

Optimal interpolation of entanglement purification protocols

Matthew Barber  and Stefano Pirandola 

Department of Computer Science, University of York, York YO10 5GH, United Kingdom



(Received 12 November 2025; accepted 29 July 2026; published 8 September 2026)

Bipartite entanglement purification is the conversion of copies of weakly entangled pairs shared between two separated parties into a smaller number of strongly entangled shared pairs using only local operations and classical communication. Choosing between different entanglement purification protocols generally involves weighing up a trade-off between the ratio of strongly entangled pairs produced to weakly entangled pairs consumed, which we call the rate of the protocol, and the degree of the entanglement of the strongly entangled pairs, typically measured by the fidelity of those pairs to maximally entangled states. By randomly choosing a protocol according to a probability distribution over a list of protocols for each pair we want to produce, we can achieve rates and fidelities not achieved by any of the original protocols. Here, we show how to choose this distribution to maximize the rate at which we produce qubit pairs with a given fidelity to a Bell state or, equivalently, to maximize the fidelity to a Bell state of the qubit pairs produced at a given rate. We investigate both the asymptotic case, where the number of initial pairs goes to infinity, and the finite-size regime, where protocols are restricted to a finite number of weakly entangled pairs.

DOI: [10.1103/v55w-6x44](https://doi.org/10.1103/v55w-6x44)

I. INTRODUCTION

In quantum information, we have resources with no counterpart in classical information. Of these, entanglement is one of the better understood. Moreover, it is one of the most useful; among other applications, entanglement is used in protocols to teleport quantum states [1], double the amount of classical information that can be communicated per use of a noiseless qubit channel [2], and share secret cryptographic keys [3–5]. Like other quantum resources, it is limited by a fundamental rate-loss scaling law [6], thus requiring the use of quantum networks for long-distance end-to-end distribution.

Entanglement can only be created locally [7]. Therefore, two separated parties, Alice and Bob, typically come to share entanglement by an entangled pair being created locally and then the two halves being sent to Alice and Bob. This process introduces noise in the entangled pair and so we cannot expect Alice and Bob's state to be maximally entangled. However, if this process produces pairs whose entanglement is of lower quality than we require or produces pairs at a higher rate than we need to use them, Alice and Bob can choose to sacrifice some of their entangled pairs in the hope of increasing the quality of the entanglement of the others. This process is known as entanglement distillation or entanglement purification [8].

We will not be concerned here with the quantum Shannon-theoretic task of converting our noisy entangled pairs into as many perfect maximally entangled states as possible in the limit as the number of pairs we have to work with goes to

infinity. Rather, we will be focused on those protocols which achieve some nonmaximal level of entanglement, measured by the fidelity of the resulting states with a maximally entangled pair. Moreover, we will focus specifically on the typical case where our initial states are independent qubit pairs.

Generally, there will be a trade-off between the number of pairs we expect to purify per initial pair consumed and the fidelity of the resulting pairs with the chosen Bell state, known as the Bell fidelity, and different purification protocols will provide us with different trade-off options. For some applications, particularly in the context of quantum networks, we may want to convert our initial states into purified states, at least at a particular rate or produce purified states with at least a particular Bell fidelity. For instance, our application might require a minimum quality of entanglement [9] or there may be a bottleneck elsewhere in the network that means Alice and Bob can, up to a point, lower the rate at which they purify pairs with little to no downside [10].

By randomly choosing a purification protocol for each pair we produce, which we shall refer to as interpolating between protocols, we can achieve trade-offs in between the options provided by our original protocols. A preliminary approach to protocol interpolation was discussed in Ref. [11]. However, in that paper, interpolation was only considered between protocols that all aimed to convert the same, fixed number of initial pairs into one purified pair. Here, we consider an optimal strategy for interpolation between protocols that may consume a variable number of pairs to produce one purified pair.

If we have a list of entanglement purification protocols and want to interpolate between them, we must choose a probability distribution over them which tells us with what probability we will choose any given protocol from our list to purify our next pair. Different options for this probability distribution result in different trade-offs between the rate of and fidelity achieved by the corresponding “interpolated” protocol. In

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.

Sec. II, we show how to find the probability distribution which produces pairs with the highest Bell fidelity at a particular rate or produces pairs with a particular Bell fidelity at the highest rate. This is done in the limit as the number of initial pairs we have to purify goes to infinity.

Then, in Sec. III, we investigate the performance of interpolated purification protocols in the case where we only have a fixed, finite number of pairs to purify. Note that although for convenience we will picture these initial pairs as all existing simultaneously in a “pool” of states to be purified, this analysis would also apply in other contexts where many of the pairs did not exist at the same time, for instance, if two parties were frequently generating weakly entangled pairs, purifying them, and then using the purified pairs for their purposes. In that case, the finite number of initial pairs consumed would be the number of weakly entangled pairs generated in total, even though they need not all exist simultaneously.

For concreteness, in both Secs. II and III, we demonstrate the application of the general techniques we develop to the case of interpolating between different numbers of iterations of the “DEJMPS” protocol [12] acting on initial pairs produced by sending halves of Bell states through simple noisy quantum channels. That is, we analyze the performance of “interpolated DEJMPS” protocols acting on initial states of the form $\rho = (\mathbb{1}_A \otimes \mathcal{E}_B)(|\Phi\rangle\langle\Phi|)$, where $|\Phi\rangle$ is our chosen Bell state, $\mathbb{1}_A$ is the identity on the half of $|\Phi\rangle$ that Alice keeps, and $\mathcal{E}_B$ is a quantum channel applied to the second, transmitted qubit. We compare the rates achieved by the interpolated protocols to the rates that would be achieved if we applied the DEJMPS protocol just enough times to reach a target fidelity of 0.9 to $|\Phi\rangle\langle\Phi|$.

II. THE ASYMPTOTIC SCENARIO

A. The general case

1. Achievable rates and fidelities

Suppose Alice and Bob have a pool of independent qubit pairs, each in some entangled state ρ , and want to convert them, via local operations and classical communication (LOCC), into as many independent pairs as possible with as high a Bell fidelity as possible where, by the Bell fidelity, we mean the fidelity to $|\Phi\rangle\langle\Phi|$. Naturally, we expect there to be a trade-off between the Bell fidelity they achieve and the number of such pairs they produce per pair consumed from the pool. Here, we will define the fidelity between two density operators, τ and τ' , to be

$$F(\tau, \tau') = (\text{Tr} \sqrt{\sqrt{\tau} \tau' \sqrt{\tau}})^2. \quad (1)$$

Moreover, for every $F' \in [0, 1]$, we will let

$$W_{F'} = \frac{4F' - 1}{3} |\Phi\rangle\langle\Phi| + \frac{4 - 4F'}{12} \mathbb{1}_4, \quad (2)$$

where $\mathbb{1}_4$ is the 4×4 identity operator, denote the Werner state of Bell fidelity F' . Now, let $H = \mathbb{C}^2 \otimes \mathbb{C}^2$ be the Hilbert space in which the state of a qubit pair exists. Then, given $F' \in (\frac{1}{2}, 1)$ and $R \in (0, \infty)$, if, for every $\delta \in (0, R)$ and $\epsilon \in (0, 1)$, there exists an $N \in \mathbb{N}$ and an LOCC, Λ , from the space of density operators on H^N to the space of density operators on

$H^{\lceil N(R-\delta) \rceil}$ such that

$$F[\Lambda(\rho^{\otimes N}), W_{F'}^{\otimes \lceil N(R-\delta) \rceil}] \geq 1 - \epsilon, \quad (3)$$

where $W_{F'}$ denotes the Werner state [13] of Bell fidelity F' , then we will say we can achieve a fidelity F' with rate R from ρ .

2. The interpolated protocol

If Alice and Bob agree on a protocol which will, on average, consume some finite, nonzero number I of states from the pool and with probability 1 will produce a single entangled qubit pair in some state ρ' , then we will say that the rate of this protocol is $\frac{1}{I}$. By the law of large numbers, we can see that if Alice and Bob repeat the process enough times, they can ensure that the probability of the number of ρ' states they produce divided by the number of ρ states they consume being arbitrarily close to the rate of the protocol is arbitrarily close to 1. Now, imagine that we have a set of K protocols, for some $K \in \mathbb{N}$, which produce a single copy of the states $\rho'_1, \rho'_2, \dots, \rho'_K$, respectively. We will denote by $I_1, I_2, \dots, I_K$ the numbers of states the respective protocols consume on average and by $R_1, R_2, \dots, R_K$ the rates of our respective protocols.

Let $p_1, p_2, \dots, p_K$ be the probabilities of a probability distribution over $\{1, 2, \dots, K\}$ and let

$$R = \frac{1}{p_1 I_1 + p_2 I_2 + \dots + p_K I_K}. \quad (4)$$

Now, choose $\delta \in (0, R)$ and $\epsilon \in (0, 1)$. Given $N \in \mathbb{N}$, let $X_1, X_2, X_3, \dots, X_{\lceil N(R-\delta) \rceil}$ be independent random variables, each distributed over $\{1, 2, \dots, K\}$ according to the chosen probability distribution. Now, imagine that Alice and Bob apply their X_1 th protocol, followed by their X_2 th protocol, and so on, until they apply the $X_{\lceil N(R-\delta) \rceil}$ th protocol. Let $Y_{\lceil N(R-\delta) \rceil} = 0$ if the number of ρ states consumed exceeds N and let $Y_{\lceil N(R-\delta) \rceil} = 1$ otherwise. If $Y_{\lceil N(R-\delta) \rceil} = 0$, then they declare failure and replace all of their qubits with $W_{\frac{1}{2}}$ or some other separable state of their choosing. Otherwise, they declare success and apply the twirling operation, the operation described as a random bilateral rotation in [14], to each of their pairs, converting them into Werner states while preserving each pair's Bell fidelity. By the weak law of large numbers, as $N \rightarrow \infty$, $\Pr(Y_{\lceil N(R-\delta) \rceil} = 1) \rightarrow 1$. Therefore, we can fix N so that $\Pr(Y_{\lceil N(R-\delta) \rceil} = 1) \geq \sqrt{1 - \epsilon}$.

Let $F_1, \dots, F_K$ denote the Bell fidelities of $\rho'_1, \dots, \rho'_K$, respectively, and let

$$F' = p_1 F_1 + p_2 F_2 + \dots + p_K F_K. \quad (5)$$

We then see that Alice and Bob's interpolated protocol maps $\rho^{\otimes N}$ to

$$\sigma^M = \Pr(Y_M = 1) \tilde{W}_{F'}^M + \Pr(Y_M = 0) W_{\frac{1}{2}}^{\otimes M}, \quad (6)$$

where

$$\tilde{W}_{F'}^M = \sum_{x \in \{1, \dots, K\}^M} \Pr(X^M = x | Y_M = 1) \bigotimes_{i=1}^M W_{F_{x_i}}, \quad (7)$$

with $M = \lceil N(R - \delta) \rceil$ and $X^M = (X_1, \dots, X_M)$. Note that both σ^M and $W_{F'}^M$ are Bell diagonal.

Let $Z_1, Z_2, \dots, Z_M$ be random variables on $\{1, 2, 3, 4\}$, conditionally independent given $(X_1, \dots, X_M)$, where, for every $i \in \{1, 2, \dots, M\}$ and $x \in \{1, 2, \dots, K\}^M$,

$$\Pr(Z_i = 1 | X^M = x) = F_{x_i} \quad (8)$$

and

$$\begin{aligned} \Pr(Z_i = 2 | X^M = x) &= \Pr(Z_i = 3 | X^M = x) \\ &= \Pr(Z_i = 4 | X^M = x) \\ &= \frac{1 - F_{x_i}}{3}. \end{aligned} \quad (9)$$

We then associate with each possible sequence of M Bell states a unique z in $\{1, 2, 3, 4\}^M$ so that the probability mass function of Z^M over $\{1, 2, 3, 4\}^M$ corresponds to diagonal elements of $W_{F'}^M$ in the Bell basis. Likewise, we define a random variable Z'^M , which is equal to Z^M if Y_M equals 1 and, if Y_M equals 0, is a sequence of M independent random variables over $\{1, 2, 3, 4\}$, which are each 1 with probability $\frac{1}{2}$, 2 with probability $\frac{1}{6}$, 3 with probability $\frac{1}{6}$, and 4 with probability $\frac{1}{6}$. Then, the probability mass function of Z'^M corresponds to the diagonal elements of σ^M in the Bell basis, just as the probability mass function of Z^M did for $W_{F'}^M$.

Now,

$$\begin{aligned} &F(\sigma^{[N(R-\delta)]}, W_{F'}^{\otimes [N(R-\delta)]}) \\ &= \left(\sum_{z \in \{1, \dots, 4\}^M} \sqrt{\Pr(Z^M = z) \Pr(Z'^M = z)} \right)^2 \\ &\geq \left(\sum_{z \in \{1, \dots, 4\}^M} \sqrt{\Pr(Z^M = z) \Pr(Z'^M = z, Y_M = 1)} \right)^2 \\ &\geq \left[\sum_{z \in \{1, \dots, 4\}^M} \Pr(Z^M = z, Y_M = 1) \right]^2 \\ &= \Pr(Y_M = 1)^2 \\ &\geq 1 - \epsilon. \end{aligned} \quad (10)$$

Therefore, we can achieve a fidelity F' with rate R with our iterated interpolated protocol. Before moving on, we note that we can, if we wish, instead say that with probability $\Pr(Y_{[N(R-\delta)]} = 1)$, we succeed in producing a state with fidelity at least $\Pr(Y_{[N(R-\delta)]} = 1)$ to $W_{F'}^{\otimes [N(R-\delta)]}$, namely, $\tilde{W}_{F'}^{[N(R-\delta)]}$, starting from $\rho^{\otimes N}$.

3. Reparametrizing the interpolation

Now, for each $k \in \{1, 2, \dots, K\}$, let

$$q_k = p_k I_k \quad (11)$$

so that the achieved fidelity is

$$\frac{q_1 R_1 F_1 + q_2 R_2 F_2 + \dots + q_K R_K F_K}{q_1 R_1 + q_2 R_2 + \dots + q_K R_K} \quad (12)$$

and the rate is

$$\frac{q_1 R_1 + q_2 R_2 + \dots + q_K R_K}{q_1 + q_2 + \dots + q_K}. \quad (13)$$

Note that the achievable fidelity and rate would not change if we multiplied $q_1, q_2, \dots, q_K$ by the same nonzero constant. Therefore, in what follows, we will drop the normalization condition that $p_1 + p_2 + \dots + p_K = 1$ and instead insist only that $q_1, q_2, \dots, q_K$ are non-negative and $q_1 + q_2 + \dots + q_K \neq 0$.

4. Optimizing the interpolation

We now turn to the question of how to choose our $q_1, \dots, q_K$ so as to maximize the fidelity achieved at a particular rate, or vice versa. If one protocol achieved both at least as high a rate and at least as high a fidelity as another, then there would be no point in ever using the latter protocol. Therefore, we assume $R_1 > \dots > R_K$ and $F_1 < \dots < F_K$. Now, if at least three of $q_1, q_2, \dots, q_K$ are positive, we can choose three distinct values, i, j , and k , from $\{1, 2, 3, \dots, K\}$ such that q_i, q_j , and q_k are positive and assume, without loss of generality, that $i < j < k$. Then, we can choose $r \in (0, 1)$ such that $rR_i + (1-r)R_k = R_j$.

For every $l \in \{1, 2, \dots, K\} \setminus \{i, j, k\}$, let $\tilde{q}_l = q_l$. If we have $rR_i F_i + (1-r)R_k F_k - R_j F_j \geq 0$, then we let $\tilde{q}_i = q_i + r q_j$, $\tilde{q}_k = q_k + (1-r)q_j$, and $\tilde{q}_j = 0$. Otherwise, we let $\tilde{q}_i = q_i - r x$, $\tilde{q}_k = q_k - (1-r)x$, and $\tilde{q}_j = q_j + x$, where $x = \min\{\frac{q_i}{r}, \frac{q_k}{1-r}\}$. In either case, we then see that $\tilde{q}_1, \tilde{q}_2, \dots, \tilde{q}_K$ are all non-negative, that the number of them that are nonzero is less than the number of $q_1, q_2, \dots, q_K$ that are nonzero, that

$$\frac{\tilde{q}_1 R_1 + \dots + \tilde{q}_K R_K}{\tilde{q}_1 + \dots + \tilde{q}_K} = \frac{q_1 R_1 + \dots + q_K R_K}{q_1 + \dots + q_K}, \quad (14)$$

and that

$$\frac{\sum_{k=1}^K \tilde{q}_k R_k F_k}{\sum_{k=1}^K \tilde{q}_k R_k} \geq \frac{\sum_{k=1}^K q_k R_k F_k}{\sum_{k=1}^K q_k R_k}. \quad (15)$$

By repeating this argument, then, we see that there must be a way of interpolating between only two of Alice and Bob's protocols to achieve at least as high a Bell fidelity as did our original interpolated protocol at the same rate as our original interpolated protocol. Therefore, when asking how we can optimize our choice of $q_1, q_2, \dots, q_K$ to maximize the Bell fidelity of the resulting states for some fixed rate, or vice versa, we need only consider those choices of $q_1, q_2, \dots, q_K$ for which all but two are nonzero. This greatly simplifies the optimization problem.

Suppose then that we decide to interpolate between two of Alice and Bob's protocols, say, the i th and j th protocols. Suppose further that we are interested in producing approximate ebits at some rate, R_{target} with $R_i \geq R_{\text{target}} \geq R_j$, with as high a Bell fidelity as possible. We can then see that the fidelity we can achieve in this way is

$$\frac{F_i R_i (R_{\text{target}} - R_j) + F_j R_j (R_i - R_{\text{target}})}{R_{\text{target}} (R_i - R_j)}. \quad (16)$$

Hence, provided $R_K \leq R_{\text{target}} \leq R_1$, the maximum fidelity we can achieve at our target rate by interpolating between the given entanglement distillation protocols is

$$\max_{(i,j) \in A} \frac{F_i R_i (R_{\text{target}} - R_j) + F_j R_j (R_i - R_{\text{target}})}{R_{\text{target}} (R_i - R_j)}, \quad (17)$$

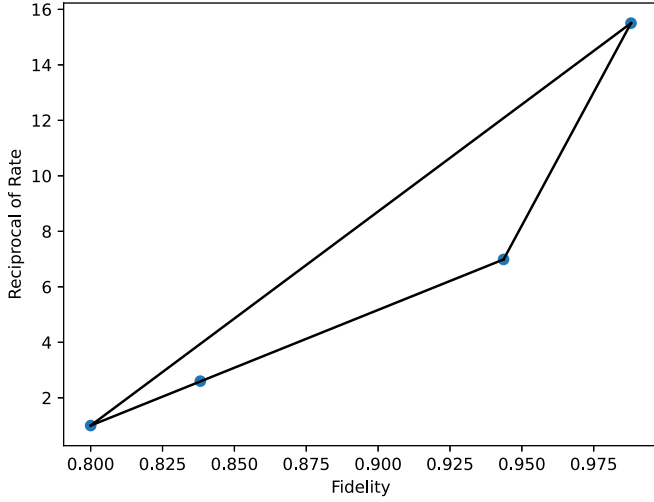


FIG. 1. The convex hull of four points, corresponding to the performance of zero, one, two, and three iterations of the DEJMPS protocol applied to $W_{0.8}$ states. Note that although it is unclear in the image, the point corresponding to one iteration of the DEJMPS protocol lies strictly in the interior of the convex hull in this case.

where

$$A = \{(i, j) \in \{1, \dots, K\}^2 \mid i < j, R_{\text{target}} \in [R_j, R_i]\}.$$

Likewise, the maximum rate at which we can produce approximate ebits with fidelity $F_{\text{target}} \in [F_1, F_K]$ by interpolating between the given entanglement distillation protocols is

$$\max_{(i,j) \in B} \frac{(F_j - F_i)R_i R_j}{R_i(F_{\text{target}} - F_i) + R_j(F_j - F_{\text{target}})}, \quad (18)$$

where

$$B = \{(i, j) \in \{1, \dots, K\}^2 \mid i < j, F_{\text{target}} \in [F_i, F_j]\}.$$

Before moving on, we note that it is also possible to understand this optimization geometrically. By Eqs. (4) and (5), we can achieve some fidelity $F' \in (\frac{1}{2}, 1)$ at a rate $R \in (0, \infty)$ by interpolating between our protocols if and only if the point $(F, \frac{1}{R})$ lies in the convex hull of the points $\{(F_1, I_1), (F_2, I_2), \dots, (F_K, I_K)\}$ plotted on the Cartesian plane. Optimal interpolations correspond to points on the boundary of the convex hull. An example is shown in Fig. 1. From this geometrical perspective, we can see, just as we proved above, that we need not consider interpolations between more than two protocols when searching for the optimal interpolation. We can also see that provided none of our protocols correspond to points in the strict interior of the convex hull, an optimal interpolation can always be found by interpolating between consecutive protocols in our list.

5. Limiting the number of protocols

Suppose Alice and Bob have a sequence of protocols which achieve fidelities $F_1, F_2, \dots$ with respective rates $R_1, R_2, \dots$ with $F_1 < F_2 < \dots$, $R_1 > R_2 > \dots$, $\lim_{k \rightarrow \infty} F_k = 1$, and $\lim_{k \rightarrow \infty} R_k = 0$. They want to find an interpolated protocol using the above ideas to, say, achieve a fidelity F_{target} at as high a rate as possible. However, without choosing a value of K , they cannot use Eq. (18). How can they choose a value of

K and be sure that a larger value would not have allowed them to find an interpolated protocol that achieved the target fidelity at a higher rate?

Naturally, we assume $F_{\text{target}} \in (F_1, 1)$. Now, let $\tilde{K} = \max\{k \in \mathbb{N} \mid F_k < F_{\text{target}}\}$. Suppose that Alice and Bob have already found some interpolated protocol which achieves the fidelity F_{target} at a rate $R_{\text{achieved}} \in (0, \infty)$. We will further assume that $R_{\tilde{K}+1} \leq R_{\text{achieved}} < R_{\tilde{K}}$ since we can clearly achieve fidelity F_{target} , which is less than or equal to $F_{\tilde{K}+1}$, with a rate at least as high as $R_{\tilde{K}+1}$ and if we could achieve it with a rate $R_{\tilde{K}}$, then the $\tilde{K}$ th protocol would be strictly worse than some interpolation of two of our other protocols and could be omitted from our set of protocols without any loss in performance. Now, if, for some $i \in \{1, 2, \dots, \tilde{K}\}$ and some $j \in \{\tilde{K} + 1, \tilde{K} + 2, \dots\}$, it is possible to achieve fidelity F_{target} with rate greater than R_{achieved} by interpolating between the i th and j th protocols, then, from Eq. (18), we see that

$$\frac{(F_j - F_i)R_i R_j}{R_i(F_{\text{target}} - F_i) + R_j(F_j - F_{\text{target}})} > R_{\text{achieved}}, \quad (19)$$

and so we have

$$\begin{aligned} R_j &> \frac{(F_{\text{target}} - F_i)R_{\text{achieved}}R_i}{(F_j - F_i)R_i - (F_j - F_{\text{target}})R_{\text{achieved}}} \\ &> \frac{(F_{\text{target}} - F_i)R_{\text{achieved}}R_i}{(1 - F_i)R_i - (1 - F_{\text{target}})R_{\text{achieved}}} \\ &\geq \Omega, \end{aligned} \quad (20)$$

where Ω denotes

$$\min_{i' \in \{1, \dots, \tilde{K}\}} \frac{(F_{\text{target}} - F_{i'})R_{\text{achieved}}R_{i'}}{(1 - F_{i'})R_{i'} - (1 - F_{\text{target}})R_{\text{achieved}}}. \quad (21)$$

Note that the expression in Eq. (21) is positive and independent of i and j . Therefore, Alice and Bob can set K to $\max\{k \in \mathbb{N} \mid R_k > \Omega\}$, thereby restricting their attention to a finite number of protocols to interpolate between while knowing that they could not have achieved a better rate by setting K to a larger value. We can use an almost identical formula to limit K if we want to maximize the fidelity that we achieve at a particular fixed rate.

B. The DEJMPS case

1. DEJMPS interpolation

We will now apply these concepts to a specific example. Imagine Alice and Bob want to produce approximate ebits with Bell fidelity $F_{\text{target}} \in (\frac{1}{2}, 1)$ at the highest rate they can by interpolating between DEJMPS protocols with different numbers of iterations. For a description of the DEJMPS protocol, see Appendix A.

Let $s_0 = 1$ and, for $i \in \mathbb{N}$, let $s_i = t_i s_{i-1} = \prod_{j=1}^i t_j$, where t_i is the probability of the DEJMPS protocol succeeding when applied to two independent pairs, each in the output state of applying the DEJMPS protocol $i - 1$ times. If we were applying successive iterations of the DEJMPS protocol to a large pool of states, then, for every $i \in \mathbb{N}$, the fraction of the qubit pairs we would expect to survive the i th iteration of the DEJMPS protocol would be $\frac{t_i}{2}$. Then we can see that for $i \in \{0, 1, 2, \dots\}$, the rate of the DEJMPS protocol performed i times is $R_i = \frac{s_i}{2^i}$. For an alternative derivation of this result, see

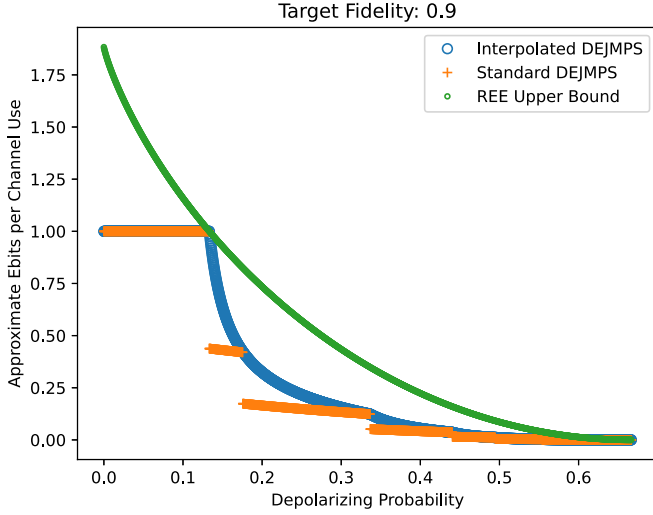


FIG. 2. The rates at which we can convert the output states of the depolarizing channel acting on true ebits into approximate ebits with fidelity 0.9 to a true ebit using the DEJMPS and interpolated DEJMPS protocols. The rate achievable by interpolating between different numbers of DEJMPS iterations is shown in blue. The rate achievable by simply applying the DEJMPS protocol iteratively without interpolation until we reach the target fidelity is shown in orange. The upper bound on the achievable rate shown in green is based on the relative entropy of entanglement (REE).

Appendix A 3 b. Figure 2 shows the rates at which the Werner states produced by applying a depolarizing channel to a true ebit can be converted into states with fidelity 0.9 to a true ebit via interpolated protocols of this kind.

2. An upper bound on the achievable rate

For reference, it may also be useful to compare the rate at which the standard, iterated DEJMPS and interpolated DEJMPS protocols achieve our target fidelity to some upper bound on the achievable rate. Suppose a fidelity F_{target} is achievable with rate R from ρ . Now, let E be an asymptotically continuous entanglement measure. We can see then that for all $\delta \in (0, R)$, we must have

$$\lim_{N \rightarrow \infty} \frac{E(W_{F_{\text{target}}}^{\otimes [N(R-\delta)]})}{N} \leq \lim_{N \rightarrow \infty} \frac{E(\rho^{\otimes N})}{N}. \quad (22)$$

For example, suppose E is the relative entropy of entanglement (REE) and ρ is some Werner state, $W_{F_{\text{initial}}}$. Although it is not additive in general, it is additive with respect to identical Werner states and so we find [15,16]

$$R \leq \frac{1 - h(F_{\text{initial}})}{1 - h(F_{\text{target}})}, \quad (23)$$

where h is the binary entropy function. See, again, Fig. 2, where we compare this upper bound with standard and interpolated DEJMPS protocols.

III. THE FINITE-SIZE SCENARIO

A. Finite N performance

In practice, the pool of states on which we perform entanglement purification will be finite. Therefore, it would be useful to be able to quantify how close the protocols described in Sec. II come to achieving their asymptotic fidelity and rate in the case where we are limited to a pool of N initial states. As before, we let F' denote the fidelity our protocol achieves in the limit as $N \rightarrow \infty$. If we aim to produce M' states and the joint output state for our protocol acting on $\rho^{\otimes N}$ is $\sigma^{M'}$, then we can define the global infidelity as

$$\epsilon_{\text{global}, M'} = 1 - F(\sigma^{M'}, W_{F'}^{\otimes M'}) \quad (24)$$

and the (average) per-pair infidelity as

$$\epsilon_{\text{pair}, M'} = 1 - (1 - \epsilon_{\text{global}, M'})^{\frac{1}{M'}}. \quad (25)$$

Here, we will be interested in the maximum number of states, M , that Alice and Bob can aim to produce while keeping either the global infidelity or the per-pair infidelity below some chosen threshold, $\tilde{\epsilon}$, in $(0, 1)$. That is, we either set

$$M = \max \{M' \in \{0, \dots, N\} \mid \epsilon_{\text{global}, M'} \leq \tilde{\epsilon}\} \quad (26)$$

or

$$M = \max \{M' \in \{0, \dots, N\} \mid \epsilon_{\text{pair}, M'} \leq \tilde{\epsilon}\}, \quad (27)$$

depending on whether we are interested in the global or the per-pair infidelity. We will then say that from $\rho^{\otimes N}$, we have achieved a fidelity F' and rate $\frac{M}{N}$ with a global or per-pair infidelity at most $\tilde{\epsilon}$.

We reiterate at this point that although, for convenience, we will speak of a pool of N initial states, these states need not all exist simultaneously. For instance, suppose two nodes in a quantum network generate initial entangled states ρ , apply their protocol as much as they can to what has been generated so far, and immediately use their purified pairs as they produce them. If, for example, they are using an interpolated DEJMPS protocol, as described in Sec. II B 1, in which the largest number of iterations of the DEJMPS protocol they apply is j , they need only store up to $j + 1$ qubit pairs at a time. Then, if we know that, say, in some time period, the two nodes will generate N copies of ρ and we want to purify them into as many copies of $W_{F'}$ as possible, up to some specified infidelity, then we can achieve this with some number of purified states, M , even though the copies of ρ need not all exist simultaneously.

B. Bounding M

In practice, it may be computationally expensive to find M . Therefore, we will find upper and lower bounds on it instead by placing upper and lower bounds on $F(\sigma^{M'}, W_{F'}^{\otimes M'})$ for different values of M' . Inequality (10) tells us that we will have

$$F(\sigma^{M'}, W_{F'}^{\otimes M'}) \geq \Pr(Y_{M'} = 1)^2.$$

If we do not use an interpolated protocol but rather one which always produces independent $W_{F'}$ states, then we can use the independence of $Z^{M'}$ and $Y_{M'}$ to modify the argument used to

derive Ineq. (10) and obtain a tighter lower bound,

$$\begin{aligned} F(\sigma^{M'}, W_{F'}^{\otimes M'}) &\geq \left(\sum_{m \in \{1,2,3,4\}^{M'}} \sqrt{\Pr(Z^{M'} = z)^2 \Pr(Y_{M'} = 1)} \right)^2 \\ &= \Pr(Y_{M'} = 1). \end{aligned} \quad (28)$$

For instance, Ineq. (28) would apply if our protocol consisted in applying enough iterations of the DEJMPS protocol for the Bell fidelity of the resulting output states to exceed F' and then applying a twirling and a depolarizing operation to convert our output states into $W_{F'}$ states. We can obtain an upper bound on $F(\sigma^{M'}, W_{F'}^{\otimes M'})$ by using the fact that the fidelity between two states increases under the action of the partial trace on any of the subsystems. Let $F_{M'}''$ equal

$$\frac{\Pr(Y_{M'} = 0)}{2} + \sum_{k=1}^K \Pr(X_{M'} = k, Y_{M'} = 1) F_k. \quad (29)$$

Then, taking the partial trace over all but the last qubit pair, we find that

$$\begin{aligned} F(\sigma^{M'}, W_{F'}^{\otimes M'}) &\leq F(W_{F'}, W_{F'}) \\ &= (\sqrt{F' F_{M'}''} + \sqrt{(1 - F')(1 - F_{M'}'')})^2. \end{aligned} \quad (30)$$

We will use these upper and lower bounds to put upper and lower bounds on M , allowing us to compare the performance of our new, interpolated protocols to our original protocols. For concreteness, we will assume that we want to limit the global infidelity of our protocol's output to be less than $\tilde{\epsilon}$, that is, we are defining M using Eq. (26). If we instead wish to use Eq. (27), what follows can be adapted straightforwardly to that case.

We have

$$M \geq \max O_1, \quad (31)$$

where O_1 denotes

$$\{M' \in \{0, \dots, N\} \mid \Pr(Y_{M'} = 1) \geq \sqrt{1 - \tilde{\epsilon}}\}. \quad (32)$$

If our protocol only produces independent $W_{F'}$ states upon success, we can improve this using Ineq. (28) and write

$$M \geq \max O_2, \quad (33)$$

where

$$O_2 = \{M' \in \{0, \dots, N\} \mid \Pr(Y_{M'} = 1) \geq 1 - \tilde{\epsilon}\}. \quad (34)$$

Finally, based on Ineq. (30), we have

$$M \leq \max O_3, \quad (35)$$

where O_3 denotes

$$\{M' \in \{0, \dots, N\} \mid F(W_{F'}, W_{F'}^{\otimes M'}) \geq 1 - \tilde{\epsilon}\}. \quad (36)$$

Hence, if we have a method for calculating $\Pr(X_{M'} = k, Y_{M'} = 1)$ for different values of M' and k , then we can bound M . In Appendix B, we describe two such methods that we have applied to our interpolated DEJMPS protocols to produce Figs. 3 and 4. These figures provide an example of the improved performance that can be obtained in certain regimes

using the interpolation techniques described in this paper. In particular, we see how the interpolated DEJMPS protocol is able to clearly outperform the rate of the standard one in various intermediate regimes. Appendix C provides additional such figures.

IV. CONCLUSION

Interpolating between different protocols often allows two parties to purify weakly entangled pairs into pairs with a given target Bell fidelity at a higher rate or to purify at a particular rate input pairs into output pairs with a higher Bell fidelity than could have been done by any of their “uninterpolated” protocols. This is particularly true when, as will typically be the case when choosing between a discrete set of protocols, none of our protocols achieve the target fidelity or target rate without excess. Therefore, interpolating between entanglement purification protocols is likely to be a useful technique for any application for which we require pairs to be purified at a particular rate or to a particular quality.

For simplicity, we have only considered protocols that purify just one pair at a time, so-called $n \rightarrow 1$ protocols, here, but our results could be extended to protocols that produce multiple purified pairs together, so-called $n \rightarrow m$ protocols. When we use $n \rightarrow m$ protocols, the situation is complicated by the fact that the purified pairs are no longer independent, but are correlated with pairs that were produced with them. For instance, if all our protocols produce two Werner states of a particular Bell fidelity, rather than one, then if you know what the state of the first purified pair is, you will also know the state of the second. For some applications, these correlations between states may not matter, but for others they might. To produce a global state which is approximately equal to a tensor product of Werner states with the target fidelity, as measured by the fidelity of our average global output state to that global target state, we could purify many pairs and then perform a random permutation of the purified pairs. One disadvantage of this would be that we would not be able to use the purified pairs as soon as they were purified. Rather, we would have to wait until we had purified many pairs so we could perform our permutation.

One question not considered here is how to optimally interpolate in the finite-size scenario. The interpolation that is optimal in the asymptotic scenario is not necessarily optimal when we have a finite N , as can be seen, for example, in Fig. 3, where the standard DEJMPS protocol performs better than our interpolated protocol for certain channel parameters and values of N . This could be an interesting avenue for future research.

A natural next step would be to apply the results developed here in a realistic setting. For instance, it would be of interest to model how effectively they can be applied as part of a practical entanglement distribution protocol in a realistic quantum network [17–22]. Note that while we have chosen to use the DEJMPS protocol to illustrate the interpolation idea, when designing an entanglement distribution protocol, we may be able to achieve better performance by considering other practical entanglement purification protocols.

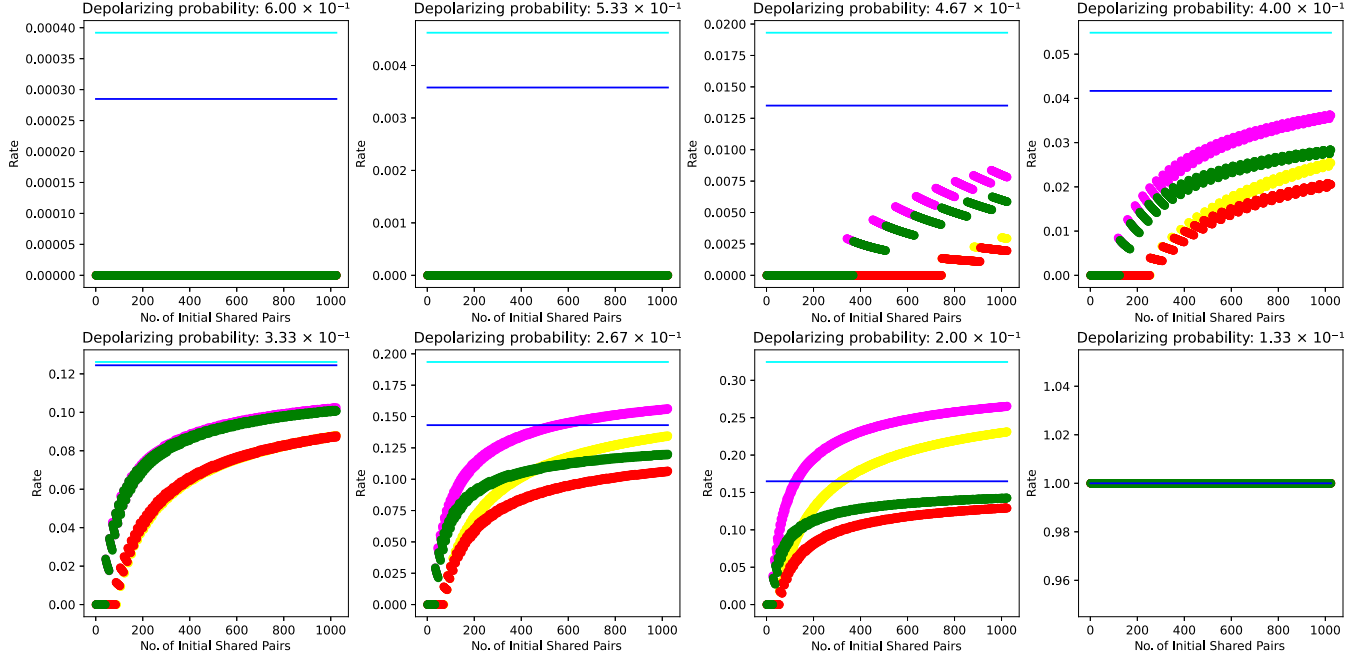


FIG. 3. Lower and upper bounds on the maximum number of output pairs per input pair at which the DEJMPS and interpolated DEJMPS protocols achieve the target fidelity of 0.9 within a global infidelity of 10^{-7} against the number of initial pairs, generated by applying a depolarizing channel to one qubit of our chosen Bell state. The Bell fidelities of the initial states are linearly spaced, ranging from 0.55 in the top-left figure to 0.9 in the bottom-right figure. At the top of each panel, we show the depolarizing probabilities corresponding to those fidelities to three significant figures. If the depolarizing probability is p , then the Bell fidelity of the initial states is $\frac{4-3p}{4}$. The lower and upper bounds for the DEJMPS protocol are in red and green, respectively, and for the interpolated DEJMPS protocol, they are in yellow and magenta, respectively. The asymptotic rates of the DEJMPS and interpolated DEJMPS protocols are shown in blue and cyan, respectively. Note that the lower bounds for the interpolated protocols are based on Ineq. (31), the lower bounds for the uninterpolated DEJMPS protocols are based on Ineq. (33), and the upper bounds are based on Ineq. (35).

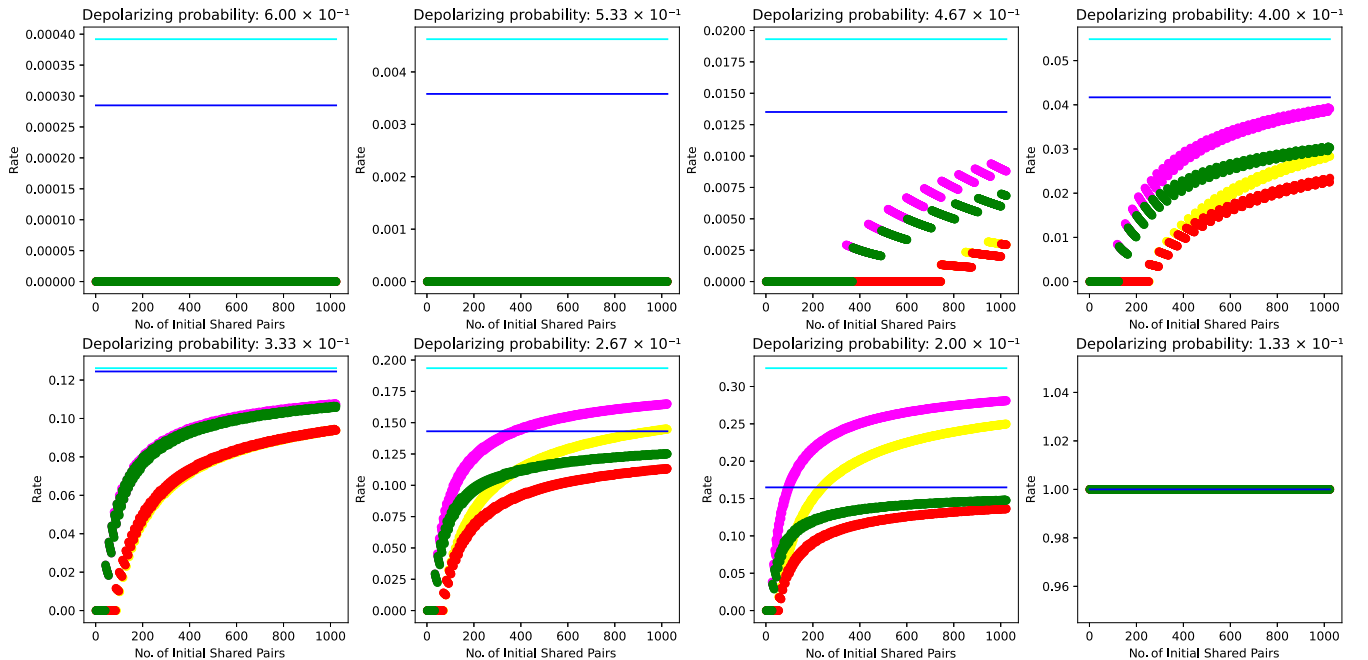


FIG. 4. The same as Fig. 3, except the maximum allowed infidelity is a per-pair infidelity of 10^{-7} .

ACKNOWLEDGMENTS

We acknowledge support from UKRI via the “Integrated Quantum Networks Research Hub” (Grant No. IQN, EP/Z533208/1). We would like to thank Cillian Harney for insightful discussions and the anonymous referees for their helpful comments.

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.

APPENDIX A: THE DEJMPS PROTOCOL

1. The basic description

The DEJMPS protocol [12] is a well-known entanglement purification protocol. It is very similar to another well-known purification protocol, often referred to as the “BBPSSW” protocol [14], although the DEJMPS protocol is regarded as more efficient [23]. As we have used the DEJMPS protocol to illustrate the interpolation techniques developed in this paper, we will briefly describe it here.

Let $|0_A\rangle$ and $|1_A\rangle$ denote the two computational basis states for Alice’s qubit and $|0_B\rangle$ and $|1_B\rangle$ denote the same for Bob’s qubit. Now, let

$$|\Phi^+\rangle = \frac{|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle}{\sqrt{2}}, \quad (\text{A1})$$

$$|\Phi^-\rangle = \frac{|0_A\rangle|0_B\rangle - |1_A\rangle|1_B\rangle}{\sqrt{2}}, \quad (\text{A2})$$

$$|\Psi^+\rangle = \frac{|0_A\rangle|1_B\rangle + |1_A\rangle|0_B\rangle}{\sqrt{2}}, \quad (\text{A3})$$

and

$$|\Psi^-\rangle = \frac{|0_A\rangle|1_B\rangle - |1_A\rangle|0_B\rangle}{\sqrt{2}}. \quad (\text{A4})$$

We will let $|\Phi^+\rangle$ be our target Bell state, which we referred to simply as $|\Phi\rangle$ in the main body of the paper. Note that we may repeat the argument for any other target Bell state.

Suppose that Alice and Bob share two qubit pairs in the joint state $\rho \otimes \rho'$, where ρ is the state of the first pair and ρ' that of the second pair. If C denotes either A or B , let U_C be the unitary operation that acts on one of Alice or Bob’s qubits accordingly and satisfies

$$U_C|0_C\rangle = \frac{|0_C\rangle - i|1_C\rangle}{\sqrt{2}} \quad (\text{A5})$$

and

$$U_C|1_C\rangle = \frac{|1_C\rangle - i|0_C\rangle}{\sqrt{2}}. \quad (\text{A6})$$

Now, Alice applies U_A to both of her qubits and Bob applies $U_B^\dagger$ to both of his. Alice and Bob then each perform a CONTROLLED-NOT operation on their respective qubits, with the qubits from the first pair being the source qubits and the qubits from the second pair being the target qubits. Finally, Alice and Bob measure their target qubits in the computational basis. If their measurement results are the same, they keep the first qubit pair and otherwise they discard them.

Let A, B, C , and D denote the diagonal elements of ρ in the Bell basis in the order $|\Phi^+\rangle, |\Psi^-\rangle, |\Psi^+\rangle, |\Phi^-\rangle$ and let A', B', C' , and D' denote the corresponding terms for the state ρ' . In that case, the probability that the protocol succeeds and we keep the source pair is

$$t = (A + B)(A' + B') + (C + D)(C' + D'). \quad (\text{A7})$$

If the protocol succeeds, the diagonal elements of the resulting state in the Bell basis with the same ordering as before are given by

$$A'' = \frac{AA' + BB'}{t}, \quad (\text{A8})$$

$$B'' = \frac{CD' + C'D}{t}, \quad (\text{A9})$$

$$C'' = \frac{CC' + DD'}{t}, \quad (\text{A10})$$

and

$$D'' = \frac{AB' + A'B}{t}. \quad (\text{A11})$$

2. Iterations of the DEJMPS protocol

In the main body of the paper, we speak of performing multiple iterations of the DEJMPS protocol. Here, we clarify what we mean by this. Suppose we start with a large pool of independent qubit pairs in some weakly entangled state ρ .

Performing zero iterations of the DEJMPS protocol means leaving the initial state alone. Performing one iteration of the DEJMPS protocol means repeatedly applying the standard DEJMPS protocol to pairs of qubits until we succeed in producing a more entangled pair. Performing two iterations of the DEJMPS protocol means applying one iteration of the DEJMPS protocol two times to produce two pairs more entangled than the initial pairs and then applying the DEJMPS protocol to the resulting two pairs to produce an even more entangled pair or to fail, in which case we repeat the whole procedure until we succeed in producing our even more entangled pair. This pattern then continues. An example of what applying three iterations of the DEJMPS protocol might look like is shown in Fig. 5. Whenever we speak of applying the DEJMPS protocol or some other purification protocol until our states reach the target fidelity, we are talking about applying Algorithm 1. Algorithm 2 is equivalent to Algorithm 1 when we are applying the DEJMPS protocol.

ALGORITHM 1. Applying an entanglement purification protocol until we reach a target Bell fidelity, F' . $P(\rho, N)$ denotes the probability distribution for the number of pairs we will purify if we apply the protocol once, $Q(\rho)$ denotes the states of the purified pairs after one successful application of the protocol, and $\sim$ denotes sampling from a probability distribution.

```

while  $\langle \Phi | \rho | \Phi \rangle < F'$  do
   $N \sim P(\rho, N)$ 
   $\rho \leftarrow Q(\rho)$ 
end while
 $\rho \leftarrow W_{F'}$ 

```

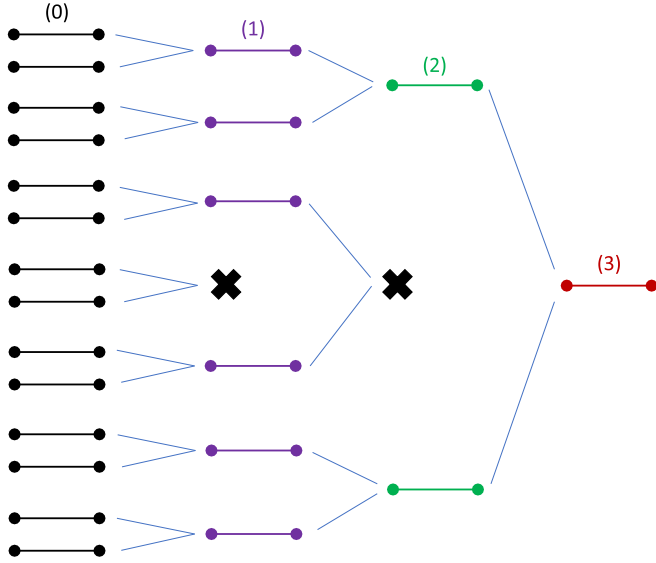


FIG. 5. An example of what performing three iterations of the DEJMPS protocol might look like. The black lines represent the initial pairs. The purple lines represent pairs produced via one iteration of the DEJMPS protocol. The green lines represent pairs produced via two iterations of the DEJMPS protocol. The red line represents a pair produced via three iterations of the DEJMPS protocol. The black crosses denote failed applications of the protocol.

3. Pairs consumed and pairs produced

a. Pairs produced from fixed pool

In the main body of the paper, we measure the error of our purification protocols by the infidelity between the average output state of the protocol and the desired number of copies of the target Werner state. We do this because it allows us to compare our interpolated protocols to our uninterpolated protocols. However, when simply performing a fixed number of iterations of the DEJMPS protocol to a pool of independent and identical initial states, the only variable is the number of output pairs we successfully purify. For completeness, we show one way in which the distribution of this random variable may be calculated.

For $(k, n) \in \{0, 1, 2, \dots\}^2$, let M_k^n denote the random variable representing the number of pairs we can purify from k iterations of the DEJMPS protocol from n initial pairs. Likewise, for all $k \in \mathbb{N}$, let t_k denote the probability that the DEJMPS protocol will succeed when applied to two pairs produced via $k-1$ iterations of the protocol. Then, for all $(m, n) \in \{0, 1, 2, \dots\}^2$, we have

$$\Pr(M_0^n = m) = \delta_{m,n}, \quad (\text{A12})$$

where δ is the Kronecker delta, and

$$\mathbb{E}(M_0^n) = n. \quad (\text{A13})$$

Similarly, we can see that for all $n \in \{0, 1, 2, \dots\}$, M_1^n follows a binomial distribution. For every $t \in [0, 1]$ and $n \in \{0, 1, 2, \dots\}$, let B_t^n be a $B(n, t)$ random variable. Then, for all $m \in \{0, 1, 2, \dots\}$,

$$\Pr(M_1^n = m) = \Pr(B_{t_1}^n = m) \quad (\text{A14})$$

ALGORITHM 2. An equivalent alternative to Algorithm 1 in the case where we are applying the DEJMPS protocol. We adopt the notation of Algorithm 1 and use $B(\lfloor \frac{N}{2} \rfloor, t)$ to denote a binomial random variable with $\lfloor \frac{N}{2} \rfloor$ trials and a trial success probability of t .

```

A ← ⟨Φ+|ρ|Φ+⟩
B ← ⟨Ψ-|ρ|Ψ-⟩
C ← ⟨Ψ+|ρ|Ψ+⟩
D ← ⟨Φ-|ρ|Φ-⟩
while A < F' do
  t ← (A + B)2 + (C + D)2
  N ∼ B(⌊N/2⌋, t)
  A' ← A2+B2/t
  B' ← 2CD/t
  C' ← C2+D2/t
  D' ← 2AB/t
  A ← A'
  B ← B'
  C ← C'
  D ← D'
end while
ρ ← WF'

```

and

$$\mathbb{E}(M_1^n) = \left\lfloor \frac{n}{2} \right\rfloor t_1. \quad (\text{A15})$$

Now, we can derive a recurrence relation relating the distribution of M_k^n to the distribution of M_{k-1}^n by conditioning on how many pairs we will be able to purify after $k-1$ iterations of the protocol. For all $k \in \mathbb{N}$ and $(m, n) \in \{0, 1, 2, \dots\}^2$, by conditioning on the number of pairs distilled after $k-1$ iterations, we find that $\Pr(M_k^n = m)$ is given by

$$\sum_{m_{k-1}=0}^{\lfloor \frac{n}{2^{k-1}} \rfloor} \Pr(M_{k-1}^n = m_{k-1}) \Pr(B_{t_k}^{\lfloor \frac{m_{k-1}}{2} \rfloor} = m) \quad (\text{A16})$$

and

$$\begin{aligned} \mathbb{E}(M_k^n) &= \sum_{m_{k-1}=0}^{\lfloor \frac{n}{2^{k-1}} \rfloor} \Pr(M_{k-1}^n = m_{k-1}) \left\lfloor \frac{m_{k-1}}{2} \right\rfloor t_k \\ &= \mathbb{E}\left(\left\lfloor \frac{M_{k-1}^n}{2} \right\rfloor\right) t_k \\ &= \frac{t_k [\mathbb{E}(M_{k-1}^n) - \Pr(M_{k-1}^n \in O)]}{2}, \end{aligned} \quad (\text{A17})$$

where O is the set of positive odd integers.

As an example, let us use Eq. (A17) to find $\mathbb{E}(M_2^n)$ for all $n \in \{0, 1, 2, \dots\}$. We see that for all $n \in \{0, 1, 2, \dots\}$,

$$\begin{aligned} \Pr(M_1^n \in O) &= \sum_{m_1 \in \{1, 3, 5, \dots\}} \binom{\lfloor \frac{n}{2} \rfloor}{m_1} t_1^{m_1} (1-t_1)^{\lfloor \frac{n}{2} \rfloor - m_1} \\ &= \frac{1 - (1-2t_1)^{\lfloor \frac{n}{2} \rfloor}}{2}. \end{aligned} \quad (\text{A18})$$

Hence, for all $n \in \{0, 1, 2, \dots\}$,

$$\mathbb{E}(M_2^n) = \frac{t_2 \left[2 \lfloor \frac{n}{2} \rfloor t_1 + (1 - 2t_1)^{\lfloor \frac{n}{2} \rfloor - 1} \right]}{4}. \quad (\text{A19})$$

b. Pairs consumed to produce M' pairs

Alternatively, given $(k, m') \in \{0, 1, 2, \dots\}^2$, we might be interested in the number of pairs from our pool that will be consumed in the production of m' output pairs generated via k iterations of the DEJMPS protocol, $I_k^{m'}$. The distribution of this variable can also be calculated using the results of the previous section because it can only take even values and, for all $(k, m) \in \{0, 1, 2, \dots\}^2$ and $n \in \{0, 2, 4, \dots\}$, we have

$$\Pr(I_k^m = n) = \Pr(M_k^n \geq m) - \Pr(M_k^{n-1} \geq m), \quad (\text{A20})$$

where $\Pr(M_k^{-1} \geq m) = 0$. Alternatively, we could use the method of Appendix B 2, which is not restricted to the DEJMPS protocol.

Having shown how we might calculate the exact distribution of the number of initial pairs required to purify M' output pairs, we also now give a description of the asymptotic behavior of this distribution in the limit as M' goes to infinity. For all $k \in \{0, 1, 2, \dots\}$, as $M' \rightarrow \infty$, $\frac{I_k^{M'}}{M'}$ converges in distribution to a normal distribution with mean μ_k and variance $\frac{\sigma_k^2}{M'}$, where μ is the mean number of states the DEJMPS protocol with k iterations consumes to produce one output state and σ^2 is the variance in the number of states consumed to do so. Hence, for all k and large M' , $I_k^{M'}$ is approximately distributed as a normal random variable with mean $M' \mu_k$ and variance $M' \sigma_k^2$.

For $k \in \mathbb{N}$, to apply the DEJMPS protocol k times, we must produce two pairs by applying it $k - 1$ times and, if we fail to apply the DEJMPS protocol to them successfully, produce two more pairs by applying the DEJMPS protocol $k - 1$ times, and so on until we succeed. Letting J_k denote the number of pairs we produce by applying the DEJMPS protocol $k - 1$ times before ultimately succeeding, we have

$$\begin{aligned} \mu_k &= \sum_{n=1}^{\infty} P(J_k = 2n) \mathbb{E}(I_k^1 | J_k = 2n) \\ &= \sum_{n=1}^{\infty} 2t_k (1 - t_k)^{n-1} n \mu_{k-1} \\ &= \frac{2\mu_{k-1}}{t_k}. \end{aligned} \quad (\text{A21})$$

Then, by induction, we have, for all $k \in \{0, 1, \dots\}$,

$$\mu_k = \frac{2^k}{s_k}, \quad (\text{A22})$$

where $s_0 = 1$ and, for all $k' \in \mathbb{N}$, $s_{k'} = t_{k'} s_{k'-1} = \prod_{i=1}^{k'} t_i$.

Similarly, for all $k \in \{0, 1, 2, \dots\}$, we let $\sigma_k^2 = \text{Var}(I_k^1)$. Then, by the law of total variance, for every $k \in \mathbb{N}$, we have

$$\begin{aligned} \sigma_k^2 &= \mathbb{E}[\text{Var}(I_k^1 | J_k)] + \text{Var}[\mathbb{E}(I_k^1 | J_k)] \\ &= \frac{2\sigma_{k-1}^2}{t_k} + \frac{2^{2k} \text{Var}(\frac{J_k}{2})}{s_{k-1}^2} \\ &= \frac{2\sigma_{k-1}^2}{t_k} + \frac{2^{2k} (1 - t_k)}{s_k^2}. \end{aligned} \quad (\text{A23})$$

We can then see by induction that $\sigma_0^2 = 0$ and, for all $k \in \mathbb{N}$, we have

$$\sigma_k^2 = \frac{2^{k+1} \left[2^{k-1} - s_k \left(1 + \sum_{i=1}^{n-1} \frac{2^{i-1}}{s_i} \right) \right]}{s_k^2}. \quad (\text{A24})$$

APPENDIX B: CALCULATING $\Pr(X_{M'} = k, Y_{M'} = 1)$

1. The Markov chain method

One way of calculating $\Pr(X_{M'} = k, Y_{M'} = 1)$ for different values of k and M' is to characterize the process of repeatedly applying our protocol as a Markov chain in which each step corresponds to consuming one more state from our initial pool. Then, we find the probability distribution for the Markov chain's state after N steps, from which we can find the probability distribution for the number of purified pairs produced by our protocol and the protocol used to produce the final pair by the time it has consumed N pairs from the pool. Of course, the exact specifications of the Markov chain will depend on the protocol we are working with. We will now aim to make this method clear by looking at the Markov chain in the case in which we apply one of our interpolated DEJMPS protocols, although it could be straightforwardly adapted to general interpolated entanglement purification recurrence protocols.

Suppose that the two protocols we are interpolating between involve applying the DEJMPS protocol i and j times with $i < j$ and we apply the former protocol with probability p . Now, let the maximum number of states we could produce in this way from our initial N states be denoted by $T = \lfloor \frac{N}{2} \rfloor$. In total, our Markov chain will then have $(2T - 1)(2^i + 2^j + 2) + 2$ states, as follows.

Two states correspond to us having successfully produced T pairs. The first of these corresponds to having produced the T th pair by performing i iterations of the DEJMPS protocol and the second corresponds to having produced the T th pair by performing j iterations of the DEJMPS protocol. Both of these states are absorbing as there is no hope of us producing any more pairs using only N initial pairs.

Suppose we wish to apply i iterations of the DEJMPS protocol. Along the way, there are 2^{i-1} stages we must pass through that we must consume input pairs to move on from. The first of these is the stage where we have produced nothing. The second is the stage where we have produced one pair via one iteration of the DEJMPS protocol. The third is the stage where we have produced one pair via two iterations of the DEJMPS protocol. The fourth is the stage where we have produced one pair via two iterations of the DEJMPS protocol and one pair via one iteration of the DEJMPS protocol. The fifth is the stage where we have produced one pair via three iterations of the DEJMPS protocol. This continues until the 2^{i-1} th stage, where we have produced one pair via $i - 1$ iterations of the DEJMPS protocol, one via $i - 2$ iterations of the DEJMPS protocol, and so on, down to one pair via 1 iteration of the DEJMPS protocol.

Now, the DEJMPS protocol consumes two pairs from our initial pool each time it moves between two of the above stages. Therefore, to ensure that each transition in the Markov chain corresponds to using one more pair from the initial pool of states, we must, in fact, associate to each of the above stages

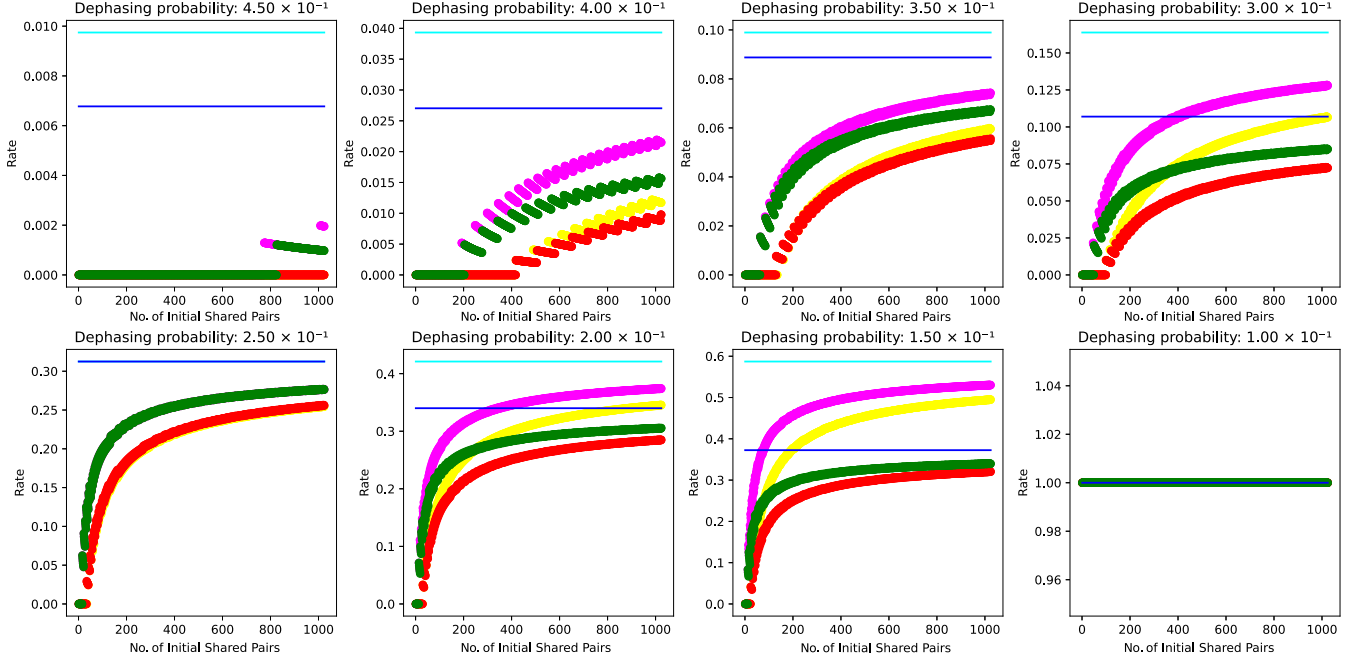


FIG. 6. The same as Fig. 3, except the initial states were generated by applying a dephasing channel to the chosen Bell state.

not one, but two states of the Markov chain, one corresponding to being at that stage and another which transitions into the former with probability 1. Associated with these stages, then, we have a total of 2^i states in our Markov chain.

On top of this, for $n \in \{0, 1, 2, \dots, T-1\}$, we need states from which we transition to a state corresponding to having produced our $n+1$ th purified pair. In fact, we must have two such states for each n , one corresponding to us being about to produce the $n+1$ th pair via i iterations of the DEJMPS protocol and one corresponding to us being about to produce the $n+1$ th pair via j iterations of the DEJMPS protocol. This gives us $2^i + 2^j + 2$ states corresponding to having produced n purified pairs and being in the process of producing our $n+1$ th. However, to keep track of whether our most recent pair was produced via i iterations or j iterations of the DEJMPS protocol, we actually need twice as many states, unless $n = 0$.

In total, then, we have, as claimed, $(2T-1)(2^i + 2^j + 2) + 2$ states in our Markov chain. Each state corresponds to the two parties having produced a particular number of purified pairs, being at a certain stage in the production of the next pair and having produced their most recent state via a certain number of DEJMPS iterations. Each transition corresponds to one more pair being consumed from the pool of initial states.

The transition probabilities of the Markov chain are determined by the success probabilities of different iterations of the DEJMPS protocol. The probability distribution for the initial state reflects the fact that we start by trying to produce a state via i iterations of the DEJMPS protocol with probability p_i and by trying to produce a state via j iterations of the DEJMPS protocol with probability $p_j = 1 - p_i$. Then, the probability distribution for the state of the Markov chain after N steps allows us to calculate $\Pr(X_{M'} = k, Y_{M'} = 1)$ for different values of k and M' .

2. The iterative method

We will now describe an alternative method which is sometimes faster than the Markov chain method described above. Given $n \in \{0, 1, 2, \dots\}$, imagine we are trying to purify a single pair from a pool of n initial pairs using our interpolated protocol and let $Y_{1,n} = 1$ if we succeed, and $Y_{1,n} = 0$ otherwise. Moreover, imagining that we have an infinite pool of initial states, for $M' \in \{0, 1, 2, \dots\}$, let $I^{M'}$ denote the number of states we consume in the process of distilling M' pairs. Then, for every $M' \in \mathbb{N}$ and $k \in \{1, 2, \dots, K\}$, we can calculate $\Pr(Y_{M'} = 1, X_{M'} = k)$ as

$$p_k \sum_{n=0}^N \Pr(I^{M'-1} = n) \Pr(Y_{1,N-n} = 1 | X_1 = k). \quad (\text{B1})$$

We might calculate $\Pr(Y_{1,N-n} = 1 | X_1 = k)$ for different values of k and n using the Markov chain method described above. Then, we note that for every $M' \in \mathbb{N}$ and $n \in \{0, 1, 2, \dots\}$, we can calculate $\Pr(I^{M'} = n)$ as

$$\sum_{n'=0}^{n-1} \Pr(I^{M'-1} = n') \Pr(I^1 = n - n'), \quad (\text{B2})$$

and, for every $n' \in \mathbb{N}$,

$$\Pr(I^1 = n') = \Pr(Y_{1,n'} = 1) - \Pr(Y_{1,n'-1} = 1). \quad (\text{B3})$$

Therefore, we can iterate over the values of M' we must consider and calculate the distribution of $I_{M'}$ for each of them, allowing us to find M .

APPENDIX C: ADDITIONAL FINITE-SIZE PLOTS

Figures 3 and 4 of the main text showed the performance of DEJMPS and interpolated DEJMPS protocols when our initial states are produced by applying a depolarizing channel

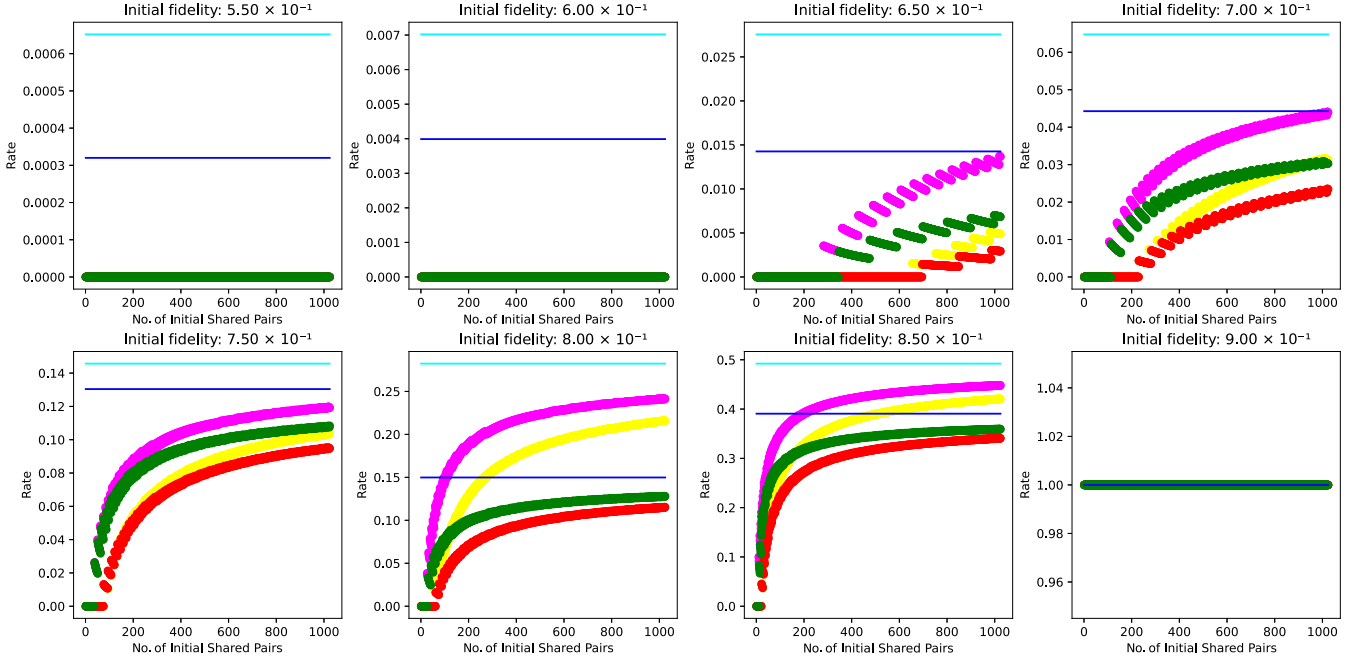


FIG. 7. The same as Fig. 3, except the initial states were generated by applying a Pauli channel where, conditional on the channel affecting the state, a phase flip is applied with probability $\frac{1}{2}$, a bit flip with probability $\frac{1}{3}$, and a bit and phase flip with probability $\frac{1}{6}$ to the chosen Bell state.

to one-half of a Bell pair. As further examples, we show in Figs. 6–8 the corresponding results for examples of other standard qubit channels, namely, dephasing channels, Pauli channels, and amplitude damping channels. Note that in all of these cases, we assume that before applying the very first iteration of the DEJMPS protocol, whether or not they are

interpolating between different numbers of iterations, Alice and Bob apply local unitary rotations to permute their Bell states so as to maximize the Bell fidelity of the output states upon success of one iteration of the DEJMPS protocol. This ensures our results are invariant under a relabelling of the Bell states.

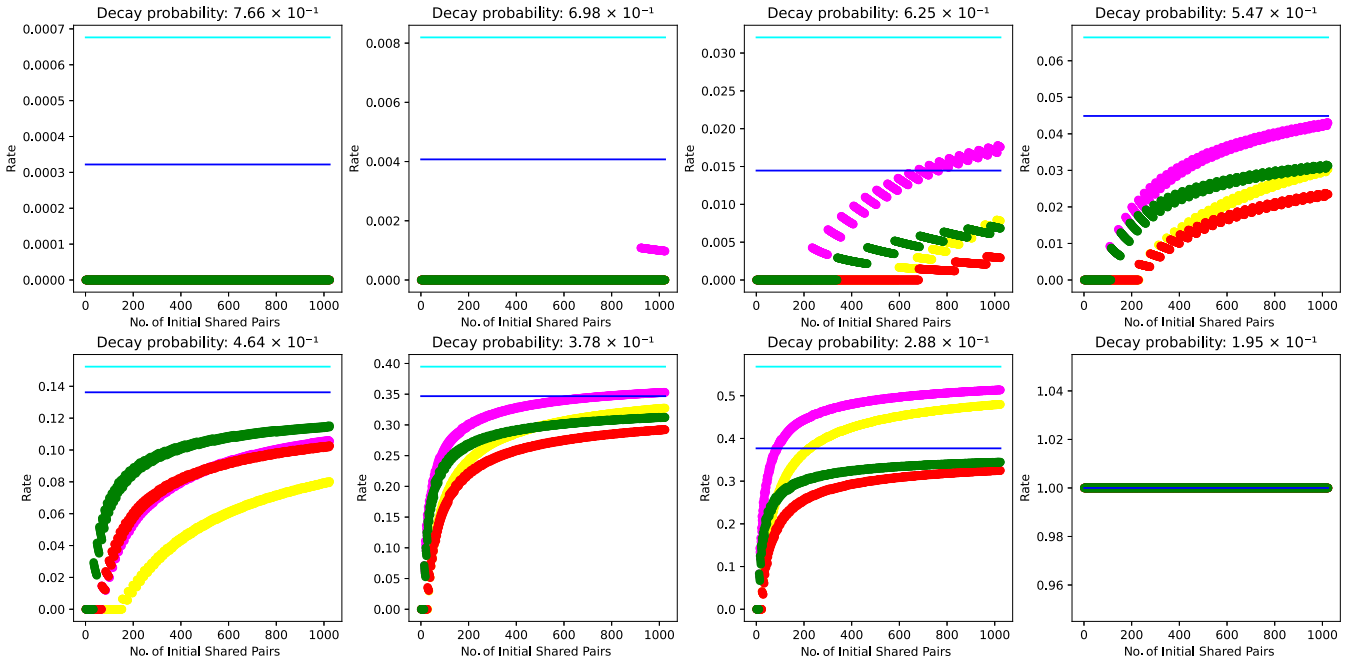


FIG. 8. The same as Fig. 3, except the initial states were generated by applying an amplitude damping channel to one-half of the chosen Bell state.

- [1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [2] C. H. Bennett and S. J. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, *Phys. Rev. Lett.* **69**, 2881 (1992).
- [3] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014).
- [4] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, *et al.*, Advances in quantum cryptography, *Adv. Opt. Photon.* **12**, 1012 (2020).
- [6] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).
- [7] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, *Rev. Mod. Phys.* **81**, 865 (2009).
- [8] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Mixed-state entanglement and quantum error correction, *Phys. Rev. A* **54**, 3824 (1996).
- [9] Á. G. Iñesta and S. Wehner, Performance metrics for the continuous distribution of entanglement in multiuser quantum networks, *Phys. Rev. A* **108**, 052615 (2023).
- [10] C. Harney and S. Pirandola, Practical routing and criticality in large-scale quantum communication networks, *Phys. Rev. Res.* **7**, 043168 (2025).
- [11] F. Rozpędek, T. Schiet, L. P. Thinh, D. Elkouss, A. C. Doherty, and S. Wehner, Optimizing practical entanglement distillation, *Phys. Rev. A* **97**, 062333 (2018).
- [12] 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).
- [13] R. F. Werner, Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, *Phys. Rev. A* **40**, 4277 (1989).
- [14] 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).
- [15] V. Vedral and M. B. Plenio, Entanglement measures and purification procedures, *Phys. Rev. A* **57**, 1619 (1998).
- [16] K. Audenaert, J. Eisert, E. Jané, M. B. Plenio, S. Virmani, and B. De Moor, Asymptotic relative entropy of entanglement, *Phys. Rev. Lett.* **87**, 217902 (2001).
- [17] S. Pirandola, End-to-end capacities of a quantum communication network, *Commun. Phys.* **2**, 51 (2019).
- [18] E. Shchukin, F. Schmidt, and P. van Loock, Waiting time in quantum repeaters with probabilistic entanglement swapping, *Phys. Rev. A* **100**, 032322 (2019).
- [19] N. Lo Piparo, M. Hanks, K. Nemoto, and W. J. Munro, Aggregating quantum networks, *Phys. Rev. A* **102**, 052613 (2020).
- [20] C. Harney and S. Pirandola, Analytical methods for high-rate global quantum networks, *PRX Quantum* **3**, 010349 (2022).
- [21] C. Harney, A. I. Fletcher, and S. Pirandola, End-to-end capacities of hybrid quantum networks, *Phys. Rev. Appl.* **18**, 014012 (2022).
- [22] N. Lo Piparo, W. J. Munro, and K. Nemoto, Quality of service in aggregated quantum networks, [arXiv:2501.18846](https://arxiv.org/abs/2501.18846).
- [23] W. Dür and H. J. Briegel, Entanglement purification and quantum error correction, *Rep. Prog. Phys.* **70**, 1381 (2007).