$. The statement follows by using Eqs. (C2) and (C1) to upper bound Eqs. (C4) and (C5), respectively, and substituting into Eq. (C3). ■

Let us now discuss the CDF of states in CW. Since the CDF is invariant under Cliffords, it suffices to consider the states $|W_n\rangle$ of Definition 2. A simple calculation yields the following Pauli expectation values:

$$\langle W_n | P_{\mathbf{a}} | W_n \rangle = \begin{cases} 1 - \frac{2z_{\mathbf{a}}}{n}, & (x_{\mathbf{a}}, y_{\mathbf{a}}) = (0, 0) \\ \frac{2}{n}, & (x_{\mathbf{a}}, y_{\mathbf{a}}) \in \{(2, 0), (0, 2)\} \\ 0, & \text{otherwise} \end{cases}$$

where $x_{\mathbf{a}} = |\{i : P_{a_i} = X\}|$ counts the number of tensor factors X in $P_{\mathbf{a}} = P_{a_1} \otimes \cdots \otimes P_{a_n}$, and similarly for $y_{\mathbf{a}}$ and $z_{\mathbf{a}}$. In particular,

$$F_\rho(\epsilon) = 0, \quad (\text{C6})$$

for $\epsilon < 4/n^2$ and $\rho \in \text{CW}(n)$. Furthermore, for some $\rho \in \text{CW}(n)$ and for arbitrary ρ' with $\|\rho - \rho'\|_{\text{tr}} \leq 1/10$, Lemma C2 and Eq. (C6) imply that for $\epsilon < 2/n^2$

$$F_{\rho'}(\epsilon) \leq \frac{4\|\rho - \rho'\|_{\text{tr}}}{1 - 2\|\rho - \rho'\|_{\text{tr}}} \leq 5\|\rho - \rho'\|_{\text{tr}}. \quad (\text{C7})$$

Lastly, an upper bound on the number of Pauli strings $P_{\mathbf{a}}$ with $|\langle P_{\mathbf{a}} \rangle_\rho| > 3/4$ for $\rho \in \text{CW}(n)$ will be useful in the proof of Proposition 3. Since $|1 - 2z/n| > 3/4$ if and only if $z < n/8$ or $z > 7n/8$, one has

$$|\{\mathbf{a} : |\langle P_{\mathbf{a}} \rangle_\rho| > 3/4\}| \leq 2 \sum_{k=0}^{\lfloor n/8 \rfloor} \binom{n}{k} \leq 2^{nH(1/8)+1} < 2^{3n/4}, \quad (\text{C8})$$

where $H(x) = -x \log x - (1-x) \log(1-x)$, by a well-known bound of the sum of binomial coefficients in terms of the binary entropy [38].

APPENDIX D: ROBUSTNESS OF rDIPE

In this section we prove the robustness result in the main text for states in CW. To this end, consider two sequences $\{\rho'\}, \{\sigma'\}$ that are within trace distance τ of $\{\rho\}, \{\sigma\} \in \text{CW}$. We have

$$\begin{aligned} \Delta \equiv \text{TV}(q'_{\text{mix}}, p'_{\text{mix}}) &\leq \frac{\text{TV}(q'_{\rho'_n}, p'_{\rho'_n})}{2} + \frac{\text{TV}(q'_{\sigma'_n}, p'_{\sigma'_n})}{2} \\ &\leq \frac{3\|\rho_n - \rho'_n\|_{\text{tr}}}{2} + \frac{3\|\sigma_n - \sigma'_n\|_{\text{tr}}}{2} \leq 3\tau. \end{aligned} \quad (\text{D1})$$

To derive the previous expression, we have used the triangle inequality $\text{TV}(q_{\rho'}, p_{\rho'}) \leq \text{TV}(q_{\rho'}, q_{\rho}) + \text{TV}(p_{\rho}, p_{\rho'})$ since for real pure states $p_{\rho} = q_{\rho}$, and similarly for the term relative to σ . Finally, we used Eq. (C2) above and the fact that $\text{TV}(q_{\rho'}, q_{\rho}) \leq \|\rho - \rho'\|_{\text{tr}}$ by the data-processing inequality [39].

Now, for all $n, \tau > 0$, consider ϵ_1, ϵ_2 given by $\epsilon_1 = \tau/8$ and $\epsilon_2 = \min\{(\tau/8)^2, 1/n^2\}$, such that $4\epsilon_1 + 4\sqrt{\epsilon_2} \leq \tau$. From Eq. (C7) we have that the CDF $F(\epsilon)$ is small whenever ϵ is inverse-polynomially small. In particular, $F_{\rho'_n}(\epsilon_2) \leq 5\|\rho_n - \rho'_n\|_{\text{tr}} \leq 5\tau$, since $\epsilon_2 \leq 1/n^2 < 2/n^2$. Similarly, $F_{\sigma'_n}(\epsilon_2) \leq 5\tau$

as well. Together with Eq. (D1), this implies

$$4\epsilon_1 + 4\sqrt{\epsilon_2} + F_{\rho'_n}(\epsilon_2) + F_{\sigma'_n}(\epsilon_2) + 6\Delta \leq 29\tau.$$

Substituting into Eq. (4) gives

$$\begin{aligned} \mathbb{P}\{|f(\rho'_n, \sigma'_n, N_1, N_2) - c(\rho'_n, \sigma'_n)| > 29\tau\} \\ < 4 \exp(-2\epsilon_1^2 N_1) + 4N_1 \exp(-\epsilon_2^2 N_2/2). \end{aligned}$$

The previous expression shows that there exist $N_1, N_2 = \text{poly}(n, 1/\tau, \delta)$ such that Eq. (9) holds when $\{\rho\}, \{\sigma\} \in \text{CW}$, for $k = 29$.

-
- [1] J. Eisert, D. Hangleiter, N. Walk, I. Roth, D. Markham, R. Parekh, U. Chabaud, and E. Kashefi, Quantum certification and benchmarking, *Nat. Rev. Phys.* **2**, 382 (2020).
 - [2] R. O'Donnell and J. Wright, Efficient quantum tomography, in *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '16 (Association for Computing Machinery, New York, NY, USA, 2016), pp. 899–912.
 - [3] M. P. da Silva, O. Landon-Cardinal, and D. Poulin, Practical characterization of quantum devices without tomography, *Phys. Rev. Lett.* **107**, 210404 (2011).
 - [4] S. T. Flammia and Y.-K. Liu, Direct fidelity estimation from few Pauli measurements, *Phys. Rev. Lett.* **106**, 230501 (2011).
 - [5] N. Schuch, M. M. Wolf, F. Verstraete, and J. I. Cirac, Entropy scaling and simulability by matrix product states, *Phys. Rev. Lett.* **100**, 030504 (2008).
 - [6] N.-H. Chia, C.-Y. Lai, and H.-H. Lin, Efficient learning of t -doped stabilizer states with single-copy measurements, *Quantum* **8**, 1250 (2024).
 - [7] L. Leone, S. F. E. Oliviero, and A. Hamma, Learning t -doped stabilizer states, *Quantum* **8**, 1361 (2024).
 - [8] U. Mahadev, Classical verification of quantum computations, in *Proceedings of the 2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)* (IEEE, Paris, France, 2018), pp. 259–267.
 - [9] Z. Brakerski, V. Koppula, U. Vazirani, and T. Vidick, Simpler proofs of quantumness, in *Proceedings of the 15th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2020)*, Leibniz International Proceedings in Informatics (LIPIcs), Vol. 158 (Schloss Dagstuhl, Germany, 2020), pp. 8:1–8:14.
 - [10] Z. Brakerski, P. Christiano, U. Mahadev, U. Vazirani, and T. Vidick, A cryptographic test of quantumness and certifiable randomness from a single quantum device, *J. ACM* **68**, 1 (2021).
 - [11] A. Elben, B. Vermersch, R. van Bijnen, C. Kokail, T. Brydges, C. Maier, M. Joshi, R. Blatt, C. F. Roos, and P. Zoller, Cross-platform verification of intermediate scale quantum devices, *Phys. Rev. Lett.* **124**, 010504 (2020).
 - [12] J. Carrasco, A. Elben, C. Kokail, B. Kraus, and P. Zoller, Theoretical and experimental perspectives of quantum verification, *PRX Quantum* **2**, 010102 (2021).
 - [13] A. Anshu, Z. Landau, and Y. Liu, Distributed quantum inner product estimation, in *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing* (ACM, New York, 2022), pp. 44–51.
 - [14] J. Knörzer, D. Malz, and J. I. Cirac, Cross-platform verification in quantum networks, *Phys. Rev. A* **107**, 062424 (2023).
 - [15] W. Gong, J. Haferkamp, Q. Ye, and Z. Zhang, On the sample complexity of purity and inner product estimation, [arXiv:2410.12712](https://arxiv.org/abs/2410.12712).
 - [16] S. Arunachalam and L. Schatzki, Distributed inner product estimation with limited quantum communication, [arXiv:2410.12684](https://arxiv.org/abs/2410.12684).
 - [17] Y. Qian, Y. Du, Z. He, M.-H. Hsieh, and D. Tao, Multimodal deep representation learning for quantum cross-platform verification, *Phys. Rev. Lett.* **133**, 130601 (2024).
 - [18] M. Hinsche, M. Ioannou, S. Jerbi, L. Leone, J. Eisert, and J. Carrasco, Efficient distributed inner product estimation via Pauli sampling, [arXiv:2405.06544](https://arxiv.org/abs/2405.06544).
 - [19] A. Montanaro, Learning stabilizer states by bell sampling, [arXiv:1707.04012](https://arxiv.org/abs/1707.04012).
 - [20] Here and in what follows, $\mathbb{P}$ will denote the probability with respect to the internal randomness of rDIPE for fixed inputs.
 - [21] A. K. Hashagen, S. T. Flammia, D. Gross, and J. J. Wallman, Real randomized benchmarking, *Quantum* **2**, 85 (2018).
 - [22] R. Ruiz, A. Sopena, B. Pozsgay, and E. López, Efficient eigenstate preparation in an integrable model with Hilbert space fragmentation, [arXiv:2411.15132](https://arxiv.org/abs/2411.15132).
 - [23] The proof is analogous for arbitrary non-Clifford gates acting on a constant number of qubits.
 - [24] D. Aharonov, A simple proof that Toffoli and Hadamard are quantum universal, [arXiv:quant-ph/0301040](https://arxiv.org/abs/quant-ph/0301040).
 - [25] Y. Shi, Both Toffoli and Controlled-NOT need little help to do universal quantum computation, [arXiv:quant-ph/0205115](https://arxiv.org/abs/quant-ph/0205115).
 - [26] J. J. Wallman and J. Emerson, Noise tailoring for scalable quantum computation via randomized compiling, *Phys. Rev. A* **94**, 052325 (2016).
 - [27] A. Dvoretzky, J. Kiefer, and J. Wolfowitz, Asymptotic minimax character of the sample distribution function and of the classical multinomial estimator, *Ann. Math. Stat.* **27**, 642 (1956).
 - [28] P. Massart, The Tight Constant in the Dvoretzky-Kiefer-Wolfowitz inequality, *Ann. Probab.* **18**, 1269 (1990).
 - [29] H.-Y. Huang, M. Broughton, J. Cotler, S. Chen, J. Li, M. Mohseni, H. Neven, R. Babbush, R. Kueng, J. Preskill, and J. R. McClean, Quantum advantage in learning from experiments, *Science* **376**, 1182 (2022).
 - [30] C. Schmid, N. Kiesel, W. Wieczorek, H. Weinfurter, F. Mintert, and A. Buchleitner, Experimental direct observation of mixed state entanglement, *Phys. Rev. Lett.* **101**, 260505 (2008).

- [31] D. Miller, K. Levi, L. Postler, A. Steiner, L. Bittel, G. A. L. White, Y. Tang, E. J. Kuehnke, A. A. Mele, S. Khatri, L. Leone, J. Carrasco, C. D. Marciniak, I. Pogorelov, M. Guevara-Bertsch, R. Freund, R. Blatt, P. Schindler, T. Monz, M. Ringbauer, and J. Eisert, Experimental measurement and a physical interpretation of quantum shadow enumerators, [arXiv:2408.16914](#).
- [32] R. Islam, R. Ma, P. M. Preiss, M. Eric Tai, A. Lukin, M. Rispoli, and M. Greiner, Measuring entanglement entropy in a quantum many-body system, [Nature \(London\) 528, 77 \(2015\)](#).
- [33] D. Bluvstein, H. Levine, G. Semeghini, T. T. Wang, S. Ebadi, M. Kalinowski, A. Keesling, N. Maskara, H. Pichler, M. Greiner, V. Vuletić, and M. D. Lukin, A quantum processor based on coherent transport of entangled atom arrays, [Nature \(London\) 604, 451 \(2022\)](#).
- [34] D. Bluvstein, S. J. Evered, A. A. Geim, S. H. Li, H. Zhou, T. Manovitz, S. Ebadi, M. Cain, M. Kalinowski, D. Hangleiter, J. P. Bonilla Ataides, N. Maskara, I. Cong, X. Gao, P. Sales Rodriguez, T. Karolyshyn, G. Semeghini, M. J. Gullans, M. Greiner, V. Vuletić, and M. D. Lukin, Logical quantum processor based on reconfigurable atom arrays, [Nature \(London\) 626, 58 \(2024\)](#).
- [35] J. Hauschild, J. Unfried, S. Anand, B. Andrews, M. Bintz, U. Borla, S. Divic, M. Drescher, J. Geiger, M. Hefel *et al.*, Tensor network Python (TeNPy) version 1, [SciPost Phys. Codebases 41, 1 \(2024\)](#).
- [36] A. A. Mele, Introduction to haar measure tools in quantum information: A beginner's tutorial, [Quantum 8, 1340 \(2024\)](#).
- [37] B. Collins and P. Dniady, Integration with respect to the haar measure on unitary, orthogonal and symplectic group, [Commun. Math. Phys. 264, 773 \(2006\)](#).
- [38] D. Galvin, Three tutorial lectures on entropy and counting, [arXiv:1406.7872](#).
- [39] Indeed, $\text{TV}(q_{\rho'}, q_{\rho}) \leq \|\rho \otimes \rho - \rho' \otimes \rho'\|_{\text{tr}}/2$ since the Bell distribution is the (diagonal) output of a quantum channel acting on two copies of a state, and $\|\rho \otimes \rho - \rho' \otimes \rho'\|_{\text{tr}} \leq 2\|\rho - \rho'\|_{\text{tr}}$.