# Efficient entanglement purification based on noise guessing decoding

André Roque[1], Diogo Cruz[1,2], Francisco A. Monteiro[2,3], and Bruno C. Coutinho[2]

[1]Instituto Superior Técnico, Universidade de Lisboa, Portugal

[2]Instituto de Telecomunicações, Portugal

[3]ISCTE - Instituto Universitário de Lisboa, Portugal

In this paper, we propose a novel bipartite entanglement purification protocol built upon hashing and upon the guessing random additive noise decoding (GRAND) approach recently devised for classical error correction codes. Our protocol offers substantial advantages over existing hashing protocols, requiring fewer qubits for purification, achieving higher fidelities, and delivering better yields with reduced computational costs. We provide numerical and semi-analytical results to corroborate our findings and provide a detailed comparison with the hashing protocol of Bennet et al. Although that pioneering work devised performance bounds, it did not offer an explicit construction for implementation. The present work fills that gap, offering both an explicit and more efficient purification method. We demonstrate that our protocol is capable of purifying states with noise on the order of 10% per Bell pair even with a small ensemble of 16 pairs. The work explores a measurement-based implementation of the protocol to address practical setups with noise. This work opens the path to practical and efficient entanglement purification using hashing-based methods with feasible computational costs. Compared to the original hashing protocol, the proposed method can achieve the same fidelities with a number of initial resources up to one hundred times smaller. The proposed method seems well-fit for future quantum networks with a limited number of resources and entails a relatively low computational overhead.

## 1 Introduction

Entanglement is considered a valuable resource for numerous applications, spanning from secure communication and scalable quantum networks [1, 2, 3], to precision measurement and timing, entanglement is a versatile resource for various quantum technologies [4], including quantum key distribution [5], state teleportation [6], distributed quantum computation [7, 8] and distributed sensing and metrology [9]. In experimental settings, notable progress has been made in establishing entanglement between different components, as evidenced by successful demonstrations in various systems, including trapped ions [10, 11, 12], NV centers [13, 14], neutral atoms [15, 16], and superconducting circuits [17, 18].

However, entanglement is susceptible to several detrimental factors. Foremost among these is decoherence, resulting from interactions with the environment or thermal fluctuations that cause a quantum system to lose its coherent superposition, ultimately leading to the breakdown of entanglement. Quantum errors, resulting from imperfect gates or measurements, can also disrupt the intricate entangled states [4, 19, 20]. It is worth noting that the fidelity of the generated Bell pairs currently stands at approximately 10%, whereas the noise stemming from local gates and measurements is considerably lower, often falling below 1%.

Unless actively corrected, the accumulation of these error processes will inevitably destroy any initial entanglement. Purification protocols (PP) are a possible solution for quantum networks that has been extensively studied in the context of quantum repeaters [21, 22, 23] and is a crucial component of entanglement routing protocols [24, 25, 26].

Bipartite entanglement purification encompasses a broad category of techniques aimed at acquiring high-fidelity copies of Bell states that are jointly held by two parties [27, 28, 29, 30, 8, 31, 32, 33, 34]. This is achieved by using local quantum operations and classical communication (LOCC) on an initially shared ensemble of entangled particles. Purification protocols are designed to operate on two or more ensembles of noisy entangled quantum states. The primary goal is to generate a reduced number of states with higher fidelity. Purification protocols can be repeatedly applied to the refined states in order to achieve states with even higher levels of purification. Protocols such as the *IBM* protocol [28, 27] or the *Oxford* protocol[29], which fall into the category of recurrence protocols [28, 33], achieve this only probabilistically. Although the recursive application of these protocols leads to convergence towards maximally entangled states, their probabilistic nature requires multiple executions to successfully obtain a purified state. Since a single successful application only results in marginal improvements to the state's fidelity, the need to repeat these protocols several times to achieve sufficiently purified states leads to an exponential increase in the resources required. Another approach to purification is provided by hashing protocols [27, 31, 32, 35]. Hashing protocols operate on a large ensemble of Bell pairs to deterministically produce a smaller number of purified pairs, whose fidelity can be arbitrarily high. However, traditional hashing protocols can be highly computationally demanding. Moreover, they often require hundreds of pairs to achieve purification and thousands of pairs to become efficient.

In this work, we introduce a novel one-way bipartite purification protocol, inspired by the recently developed decoding technique for quantum error correction codes (QECCs) known as quantum random additive noise decoding (QGRAND) [36, 37]. QGRAND was initially proposed by [36] for quantum random linear codes and latter has been used to decode other QECCs in [37]. QGRAND takes advantage of the noise statistics and provides an efficient decoding process. Employing a hashing-based approach, our protocol represents a substantial advancement over the hashing protocol [27], with the distinguished advantages: i) decreased qubit demand for purification, ii) achievement of heightened fi-

delities for equal initial ensembles (maintaining equal qubit count and noise conditions), iii) augmented yields for smaller ensembles, iv) attainment of computationally feasible costs.

Hashing protocols, while efficient, encounter a significant practical limitation: their viability diminishes in real-world scenarios with noisy local operations and measurements. Even some minimal noise disrupts these protocols due to global operation requirements and the cumulative entropy increase from noisy operations. Building upon the concepts introduced by [38, 39], we also put forward a measurement-based [40, 41] version of our protocol and provide numerical results regarding the protocol's potential noise tolerance and its impact on the performance.

This paper is organized as follows. In Section 2 we introduce a classical error decoding procedure along with its quantum equivalent and explain how a purification protocol can be obtained from a quantum error correction code. In Section 3 our purification protocol is presented and some results about its performance are provided. Section 4 is devoted to establishing a comparison between our protocol and the hashing protocol. In Section 5 we present a measurement-based version of our protocol before some conclusions being presented in Section 6.

## 2 Background

### 2.1 QGRAND

While traditional decoding algorithms of classical error correction codes primarily concentrate on detecting error patterns through codeword analysis, a recent innovative proposal has surfaced, that focuses on "decoding" the noise; the algorithm was named GRAND (guessing random additive noise decoding) [42]. This algorithm redirects the decoding process toward discovering the error pattern that affected a transmitted codeword rather than focusing on the codebook.

Consider a finite alphabet of symbols $\mathcal{A}$. Let $\mathcal{C}$ be a discrete communication channel with a block of $n$ input symbols denoted by $X^n$, which are subjected to a noise block $N^n$, also composed of $n$ symbols. Denoting the action of the channel on the input block by $\oplus$, the output block of $n$ symbols is $Y^n = X^n \oplus N^n$. Assuming that the channel's action is invertible, let $\ominus$ denote the inverse function, so that the inputs can be

written as $X^n = Y^n \ominus N^n$. Suppose that this channel is employed for communication between a sender and a receiver, both of whom share a codebook $\mathcal{B}^{(n,M_k)}$ containing $M_k$ codewords, each of which is made of $n$ symbols taken from the alphabet $\mathcal{A}$. Each particular random set of $n$ symbols forming a block $N_i^n$ is said to be a *noise pattern*, which occurs with some known probability $P(N_i^n)$, according to the noise statistics. GRAND operates by successively testing noise patterns (in decreasing order of their probability) until finding one that generates a valid codeword, that is: $X^n = Y^n \ominus N_i^n$, such that $X^n \in \mathcal{B}^{(n,M_k)}$. When this is true, then $X^n = Y^n \ominus N_i^n$ is accepted as the decoded data. Otherwise, the algorithm moves to the next most likely error pattern. It was shown in [42] that this decoding procedure returns the maximum likelihood solution, i.e.,

$$b_i^{(n,M_k)} = \underset{b_i^{(n,M_k)} \in \mathcal{B}^{(n,M_k)}}{\operatorname{argmax}} \{P(N^n = Y^n \ominus b_i^{(n,M_k)})\}. \tag{1}$$

As mentioned, the probabilities for each noise sequence can be estimated using the specific noise statistics of the channel.

Quantum GRAND (QGRAND) is a recently proposed decoder that adapted the classical GRAND to a QEC setup [36]. It allows to decode quantum random linear codes (QRLC) with the distinguished advantages of maximizing the use of information about the noise while providing a simple encoding/decoding process. QGRAND was defined for stabilizer codes and leverages noise statistics to establish a recovery procedure similar to the one used by GRAND. Consider an initial setup of some $k$-qubit state that one wants to protect against some source of noise. The encoding is generated by randomly choosing two-qubit Clifford gates randomly selected and applied to the $n$ qubit system ($k$ initial qubits plus $n-k$ additional qubits in the state $|0\rangle$). The target pairs of such gates are also randomly chosen, assuming that all-to-all connectivity between the $n$ qubits is possible. This encoding has been shown to be robust to depolarizing noise provided that the number of gates used is large enough.

QGRAND can be done implemented in slightly different ways. In the following, we describe the approach taken in the present work. Let $\mathcal{N}$ be the noise statistics of the error source considered. Since the circuit (composed of both the encoder and the stabilizers) is composed of Clif-

ford gates, it is possible to classically simulate it in a efficient manner. By doing so, we can pre-compute a set $\mathcal{N}_P \subseteq \mathcal{N}$ of error patterns. A set $\mathcal{N}_J \subseteq \mathcal{N} \setminus \mathcal{N}_P$ of error patterns whose syndrome needs to be computed on the fly can also be considered, at the cost of some extra processing time. For each syndrome, only the most likely error pattern is stored, allowing one to establish a one-to-one correspondence between each syndrome and the set of correctable error patterns. Such correspondences between syndromes and error patterns can be adjusted to different error models. Similarly, this is done in classical communications using GRAND: the testing order of the error patterns can be computed in advance for a number of different channel conditions and stored in tables. Those tables can be selected on the fly, according to varying channel conditions [43]. Once the syndrome has been extracted, a correction attempt is made. The correction process should be reversible, as the encoding, syndrome measurement, and decoding procedures can fail. In that case, the applied correction is reversed and another correction procedure is tried. This process is repeated until an error pattern that leads to a valid codeword is found.

## 2.2 Equivalence between Quantum Error Correction and One-Way Purification Protocols

Both QEC and purification protocols (PP) are strategies for managing the challenges of noisy quantum communication that are intricately interconnected. This relation was first observed in the early exploration of entanglement purification in [27, 44], where a general methodology has been introduced to construct QECCs from one-way entanglement purification protocols. In cases where a code employs $n$ physical qubits to encode $k$ logical qubits ($k < n$), it becomes feasible to devise a purification protocol that makes use of $n$ copies of two-qubit states and produces $k$ pairs with enhanced fidelity. The remaining $n-k$ pairs undergo measurement for revealing information concerning the obtained pairs [45, 44].

To understand the main idea, let us consider a noisy channel $\mathcal{C}$, established between two parties, A (Alice) and B (Bob), to be used for distributing $n$ perfect Bell pairs. We denote the four Bell basis states as $\{|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)\}$ and consider a Bell pair to be

the state $|\phi^+\rangle$, although any other of the 4 states could be considered. Although the construction can be generalized for any QEC code, we shall consider a stabilizer code for simplicity. For stabilizer codes, one can consider that the encoding and decoding operations consist of unitary operations $U_{\text{enc}} = U$ and $U_{\text{dec}} = U_{\text{enc}}^{-1} = U^{-1}$. In order to obtain a purification protocol, we start by noticing the fact that performing any unitary transformation (and this holds for any linear transformation) at B is equivalent to performing the transpose of that same transformation at A [27], that is,

$$U_A^T \otimes I_B \, |\phi_{AB}^+\rangle^{\otimes n} = I_A \otimes U_B \, |\phi_{AB}^+\rangle^{\otimes n}. \quad (2)$$

This allows us to perform encoding operations locally by A, and decoding to be performed locally by B. The channel affects the ensemble with some noise, which we shall assume to be a Pauli string $E$, and a mixed state

$$\rho = \mathcal{C}(|\phi_{AB}^+\rangle^{\otimes n}) \quad (3)$$
$$= (1-p)(|\phi_{AB}^+\rangle\langle\phi_{AB}^+|)^{\otimes n} + pE(|\phi_{AB}^+\rangle\langle\phi_{AB}^+|)^{\otimes n}E^\dagger, \quad (4)$$

is obtained. In order to purify $\rho$, Alice starts by applying the encoding on her qubits, projecting them into a $+1$ eigenspace defined by the code. Now Alice can perform measurements on $n - k$ of her qubits to obtain information about the ensemble $\rho$. Let $\{P_i\}$ be the set of $2^{n-k}$ projectors defined by the code. Since each projector $P_i$ either commutes or anticommutes with any Pauli string, we have that

$$(P_i \otimes I)(I \otimes E)|\phi^+\rangle^{\otimes n} = \pm(I \otimes E)(P_i \otimes I)|\phi^+\rangle^{\otimes n}. \quad (5)$$

Using Equation (2), we obtain that

$$(P_i^2 \otimes I)(I \otimes E)|\phi^+\rangle^{\otimes n} = \pm(I \otimes E)(P_i \otimes P_i^T)|\phi^+\rangle^{\otimes n}. \quad (6)$$

Hence, every time Alice applies a projector $P_i$ on her qubits, Bob's qubits are projected through $P_i^T$. After obtaining information about the measurements, Alice might restore her qubits to the $+1$ eigenspace defined by the encoding, although this is not strictly necessary if one "adapts" the measurement information to the projection that was performed. The measurement information is transmitted to Bob through a classical channel, allowing him to adjust the correction operation

required to return his $n - k$ qubits to the code space. Finally, decoding operations are applied so that a state with higher fidelity is obtained. Thus, a purification protocol was obtained using only LOCC.

This construction can be summarized as follows:

1. Generate $n$ copies of a maximally entangled bipartite state and distribute them between A and B.

2. Apply locally on A the coding operation $U^T$ and Pauli measurements on $n - k$ of the $n$ qubits. The information about the measurements is sent classically to B.

3. Extract the syndrome on B. Apply on B the correction operation determined from that measured syndrome.

4. Apply the decoding operation $U^{-1}$ on B.

In the end, one obtains $k$ Bell pairs shared between Alice and Bob, while the remaining $n - k$ pairs are discarded. The $k$ purified pairs have higher fidelity than the initial $n$ shared pairs.

## 2.3 Noise modeling

In order to evaluate the performance of the proposed protocol, we model both coherent and decoherence errors in bipartite states through a depolarizing channel. A **depolarizing channel** $\mathcal{D}$ is a quantum channel that maps a quantum state onto a mixture of the original state and a maximally mixed state. If $\rho$ represents the density matrix of some state, the action of $\mathcal{D}$ on qubit $i$ of the state $\rho$ is naturally described by

$$\mathcal{D}_p^i(\rho) = (1-p)\rho + \frac{p}{3}(X_i\rho X_i + Y_i\rho Y_i + Z_i\rho Z_i), \quad (7)$$

where $p$ is the depolarization probability, that can be interpreted as an error probability, and $X, Y$ and $Z$ are the Pauli matrices.

Using this channel to model noise requires the following assumptions: i) the qubit errors that affect one qubit are independent from the errors that affect the remaining system, ii) single-qubit errors ($X$, $Y$ and $Z$) are equally likely and iii) all qubits belonging to the same system have the same error probability $p$. Throughout this work, we will refer to noise of this form as local depolarizing noise (LDN). Applying a depolarizing channel to either the first or the second qubit of

a Bell pair results in a state known as a Werner state, $W_F$, [46] with fidelity $F = \mathcal{F}(W_F, |\phi^+\rangle) = \langle\phi^+|W_F|\phi^+\rangle = 1 - p$. This enables us to express this state in terms of its fidelity:

$$W_F = \mathcal{D}_p^2(|\phi^+\rangle\langle\phi^+|) = \mathcal{D}_p^1(|\phi^+\rangle\langle\phi^+|)$$
$$= \frac{1-F}{3}I + \frac{4F-1}{3}|\phi^+\rangle\langle\phi^+|, \qquad (8)$$

meaning that the obtained state can be interpreted as a classical mixture of the four Bell states. Notice that the qubit to which the channel is applied is irrelevant.

Werner states hold significance in the examination of random two-qubit states, as the conversion of any bipartite mixed state to a Werner state is attainable through an irreversible process termed "twirl". This procedure involves the application of independent and random rotations from the $SU(2)$ group to each particle within the pair [27, 47].

## 2.4 Measurement Based Quantum Computation

The measurement-based quantum computation (MBQC) [40, 41, 48] is a model of quantum computation where computations are performed through measurements on an initial resource state, rather than using gates. It provides a universal framework for performing quantum computations utilizing only single-qubit measurements.

One of the most extensively studied and promising approaches in MBQC involves using as resource state a highly entangled state known as *the cluster state*. These states can be generated in lattices of qubits through Ising type interactions [41, 40]. This process generates a highly entangled state with the topology of a 2D square lattice, commonly referred to as a cluster state, as mentioned earlier. These cluster states are a specific type of state from a class of states that can be represented using graphs, known as graph states. To define a graph state, consider a graph $G = (V, E)$ with a finite set of vertices $V$ and edges $E \in V \times V$. The graph state associated with $G$ is defined as

$$|G\rangle = \prod_{(a,b)\in E} CZ_{a,b}\left(\bigotimes_{a\in V}|+\rangle^a\right), \qquad (9)$$

with $CZ_{a,b}$ representing the controlled-$Z$ gate on qubits $a$ and $b$ and $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$. Some graph operations such as vertex deletion and edge addition or deletion have a physical correspondence with operations on the graph state. Keeping this in mind, two-dimensional cluster states can be defined as graph states obtained from a graph with the topology of a square lattice. By systematically choosing the measurement sequence and bases, any arbitrary quantum circuit can, in principle, be simulated utilizing only single-qubit measurements on the cluster state [40].

This paradigm of quantum computation is especially relevant for the development of fault-tolerant quantum computation [49, 50, 51, 52]. Moreover, experimental realizations of multiparty purification protocols in optical lattices, aimed at improving the fidelity of cluster states, have already been presented [53, 35].

# 3 Proposed Protocol

## 3.1 Protocol Overview

Following the construction proposed in Section 2.2, we now present a purification protocol developed through an adaptation of QGRAND, which we will refer to as Purification GRAND (PGRAND). Let us assume an initial setup of $n$ Bell pairs shared between Alice and Bob through a noisy quantum channel $\mathcal{C}$. At the end of the protocol procedures, both parties will share $k$ Bell pairs with higher fidelity. The protocol is depicted in Figure 1 and can be summarized by the following steps:

1. Apply a random encoding on Alice's $n$ qubits. Share the encoding information with Bob.

2. Perform single-qubit measurements in the computational basis on $n - k$ of Alice's $n$ qubits, followed by the classical transmission of the measurement outcomes to Bob.

3. With the information about the encoding, simulate the stabilizer circuit and determine the stabilizers for the qubits which were initially entangled with the measured ones.

4. Using the stabilizer information, compute the syndromes associated with the most likely errors. Construct a lookup table (LUT) containing the most likely errors associated to each syndrome.

5. Measure the syndrome using all the determined $n - k$ stabilizers.

6. Update the syndrome obtained with the information sent by Alice.

7. Use a noise guessing approach to identify the error pattern and apply the recovery procedure on the corrupted state.

8. Apply the decoding at B. Discard the measured pairs and keep the $k$ remaining ones.

### 3.1.1 Encoding

The protocol starts by applying an encoding on Alice's qubits, composed of randomly selected 2-qubit Clifford gates. To do so, one can generate a random tensor product of Clifford gates, transpose it, and apply it to the initial state. The information about the original tensor product has to be sent classically to Bob. Alternatively, both parties could previously agree on the random encoding to be used. To obtain a highly performant code, $0.14n \log^2(n)$ Clifford gates are required on average [36]. As most of the gates can be applied in parallel, the encoding has a circuit depth of $\mathcal{O}\left(\log^3(n)\right)$. We remark that, while the encoding should be generated randomly, the same encoding can be applied for subsequent uses, provided that the total number of pairs remains the same. By reusing the code, we may skip steps 3 and 4, which are the most computationally heavy of the entire protocol. This reuse significantly reduces the computational overhead associated with generating new LUTs for each round. Additionally, even when there are variations in the noise parameters, the precomputed LUTs can remain effective if these variations are minimal. For more complex changes in error rates across different qubits, the existing LUTs may still be employed, albeit with potentially suboptimal decoding performance. Precomputing LUTs for different anticipated noise channels or employing robust codes that are adaptable to on-the-fly modifications can further mitigate the computational demands and ensure efficient error correction. This flexibility and adaptability in the LUT management underscore the feasibility of our approach in practical quantum error correction scenarios.

### 3.1.2 Determining the stabilizers

After the qubits are generated and subjected to noise, the process of gathering information about the state is limited to local operations. To overcome that issue, we can still make use of local stabilizers on Bob's qubits, but it is required that the respective entangled qubits on Alice's side be measured. After some initial state $|\psi\rangle_I$ has been encoded with an unitary transformation $U$, the stabilizers of the encoded state $|\psi\rangle_F = U|\psi\rangle_I$ can be obtained by evolving the initial stabilizers through the encoding, that is, if $S_I$ is a stabilizer of the initial state, then $S_F = U S_I U^{-1}$ is a stabilizer of the final encoded state since

$$S_F|\psi\rangle_F = (US_I U^{-1})U|\psi\rangle_I = US_I|\psi\rangle_I = \quad (10)$$
$$U|\psi\rangle_I = |\psi\rangle_F.$$

Although the proposed protocol performs the measurements after the encoding operation, given Equation (2) it is possible to assume that, for those qubits that are being measured, the measurements on Alice's side are performed before the encoding operation on Bob's side. Hence, we can focus our attention in evolving the stabilizers of the measured states. If the initial state is a Bell pair, the operators $S_{M=0} = I_A \otimes Z_B$ and $S_{M=1} = I_A \otimes (-Z)_B$ are able to stabilize locally on Bob's side the states obtained after a $Z$-measurement of a Bell pair, $|00\rangle_{AB}$ and $|11\rangle_{AB}$, respectively. Hence, each stabilizer can be evolved through $U^T$, that is, we obtain the stabilizers $S'_{M=0} = I_A \otimes ((U^T)^{-1}ZU^T)_B$ and $S'_{M=1} = I_A \otimes (-(U^T)^{-1}ZU^T)_B$. Since $S'_{M=1} = -S'_{M=0}$, changing the stabilizers according to the measurement is equivalent to performing a classical bit-XOR operation of the syndrome with the measurement result.

According to the Gottesman-Knill theorem [54, 55], for a quantum circuit of $n$ qubits, updating the stabilizer specification requires $\mathcal{O}(n)$ time for each Clifford gate in the circuit. The encoding operation made by $U$ is a stabilizer circuit, and thus it has depth $\mathcal{O}\left(\log^3(n)\right)$, determining the stabilizers requires $\mathcal{O}(n \log^3(n))$ time.

### 3.1.3 Noise guessing and correction

Bob can efficiently simulate the encoding circuit and build a parity check matrix to map each error pattern to the respective syndrome. With the
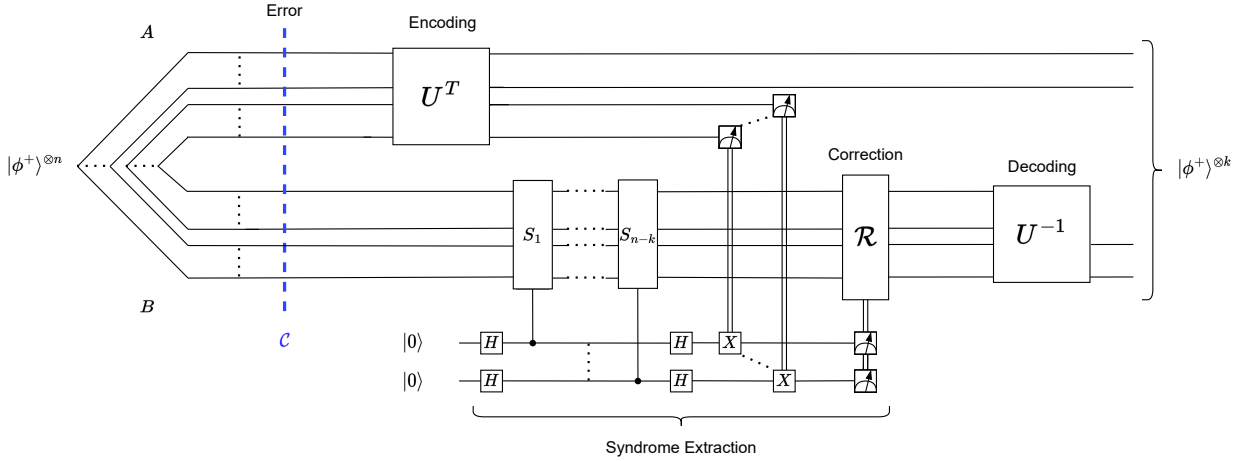
Figure 1: Quantum circuit for the PGRAND applied to $n$ Bell pairs distributed between Alice (A) and Bob (B) in order to obtain $k$ purified pairs. The error is described by a quantum channel $\mathcal{C}$. In the circuit, the measurements performed by Alice are depicted changing the ancilla qubits, but in reality only a virtual syndrome update needs do be done. The same goes to the recovery procedure: if it consists only of Pauli strings, then $\mathcal{R}$ can be performed virtually (in software), without the need to apply extra gates.

noise statistics, Bob can determine the most likely error associated with a syndrome, so that whenever that syndrome is measured, the recovery procedure is done such that the most likely error is selected and corrected.

Since the possible number of error patterns increases exponentially on the number of qubits for most of the error models, Bob might only be able to precompute the syndromes associated with a fraction of the total possible errors. The number of syndromes that are computed should be chosen according to the initial fidelity of the pairs, the number $n$ of qubits and the required final fidelity. This approach will save resources and make the computation possible at the cost of a decrease in performance. The computation of the syndrome of each error pattern involves multiplying a $2n$-bit array representing the error with a $(2n) \times (n-k)$ matrix representing the stabilizers, requiring $\mathcal{O}(n^\omega)$ time. In practice, this procedure can be efficiently parallelized. When aiming to correct the $N$ error patterns with a weight up to $t$, we may take advantage of previously computed syndromes for lower weight errors to achieve a $\mathcal{O}(Nn)$ computation cost in obtaining the syndrome table.

It is important to note that this step is the primary limiting factor in what regards the classical computational cost, just like in the case of the hashing protocol [27, 30], with the circuit simulation playing a negligible role in the overall cost.

After mapping each error pattern with a syn-

drome, only the most likely error pattern associated to each syndrome needs to be stored, and the remaining can be discarded. The number of possible error patterns is $N$ and $S = 2^{(n-k)}$ is the number of available syndromes. Whenever a syndrome is extracted, all that is needed to identify the recovery procedure is a linear search on a table of at most size $T = \min\{N, S\}$, which requires $\mathcal{O}(Tn)$ space and time to store the syndromes and perform a search.

### 3.1.4 Decoding

As outlined in the protocol's presentation, the decoding entails reversing the encoding operation and discarding the measured qubits. Nevertheless, since only Clifford gates are used in the decoding, a virtual execution prior to the recovery operation is also feasible. In that case, all that needs to be done is to make the appropriate adjustments to the recovery operation. Both the decoding (except for the discarding of pairs) and the correction involve Clifford gates, so all of this can be performed classically through software [56].

Overall, for a single PGRAND application that uses $n$ Bell pairs to obtain $k$, the overhead per pair, that is, the number of qubits that are spent in the use of the protocol, is given by $3(n/k - 1)$ (due to the $2(n - k)$ qubits that are required to be measured and the $n - k$ qubits that are used as ancillas). For the syndrome extraction, each of the $n - k$ stabilizer applications is composed by,

Accepted in ⟨ ⟩uantum 2024-09-04, click title to verify. Published under CC-BY 4.0.

7

on average, $3n/4$ CNOT gates and $7n/2$ single-qubit gates, requiring a total of $\mathcal{O}(n^2)$ gates.

## 3.2 Results

Consider a setup of Werner states with initial fidelity $F_i = 1 - p$, with $p$ being the parameter of a depolarizing channel. Define $\mathcal{W} : \mathcal{E} \to \mathbb{N}$ to be the map between each error pattern $E_i \in \mathcal{E}$ and its weight. Let $N_w$ be the number of possible error patterns with weight $w$ and $N_{\leq w}$ the number of possible error patterns with equal or less weight than $w$. For depolarizing noise these quantities are given by

$$N_w = \binom{n}{w} 3^w, \quad N_{\leq w} = \sum_{i=0}^{w} N_i. \quad (11)$$

Let $f_{\mathrm{Bin}(n,p)}(w)$ be the binomial probability mass function. For each error pattern $E_i$, we have that

$$P(\{E_i\}|\mathcal{W}(E_i) = w) = \frac{f_{\mathrm{Bin}(n,p)}(w)}{N_w} \quad (12)$$
$$= \left(\frac{p}{3}\right)^w (1-p)^{n-w},$$

from which we immediately conclude that $P(\{E_i\}) \geq P(\{E_j\}) \Rightarrow \mathcal{W}(E_i) \leq \mathcal{W}(E_j)$ for any $E_i, E_j \in \mathcal{P}^n$ (as long as $p < 3/4$).

The approach of correcting the most likely errors in this noise scenario prioritizes the correction of lower-weight errors. That is, for a set of error patterns that share the same syndrome, the protocol considers the error that has occurred to be the error pattern with the lowest weight.

Under the assumption that any correctly identified error can be completely corrected, it is useful for the analysis of the protocol to define the correctable fraction of weight $w$ as

$$f_w = \frac{|\{E_i : \mathcal{W}(E_i) = w \ , \ E_i \text{ is correctable}\}|}{|\{E_i : \mathcal{W}(E_i) = w\}|}. \quad (13)$$

Then, if degenerate scenarios are disregarded, the average correctable fraction is approximately [36]

$$\langle f_w \rangle \simeq \frac{S}{N_w} e^{-\frac{N_{\leq (w-1)}}{S}} \left(1 - e^{-\frac{N_w}{S}}\right) \quad \text{for } S \gg 1, \quad (14)$$

Note that computing the syndromes associated with every possible error pattern has a high computational cost and it might be impossible even

for relatively small values of $n$. Thus we introduce a threshold parameter $t \leq n$ that defines the maximum weight of the error patterns for which the syndromes are computed, implying that $f_w = 0, \quad \forall_{w > t}$. Now we can compute probability of error $p_e$ of the protocol as follows

$$p_e = 1 - \sum_{i=0}^{n} \langle f_i \rangle f_{\mathrm{Bin}(n,p)}(i) = 1 - \sum_{i=0}^{t} \langle f_i \rangle f_{\mathrm{Bin}(n,p)}(i). \quad (15)$$

This provides a useful lower bound for the achieved average fidelity, $\langle F_a \rangle$, of the output pairs, as explained in Appendix A. Therefore, we say that the protocol achieves purification if one obtains that $\langle F_a \rangle \geq 1 - p_e > F_i$. Note that, as it is defined, the probability of error corresponds to the probability of not correctly identifying an error pattern. This means that, in the limit situation, where no syndrome is extracted (and consequently no correction is applied to the ensemble), one obtains $p_e = 1 - f_{\mathrm{Bin}(n,p)}(0)$, while in practice the fidelity achieved is equal to the initial fidelity.

The efficiency of a protocol is determined by its yield, which is normally defined as the ratio between the number of purified pairs with fidelity arbitrarily close to unity and the initial number of pairs required by the protocol , that is, for a protocol that uses $n$ Bell pairs to produce $k$ Bell pairs with fidelity $F \geq 1 - \epsilon \quad \forall_{\epsilon > 0}$, the yield is defined as $\lim_{n \to \infty} \frac{k}{n}$ [28, 33]. Such a definition would imply that many protocols would have a zero yield, including the hashing protocol when employed for finite-sized ensembles. Therefore, we shall consider a relaxed version of this definition, by defining the yield $Y$ simply as the ratio between the number of output and the number of input Bell pairs in analogy to the rate in the context of QECCs, as it is a common pratice in the literature [31, 32].

To assess the accuracy of the results obtained using Equation (14), the random encoding was simulated by generating a random parity check matrix, and the syndromes for each considered error pattern were computed using the techniques explained in Ref. [54]. This was performed considering 32 and 128 Bell pairs, affected by 1% LDN. The results are shown in Figure 2. These results were obtained for each value by performing twenty Monte Carlo simulations for each yield value considered. In the figure, each data point represents the average result of these simulations. The plots in the figure illustrate how the com-
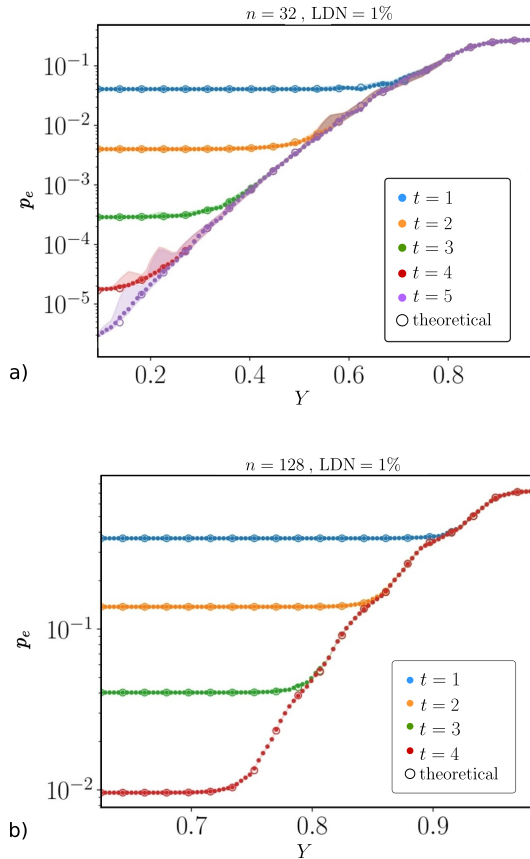
Figure 2: Simulation results of the protocol probability of error $p_e$ as a function of the yield, for a) 32 and b) 128 Bell pairs, assuming $1\%$ of LDN. While on plot a) we simulated the procedure for errors with a weight up to $t = 5$, on b) we restricted to $t = 4$. The larger white dots represent the values obtained by combining expressions (14), and (15). The simulation results show that the probability of error closely agrees with the values obtained via the theoretical expression when using a relatively large number of gates for the encoding (120 gates for plot a) and 1000 for plot b)).

putational cost, represented by the parameter $t$, constrains the purification capabilities of the protocol. The presence of a horizontal line on each curve signifies the existence of a saturation point. At this point, the majority of the analyzed error patterns are successfully mapped to a syndrome, and further sacrificing of pairs (i.e., utilizing lower yields) does not translate into any additional advantage, meaning that in scenarios characterized by high levels of noise and/or a large number of pairs, the computational cost emerges as a limiting factor in achieving purification.

Given the computational complexity and hardware constraints associated with conducting these extensive simulations, the subsequent findings in this section are derived from their analytical approximations. The numerical results obtained using these expressions for various values of $n$, $p$, and $t$ can be found in Appendix D

The approach of correcting the most likely errors implies that, in order to achieve purification, at least all the error patterns with weight up to $np$ must be considered by the protocol.

The capacity (i.e., the highest rate or yield one can possibly obtain using a quantum error correction code and PP) of the depolarizing channel for non-degenerate stabilizer codes is upper bounded by

$$\frac{k}{n} < 1 - p \log_2(3) - H(p), \qquad (16)$$

where $H(p) = -p \log_2(p) - (1 - p) \log_2(1 - p)$ is the binary entropy function [57]. This bound is known as the quantum Hamming bound, and it can be exceeded by degenerate codes [58]. Although the capacity of the depolarizing channel has already been determined [59, 60], this bound provides a more manageable expression for evaluating the performance of a stabilizer code in a setup that involves a large number of channel uses.

Using similar arguments as the ones in [61], one can prove that the yield of our protocol is upper bounded by this bound. However, it is worth evaluating how close the yield requirements are to that bound. Assuming an initial fidelity $F_i$, Figure 3 illustrates the maximum yield required to achieve an error probability below a specified threshold. These results are derived without imposing any constraints on the weight of the errors considered. Thus, the number of available syndromes emerges as the sole limiting factor influencing the outcomes.

The most significant observation from fig. 3 is the initial growth in the required yield as the number of pairs increases up to a few hundred. Notably, by employing the protocol on ensembles with a few more qubits, much superior efficiencies can be obtained. However, using more than five hundred pairs leads to only marginal changes in the yield required to obtain the same error probabilities, since in this regime the yield is already close to the capacity of the channel. This observation may have critical implications for the realistic implementation of the protocol, as the challenge of generating and manipulating larger qubit ensembles could pose a substantial obstacle.
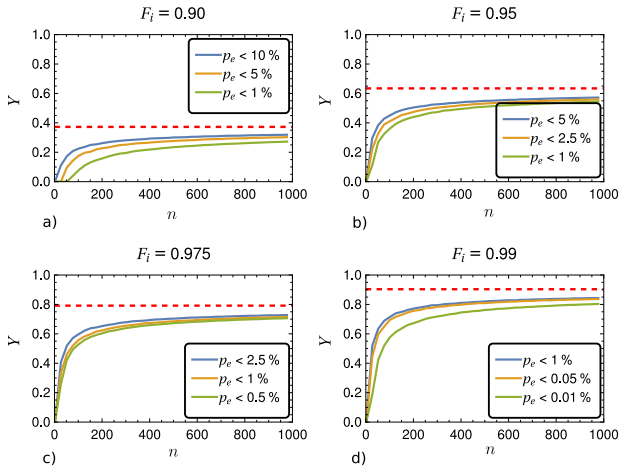
Figure 3: Maximum achievable yield to purify $n$ Bell pairs with an initial fidelity $F_i$ with a probability of error inferior to $p_e$. The initial fidelity is equal to a) $F_i = 0.90$, b) $F_i = 0.95$, c) $F_i = 0.975$ and d) $F_i = 0.99$. For each graph, the blue line represents the maximum yield at which purification is achievable. The dashed red line represents the bound given by Equation (16). Applying the protocol to ensembles with more than one hundred pairs allows for a substantial increase in the efficiency of the protocol.

Another noteworthy aspect is the minimal difference in the required yields for achieving pairs with varying error probabilities. This is evident by the proximity between the curves in each plot, indicating that a much more purified state can be obtained by slightly sacrificing the protocol's yield.

## 3.3 Computational limitations

In some situations, it may prove infeasible to account for error patterns that are extremely unlikely, such as those with very high weight, when the noise model is a Pauli channel. Figure 4 showcases the regimes that are more realistic to consider.

As we limit the correction process to only account for error patterns with weight at most $t$, PGRAND's performance may be degraded. In Figure 5 it is possible to see the minimum value of fidelity needed to achieve purification, $F_{\min}$, according to the number of pairs and the constraint imposed on the value of $t$. If no constraints were imposed, this value is expected to solely decrease with the number of pairs, since in this scenario the only limiting factor is the number of available syndromes.

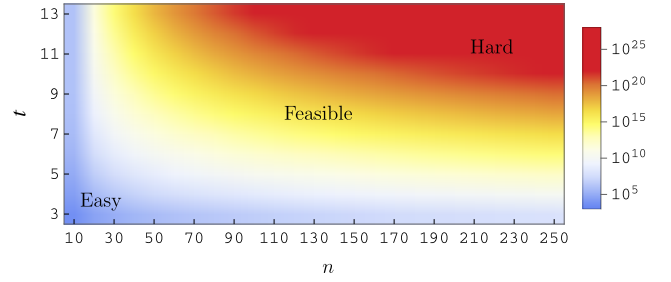However, following section 3.1.3, if one limits



Figure 4: Contour plot of the number of possible error patterns with weight equal or inferior to $t$ on an ensemble of $n$ Bell pairs. Here it is possible to see that the number of error patterns increases exponentially with their weight, but sub-exponentially with the size of the ensemble. The yellowish zone marks the frontier between what is computationally feasible with the actual standards.

the number of error patterns considered, a saturation point is reached. In this scenario, the number of possible syndromes surpasses the number of considered error patterns, and no advantage is obtained by having more syndromes. As the number of pairs increases, errors with greater weight become more likely, causing an increase in the error probability and the value of $F_{\min}$.
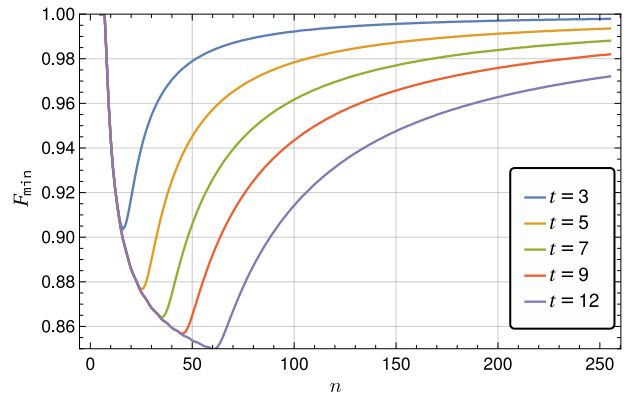


Figure 5: Minimum initial fidelity $F_{\min}$ required to achieve purification as a function of the number of pairs in Werner form when attempting to correct errors with a weight up to $t \in \{3, 5, 7, 9, 12\}$. These results were obtained by considering that only one purified Bell pair is obtained $n$-to-one. If no constraints were imposed on $t$, the value of $F_{\min}$ would strictly decrease with the number of pairs. However, if one limits the number of precomputed syndromes, a saturation point is reached.

It is also possible to determine a bound for the value of $F_{\min}$ regardless of the number of pairs, following a similar reasoning as the one used in Ref. [27]. Indeed, given that the yield of the protocol is bounded by Equation (16), a positive

| $t$ | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|
| $n$ | 30 | 35 | 40 | 45 | 50 | 56 | 61 |
| $F_{\min}$ | 0.8695 | 0.8642 | 0.8601 | 0.8578 | 0.8542 | 0.8512 | 0.8499 |

Table 1: Minimum fidelity to achieve purification and respective number of pairs required as a function of the parameter $t$.

yield can only be obtained as long as $p > 0.1893$, that is, $F_{\min} > 0.8107$.

## 4   Comparison of approaches

### 4.1   The Hashing Protocol

A similar approach to purification is performed by the Hashing protocol. The Hashing protocol [27] is a one-way entanglement purification protocol that operates on a large ensemble of noisy $n$ entangled pairs. Representing by $W$ the density matrix of the initial ensemble, the hashing protocol is capable of distilling a smaller number of pairs $k \approx n((1 - S(W))$, where $S(W)$ is the Von Neumann entropy, with fidelity arbitrarily close to unity in the asymptotic regime where $n \to \infty$.

The protocol consists of $n - k$ rounds where, at each round one of the parties performs some unitary operations and one of the qubits is measured and sacrificed to reveal information about the system, with each measurement revealing one bit about the unmeasured pairs. The result of the measurement is sent classically to the other party, which by measuring the corresponding qubit obtains information about the parity of the ensemble.

For a small parameter $\delta > 0$, the protocol attempts to correct errors that belong to the following set

$$T_\delta = \left\{ E_i : \left| -\frac{1}{n} \log_2(P(\{E_i\})) - S(W) \right| < \delta \right\}. \tag{17}$$

While the original intention of the hashing protocol was to operate with an asymptotically large number of Bell pairs, our interest is to assess its performance with a finite (and possibly small) ensemble. For this reason, we consider the yield of the hashing protocol with $k$ rounds to be given by $k/n$.

Nonetheless, we present a comparison of performance between PGRAND and this protocol. The first challenge of establishing a fair comparison lies in the absence of a straightforward ex-

pression for the fidelity of the states produced by the hashing protocol. To enable the comparison, we rely on a bound derived in Ref. [62] concerning the average fidelity achieved by the hashing protocol when applied to Werner states with fidelity parameter $F_i$. The bounding expression is as follows:

$$\langle F_a \rangle \geq 1 - 2e^{\left\{ \frac{-n}{a(F_i)} \left[ (g(F_i) + \delta) \ln \left( 1 + \frac{\delta}{g(F_i)} \right) - \delta \right] \right\}}$$
$$- 2^{-n[S(F_i) + \delta] - (n-k)},$$

where

$$S(F) = $$
$$- F \log_2(F) - (1 - F) \log_2 \left( \frac{1 - F}{3} \right),$$
$$a(F) = $$
$$\log_2 \left( \frac{1 - F}{3} \right) | + S(F),$$
$$g(F) = $$
$$\frac{F \log_2^2(F) + (1 - F) \log_2^2 \left( \frac{1-F}{3} \right) - S^2(F)}{a(F)}.$$
$$\tag{18}$$

This bound was established by bounding the probability of failure of the hashing protocol

The parameter $\delta$ presents a challenge to our comparison, as its smaller values prompt the hashing protocol to attempt to correct a larger number of error patterns, as stipulated by eq. (17). However, if the yield is not sufficiently small, an increase in $\delta$ leads to a reduction in the fidelity of the output pairs ( see Appendix B). This trade-off is evident in Figure 6, where we compare the fidelity achieved by PGRAND (without imposing a restriction on the number of corrected errors) to that achieved by the hashing protocol, for similar values of $\delta$ as the ones used in other references [27, 62, 32].

Nevertheless, it is clear that PGRAND outperforms the hashing protocol, particularly when 128 pairs are used. For $\delta > n^{-\frac{1}{3.5}}$ the hashing protocol fails to achieve purification for the number of pairs considered.
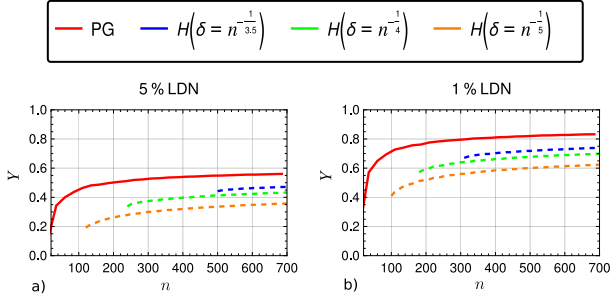
Figure 6: Average fidelity achieved $\langle F_a \rangle$ of the output pairs from the hashing protocol and PGRAND as a function of the yield, for 128 (a) and 256 (b) pairs. For $\delta = n^{-\frac{1}{3.5}}$ the hashing protocol is unable to achieve purification, meaning that considering lower values of $\delta$ is pointless. For the PGRAND curve, no constraints were imposed on the value of $t$. It is possible to observe the trade-off between the yield and output fidelity that comes from choosing different values for the parameter $\delta$ of the hashing protocol.

Next, we compare how the initial pair count in the ensemble changes the yield required for purification ($F_a \geq 1 - p$). The results in Figure 7 show us that the hashing protocol demands a larger ensemble of pairs. The increase of the number of pairs enables the use of a greater value for the parameter $\delta$, leading to higher yields. It becomes clear that as $n$ increases the hashing protocol performance approaches the performance of our protocol. In the considered noise scenarios, using higher values of $\delta$ would lead to similar yields for both protocols.

To evaluate the minimum number of pairs required, denoted as $n_{\min}$, for achieving purification, the protocols were examined under the condition where only one purified pair is generated. Specifically, this corresponds to the case where $k = 1$, enabling the establishment of a limiting scenario. For the PGRAND evaluation, no constraints were imposed on the value of $t$ (which corresponds to considering $t = n$).

When setting $k = 1$ for the hashing protocol, it is common in the literature to use $\delta_{\text{reference}} = \frac{1}{2}\left(\frac{n-1}{n} - S(F)\right)$ [62, 32]. However, this choice of $\delta$ is suboptimal, as demonstrated in Figure 8, where we compare the values of $n_{\min}$ for our protocol and the hashing protocol. Therefore, we include a comparison with the results obtained by the hashing protocol when selecting an $\delta_{\text{optimal}}$ that maximizes the fidelity for each considered fidelity value $F_i$. The results at some notable
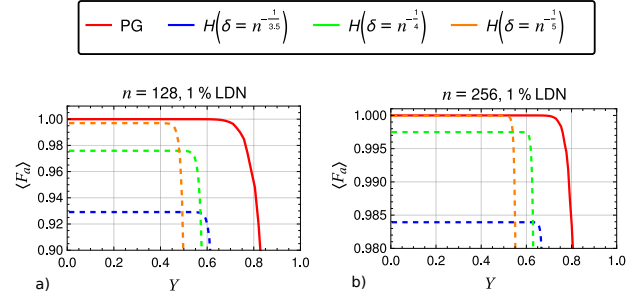


Figure 7: Yield required to achieve purification as a function of the number of pairs of the initial ensemble for the hashing protocol and PGRAND, for 1% (a) and 5% (b) of LDN. For the PGRAND curve, no constraints were imposed on the value of $t$. For the hashing protocol, increasing the number of pairs allows the choice of a smaller $\delta$. As the number of pairs increases, the differences between the efficiencies of the protocols become smaller.
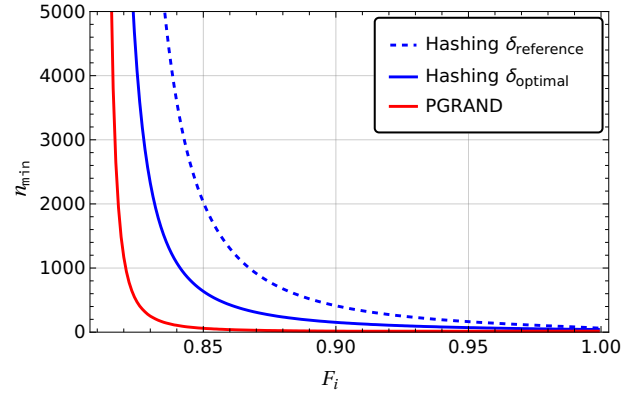


Figure 8: Number of pairs in Werner form with fidelity $F_i$ required to achieve purification. While in both protocols there is an exponential increase in the number of required pairs with the amount of noise, the requirements of our protocol are substantially lower than the ones of the hashing protocol.

points of the curves are detailed in Table 2.

There is a clear exponential relationship between $F_i$ and $n_{\min}$, and as expected, the higher the initial fidelity the fewer initial pairs are required to achieve purification. For example, while for achieving purification with $F_i = 0.850$ it is required that $n_{\min} = 60$, for $F_i = 0.818$ we have that $n_{\min} = 1947$. Nevertheless, employing as few as 10 qubits enables the purification of states with $F_i = 0.95$, while increasing the qubit count to 16 lowers this threshold to $F_i = 0.90$. This is in striking contrast with the hashing protocol, which requires at least an ensemble with a size in the order of the hundred qubits for most noise regimes.

| $n_{\min}$ | | | | | |
|---|---|---|---|---|---|
| $F_i$ | 0.83 | 0.85 | 0.90 | 0.95 | 0.99 |
| PGRAND | 251 | 60 | 16 | 10 | 8 |
| Hashing $\delta_{\text{optimal}}$ | 2326 | 637 | 153 | 71 | 45 |
| Hashing $\delta_{\text{reference}}$ | 8116 | 2027 | 412 | 164 | 82 |

Table 2: Minimum number of pairs required to achieve purification for an ensemble with fidelity $F_i$. While choosing an optimal value for $\delta$ greatly reduces the number of required pairs, PGRAND can reduce this number up to 10 times.

For a practical scenario, it is crucial to assess the performance of both protocols under equivalent computational constraints. This entails examining how they fare when correcting a comparable number of errors. However, while PGRAND's performance improves with the number of errors it aims to correct (set by the parameter $t$), the hashing protocol doesn't necessarily follow the same trend. Increasing the number of errors under consideration (represented by a lower value of $\delta$) may result in a decline of its performance, as detailed in Appendix B, making direct comparisons challenging.

Nonetheless, we define $\delta'(t) = \frac{1}{n} \log_2(N_{\leq t}) - S(F_i)$ and compare the fidelity achieved by the hashing protocol using $\delta'(t)$ with the fidelity attained by PGRAND when limiting the error correction to errors with weight up to $t$. The choice of a suitable value for $t$ is made to ensure a fair and balanced comparison with PGRAND under similar error correction conditions. For both protocols, we considered the scenario where only one purified pair is obtained ($k = 1$). Therefore the results depicted in Figure 9 serve only to illustrate how both protocols perform under the same computational constraints.

We observe that for a small number of pairs, PGRAND exhibits superior performance compared to the hashing protocol. As the number of pairs in the initial ensemble increases, the performance differences between the two approaches tend to diminish. However, it is crucial to consider the computational cost associated with larger initial ensembles. The hashing protocol becomes impractical due to this increased computational burden, while PGRAND maintains the advantage of achieving purification with a smaller number of pairs and manageable computational resources.

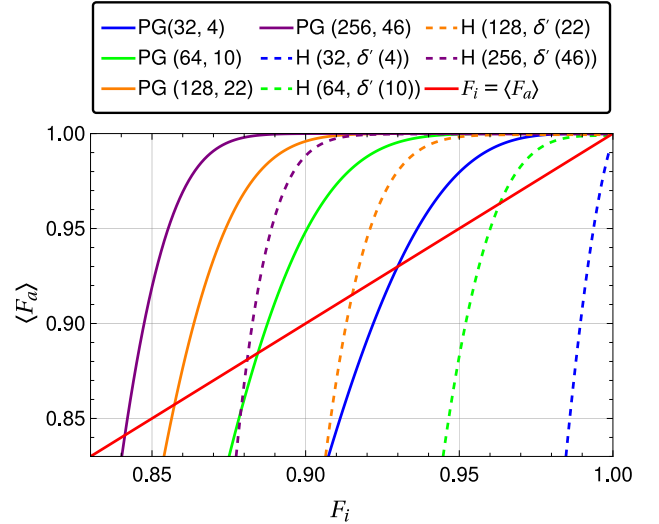PGRAND appears to offer a distinct improvement over the hashing protocol. However, its



Figure 9: Fidelities $\langle F_a \rangle$ by the hashing protocol with $n$ pairs and parameter $\delta$ (denoted by H($n$, $\delta$)) and PGRAND with $n$ pairs and maximum weight $t$ (denoted by PG($n,t$)) as a function of the fidelity of Werner pairs $F_i$, when constrained to correct the same number of errors. The solid red line indicates the range where purification is achievable.

implementation demands more gates and qubits compared to the hashing protocol; while both require $\mathcal{O}(n^2)$ gates, the hashing protocol does not use ancilla qubits. Consequently, the advantage of using PGRAND might be diminished if one considers the noise introduced by each gate.

## 4.2 Recurrence Protocols

The comparison between deterministic protocols, such as ours, and recurrence protocols remains relatively unexplored in the literature. This is primarily due to their design for application in different regimes, rendering the construction of effective metrics for their evaluation an ongoing challenge in the field. Some insights about this class of protocols are provided in Appendix C.

Due to their inherent probabilistic nature, our yield definition is no longer appropriate since it does not take into account the possibility of failure of these protocols, in the sense that it does not provides a good insight about the final cost of purification in terms of used Bell pairs, (which is given by $n/P_{\text{suc}}$, with $P_{\text{suc}}$ being the probability of success of the protocol. For example, according to our definition the Oxford protocol would have a constant yield of $\frac{1}{2}$ for any given initial fidelity. Furthermore for recurrence protocols the expected yield and the achieved fidelity is automatically determined by the protocol, the initial state, and its fidelity. However, in hashing protocols one can manipulate the yield in order to obtain different fidelities. Thus, in order to be able to compare both classes of these protocols, we introduce a new type of yield, which we name the effective yield $Y_E$, and define it as

$$Y_E = \frac{k}{n/P_{\text{suc}}}(F_a - F_i) = P_{\text{suc}} Y \Delta F \in [0, 1]. \quad (19)$$

The effective yield offers a comprehensive assessment metric for purification protocols by integrating both yield and fidelity increase aspects. While lacking a direct physical interpretation, $Y_E$ effectively quantifies the efficiency of protocols in terms of yield and fidelity enhancement, constrained to non-negative values under the assumption that purification protocols cannot diminish fidelity. However, $Y_E$ prioritizes the purification cost of a protocol over fidelity increase, particularly accentuated in high initial fidelity regimes where minimizing purification cost is critical. As such, $Y_E$ serves as a valuable tool for identifying protocols that strike an effective balance between fidelity enhancement and purification cost reduction, addressing a significant gap in the evaluation of entanglement purification protocols.

The results for the various protocols regarding the effective yield, when considering an initial ensemble composed by Werner states with fidelity $F_i$ can be seen in Figure 10. While for computing $Y_E$ for the case of PGRAN the probability of error to has been used to lower bound the fidelity achieved, for the remaining protocols this quantity was directly computed without approximations, meaning that the comparison is in favor of the recurrence protocols.

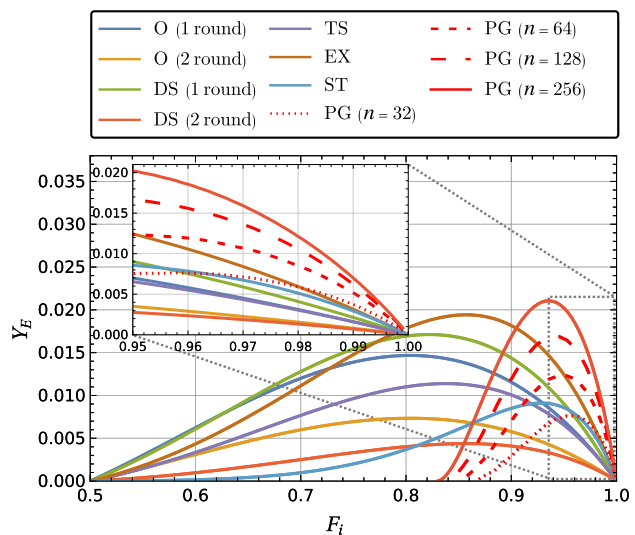Upon examining the findings depicted in the figure, it becomes apparent that the increment in



Figure 10: Effective yield $Y_E$ of different protocols (Oxford (O), Double Selection (DS), Triple Selection (TS), EXPEDIENT (EX), STRINGENT (ST) and PGRAND (PG)) as a function of the initial fidelity $F_i$ of a Werner State, applied in a noiseless scenario.

the number of rounds does not necessarily correspond to an elevation in the effective yield. This observation is intricately linked to the definition of the effective yield, which places a greater emphasis on the purification cost rather than the fidelity enhancement.

In high entropy regimes, EXPEDIENT and Triple Selection protocols (see appendix C) emerge as optimal choices in terms of this metric. This superiority can be attributed to the potential for achieving a significant fidelity increase within a high entropy regime, while maintaining reasonable purification costs.

Conversely, in low entropy settings, PGRAND exhibits dominance, with its advantage escalating proportionally with the initial ensemble's size. Within this regime, the primary determinant of the effective yield lies in the diminished purification cost, where PGRAND notably outperforms other protocols, rather than in the fidelity improvement.

# 5 Measurement-based version of PGRAND

During the analysis of the protocol we assumed that the operations were noiseless. Nonetheless, this is an unrealistic approach, and even a slight amount of noise can compromise the entire protocol, since the entropy of the ensemble is amplified

by each noisy operation. Considering that $\mathcal{O}(n^2)$ two-qubit operations are required, the increase in entropy caused by noisy operations can easily exceed the information obtained from the measurement. This holds even for minor imperfections, posing a threat to the entire protocol.

Although Clifford gates can be implemented in a fault tolerant manner, this problem can be circumvented by using a measurement-based approach. The main concept revolves around the preparation of a resource state using measurement-based methods, which incorporate both the encoding, stabilizer measurement, and decoding of the protocol. Afterward, the Bell pairs are coupled to the resource state using Bell measurements [1], in a manner similar to what is carried out in Refs. [63, 64, 38, 39, 32, 65, 66].

For an entanglement purification protocol that uses only Clifford gates to distill $k$ pairs from an initial ensemble of $n$ pairs, a minimal resource state can be obtained with $2(n + k)$ qubits. Although the measurement-based approach requires more qubits, ancilla qubits are not needed, as explained in [40, 49]. Additionally, any Clifford circuit can be implemented using only one *measurement layer*, that is, with all measurements being parallelizable. However, it is essential to note that, despite the resulting state is no longer a cluster state (and therefore is no longer universal) it is, up to local unitaries, equivalent to a graph state [40, 67].

The resource states can be obtained from a cluster state and then purified and encoded. Quantum communication via measurement-based entanglement purification has been shown to outperform direct transmission, gate-based error correction, and measurement-based schemes generating resource states directly [68].

The fact that the resource state can be prepared in advance is especially relevant because qubits may experience dephasing during the processing time of the protocol. However, with the resource state prepared beforehand, the processing time is uniquely limited to the time required to perform the Bell measurements and classically communicate the results.

To explore how imperfections in quantum operations and noisy Bell measurements affect

---

[1]Executing the purification protocol in this manner renders it non-deterministic due inherent probabilistic nature of Bell measurements.
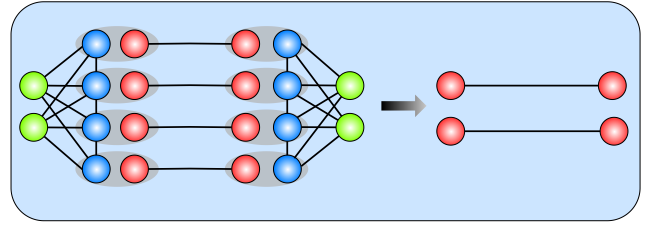


Figure 11: Illustration of the implementation of the protocol in a measurement-based manner. The Bell pairs (red vertices) are coupled to the input qubits of the resource state (blue vertices) via Bell Measurements. The output qubits of the resource state (green vertices) are kept and the remaining ones are discarded. After communicating classically the measurement results and applying the corrections, purified Bell pairs are obtained.

a measurement-based entanglement purification protocol, specifically, the impact of imperfect resource states, we consider LDN on each particle of the resource states. For estimating the error thresholds in a noisy implementation for this protocol, we remark that it has been proven that it is possible to formally transfer the noise affecting the input qubits of the resource state to the Bell pairs targeted for purification [64]. Consider that the Bell pairs and the resource states are affected by LDN with parameters $p$ and $q$ respectively.

It is easily verifiable through simple computations that this is equivalent to considering that one starts with Werner states with fidelity

$$F_i = 1 - p - q + \frac{4}{3}pq. \tag{20}$$

Similarly, the noise present in the output qubits can also be transferred to the final state, given that one can always assume that the protocol outputs Werner states with fidelity $\langle F_a \rangle$. Thus, after moving the noise from the output qubits of the resource state to the output Bell pairs, one ends up again with a Werner state with fidelity

$$\langle F_a \rangle = 1 - p_e - q + \frac{4}{3}p_e q. \tag{21}$$

The advantage of this decomposition is that, once the noise has been transferred, we are left with a perfect purification process to which our previously presented analytical results still apply. With that in mind, we can now deduce a threshold for the tolerable error value of the resource states. By recognizing that it is impossible to purify Bell pairs with a fidelity lower than that of the resource state, we obtain the condition $p \geq q$. This condition arises from the requirement
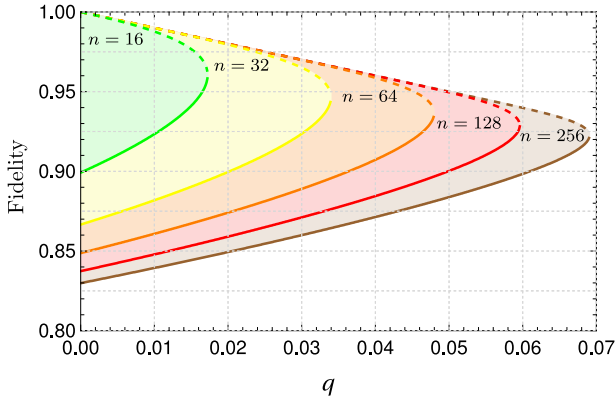
Figure 12: Maximum achievable fidelity (dashed lines) and minimum required fidelity (solid lines) of PGRAND as a function of the noise depolarization probability $q$ of the resource states, for $n$ qubits. The colored space between the solid and the dashed lines of the same color represents the purification range of the protocol, meaning that in these areas purification is achievable.

that the purification process must be achievable, which imposes $F_a \geq F_i$. Moreover, the protocol can only operate on a depolarized state with fidelity $F_i \geq F_{\min} = 0.8107$. Hence the following condition is obtained

$$1 - 2q + \frac{4}{3}q^2 \leq F_{\min}, \qquad (22)$$

implying the threshold to be $q_{\min} = 0.0859$. Figure 12 presents a numerical analysis of the purification ranges corresponding to various numbers of initial pairs, while Table 3 displays the error thresholds for the same numbers of initial pairs. These thresholds for the minimum required fidelity $F_{\min}$ and the maximum achievable fidelity $F_{\max}$ were obtained by inspecting the $n$-to-one routine. These values can be seen in Table 4 and Table 5, respectively. It is important to highlight that these error thresholds align with a reasonable and conservative error model consistent with measurement-based quantum information processing principles. However, it is not straightforward to compare these thresholds directly with those derived from gate-based error models, such as the ones used in [29, 31]. Establishing such a connection presents an open challenge. Furthermore, extending the analysis to include correlated errors would be valuable. This extension could involve exploring how errors are localized and justifying a local error model through the application of multipartite entanglement purification for resource states [63, 35, 53].
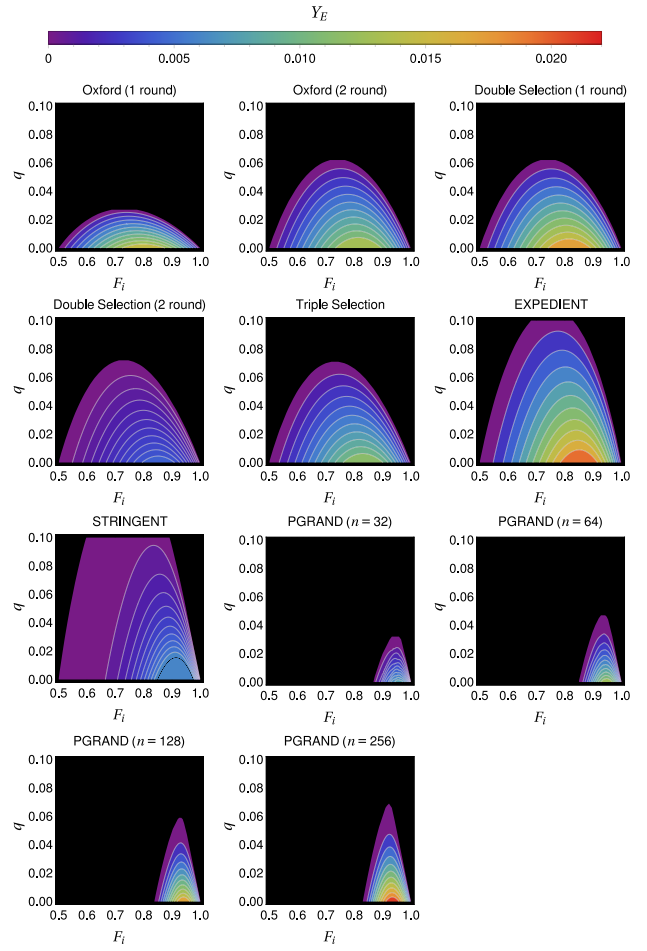


Figure 13: Contour plots of the effective yield $Y_E$ for different protocols as a function of the initial fidelity $F_i$ of a Werner State and the parameter $q$ of LDN in the resource states. The black area denotes the zone where purification is not achieved.

| Error Threshold | | | | | |
|---|---|---|---|---|---|
| $n$ | 16 | 32 | 64 | 128 | 256 |
| $q$ | 1.72% | 3.39% | 4.79% | 5.96% | 6.89% |

Table 3: Resource states error thresholds as a function of the number of required Bell pairs, expressed by the LDN parameter $p$ per qubit. All of these results are referent to the $n$-to-one routine.

In order to establish a comparison, one can also apply the explained formalism to create measurement-based versions of the purification protocols presented in Section 4.2. The noise of the resource states can be modelled in the same way. Just like in the previous scenario, we used the effective yield as a measure of performance of the protocols.

The results are shown in the form of contour plots in Figure 13. For the cases where 2 rounds

of a recurrence protocol were applied, we considered resource states of reduced size that apply the purification procedures within a single step [39]. Notice that this results in the increase of the contour area, since purification can be achieved more easily given that more rounds allow greater fidelity increases. This comes with the trade off of diminishing the efficient yield due to lower success probabilities, which ultimately translates into higher purification costs.

The results also indicate recurrence protocols to be much more resilient to the effect of noise, as it has already been pointed out in [64]. This is attributed to those protocols' larger tolerance to initial noise, given that they are able to theoretically tolerate any $F_{\min} \geq 0.5$, while PGRAND and the hashing protocol require $F_{\min} \geq 0.8107$. EXPEDIENT seems to be the best performing protocol according to the effective yield for the widest ranges of $F_i$ and $q$. Nonetheless, an advantage of using PGRAND can be seen again in the low entropy scenario ( $q < 0.001$ and $F_i > 0.90$)), and the advantage is more prominent as the size of the initial ensemble grows.

# 6 Conclusions

Quantum entanglement purification methods are vital in quantum information processing. They help mitigate noise and enable the recovery of highly entangled states, making them essential tools for various quantum information tasks. In this paper, we present a purification protocol that represents a significant improvement over Bennett's hashing protocol. We provide a detailed explanation of the protocol's construction concepts and the underlying principles, along with a comprehensive analysis of its performance across different ensemble sizes, noise regimes, and computational constraints. Our findings demonstrate that our protocol can achieve a fidelity of 90% when purifying states, even with a relatively small ensemble size of just 16 Bell pairs. While hashing protocols offer distinct advantages over other types of protocols due to their non-probabilistic nature (unlike recurrence protocols) and high performance as the initial ensemble size increases, they are constrained by the computational resources they require [30, 62, 38]. The requirement of such a small initial ensemble in our protocol not only reduces computational costs significantly

but also paves the way for a more realistic implementation. This is especially relevant in practical scenarios where there is a preference for employing fewer qubits. Moreover, if one manages to obtain a larger ensemble of Bell pairs with sufficiently low levels of noise, high efficiencies can be obtained while maintaining a feasible computational cost. Thus, PGRAND purports to be specially relevant in low-entropy noise regimes. The assumption of using noiseless gates can be overcome by using a measurement-based implementation of these protocols. Furthermore, it is known that classical RLCs can reach Shannon's channel capacity and are easy to generate. Low-density parity-check (LDPC) codes are also capacity-achieving when decoded with the belief propagation algorithm, but their construction imposes some constraints and not all $(n, k)$ pairs may be feasible. A fundamental characteristic of LDPC codes is the sparsity of the parity-check matrix. In a quantum setup using noise-guessing framework with a syndrome-based membership test, this sparsity induces a syndrome-checking procedure that involves many fewer gates than the one using QRLCs. For this reason, for fault-tolerant syndrome computation, the use of LDPC codes may be preferable when using the proposed PGRAND, given their more limited exposure to gate errors. The general fault-tolerance of a gate implementation of QGRAND/PGRAND is subject of ongoing work [69]. The extension of our protocol to multipartite entanglement is also an interesting question to study. Given that the Bell matrix identity can generalized to GHZ states [70], a version of the protocol to these states should be conceivable. Furthermore, the performance of our protocol could be improved by considering its generalization to multi-level systems (qudits), since notable improvements were found for a bipartite qudit implementation of the hashing protocol [32]. It would also be worthy to study in a more detailed scenario the feasibility of the measurement-based of this protocol, and how the cluster state size/complexity would influence the error of the resource states in a realistic implementation.

## References

[1] H. J. Kimble. "The quantum internet". Nature **453**, 1023–1030 (2008).

[2] Marcello Caleffi, Angela Sara Cacciapuoti, and Giuseppe Bianchi. "Quantum internet: from communication to distributed computing!". In Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication. Pages 1–4. Reykjavik Iceland (2018). ACM.

[3] Ang-Kun Wu, Liang Tian, Bruno Coelho Coutinho, Yasser Omar, and Yang-Yu Liu. "Structural vulnerability of quantum networks". Phys. Rev. A **101**, 052315 (2020).

[4] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. "Quantum entanglement". Reviews of Modern Physics **81**, 865–942 (2009).

[5] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". Theoretical Computer Science **560**, 7–11 (2014).

[6] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels". Physical Review Letters **70**, 1895–1899 (1993).

[7] J. I. Cirac, A. K. Ekert, S. F. Huelga, and C. Macchiavello. "Distributed quantum computation over noisy channels". Physical Review A **59**, 4249–4254 (1999).

[8] W. Dür and H.-J. Briegel. "Entanglement Purification for Quantum Computation". Physical Review Letters **90**, 067901 (2003).

[9] P. Sekatski, M. Skotiniotis, and W. Dür. "Improved sensing with a single qubit". Physical Review Letters **118**, 170801 (2017).

[10] V. Krutyanskiy, M. Galli, V. Krcmarsky, S. Baier, D. A. Fioretto, Y. Pu, A. Mazloom, P. Sekatski, M. Canteri, M. Teller, J. Schupp, J. Bate, M. Meraner, N. Sangouard, B. P. Lanyon, and T. E. Northup. "Entanglement of Trapped-Ion Qubits Separated by 230 Meters". Physical Review Letters **130**, 050803 (2023).

[11] C. Figgatt, A. Ostrander, N. M. Linke, K. A. Landsman, D. Zhu, D. Maslov, and C. Monroe. "Parallel entangling operations on a universal ion-trap quantum computer". Nature **572**, 368–372 (2019).

[12] Colin D. Bruzewicz, John Chiaverini, Robert McConnell, and Jeremy M. Sage. "Trapped-ion quantum computing: Progress and challenges". Applied Physics Reviews **6**, 021314 (2019).

[13] Daniel Riedel, Immo Söllner, Brendan J. Shields, Sebastian Starosielec, Patrick Appel, Elke Neu, Patrick Maletinsky, and Richard J. Warburton. "Deterministic enhancement of coherent photon generation from a nitrogen-vacancy center in ultrapure diamond". Physical Review X **7**, 031040 (2017).

[14] Maximilian Ruf, Mark IJspeert, Suzanne Van Dam, Nick De Jong, Hans Van Den Berg, Guus Evers, and Ronald Hanson. "Optically coherent nitrogen-vacancy centers in micrometer-thin etched diamond membranes". Nano Letters **19**, 3987–3992 (2019).

[15] A. M. Kaufman, B. J. Lester, M. Foss-Feig, M. L. Wall, A. M. Rey, and C. A. Regal. "Entangling two transportable neutral atoms via local spin exchange". Nature **527**, 208–211 (2015).

[16] Ivaylo S. Madjarov, Jacob P. Covey, Adam L. Shaw, Joonhee Choi, Anant Kale, Alexandre Cooper, Hannes Pichler, Vladimir Schkolnik, Jason R. Williams, and Manuel Endres. "High-fidelity entanglement and detection of alkaline-earth Rydberg atoms". Nature Physics **16**, 857–861 (2020).

[17] N. Leung, Y. Lu, S. Chakram, R. K. Naik, N. Earnest, R. Ma, K. Jacobs, A. N. Cleland, and D. I. Schuster. "Deterministic bidirectional communication and remote entanglement generation between superconducting qubits". npj Quantum Information **5**, 1–5 (2019).

[18] E. Flurin, N. Roch, J. D. Pillet, F. Mallet, and B. Huard. "Superconducting Quantum Node for Entanglement and Storage of Microwave Radiation". Physical Review Letters 114, 090503 (2015).

[19] Joschka Roffe. "Quantum error correction: an introductory guide". Contemporary Physics 60, 226–245 (2019).

[20] Simon J. Devitt, William J. Munro, and Kae Nemoto. "Quantum error correction for beginners". Reports on Progress in Physics 76, 076001 (2013).

[21] Michelle Victora, Spyros Tserkis, Stefan Krastanov, Alexander Sanchez de la Cerda, Steven Willis, and Prineha Narang. "Entanglement purification on quantum networks". Phys. Rev. Res. 5, 033171 (2023).

[22] William J. Munro, Koji Azuma, Kiyoshi Tamaki, and Kae Nemoto. "Inside Quantum Repeaters". IEEE Journal of Selected Topics in Quantum Electronics 21, 78–90 (2015).

[23] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. "Long-distance quantum communication with atomic ensembles and linear optics". Nature 414, 413–418 (2001).

[24] Sara Santos, Francisco A. Monteiro, Bruno C. Coutinho, and Yasser Omar. "Shortest Path Finding in Quantum Networks With Quasi-Linear Complexity". IEEE Access 11, 7180–7194 (2023).

[25] Luís Bugalho, Bruno C. Coutinho, Francisco A. Monteiro, and Yasser Omar. "Distributing Multipartite Entanglement over Noisy Quantum Networks". Quantum 7, 920 (2023).

[26] Bruno C. Coutinho, Raul Monteiro, Luís Bugalho, and Francisco A. Monteiro. "Entanglement routing based on fidelity curves" (2024). arXiv:2303.12864.

[27] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. "Mixed-state entanglement and quantum error correction". Physical Review A 54, 3824–3851 (1996).

[28] Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. "Purification of noisy entanglement and faithful teleportation via noisy channels". Physical Review Letters 76, 722–725 (1996).

[29] David Deutsch, Artur Ekert, Richard Jozsa, Chiara Macchiavello, Sandu Popescu, and Anna Sanpera. "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels". Physical Review Letters 77, 2818–2821 (1996).

[30] H. F. Chau and K. H. Ho. "Practical entanglement distillation scheme using recurrence method and quantum low density parity check codes". Quantum Information Processing 10, 213–229 (2011).

[31] Stefan Krastanov, Victor V. Albert, and Liang Jiang. "Optimized Entanglement Purification". Quantum 3, 123 (2019).

[32] J. Miguel-Ramiro and W. Dür. "Efficient entanglement purification protocols for d-level systems". Physical Review A 98, 042309 (2018).

[33] W. Dür and H. J. Briegel. "Entanglement purification and quantum error correction". Reports on Progress in Physics 70, 1381 (2007).

[34] Pei-Shun Yan, Lan Zhou, Wei Zhong, and Yu-Bo Sheng. "Advances in quantum entanglement purification". Science China Physics, Mechanics & Astronomy 66, 250301 (2023).

[35] H. Aschauer, W. Dür, and H.-J. Briegel. "Multiparticle entanglement purification for two-colorable graph states". Physical Review A 71, 012319 (2005).

[36] Diogo Cruz, Francisco A. Monteiro, and Bruno C. Coutinho. "Quantum error correction via noise guessing decoding". IEEE Access11 (2023).

[37] Daryus Chandra, Zeynep B. Kaykac Egilmez, Yifeng Xiong, Soon Xin Ng, Robert G. Maunder, and Lajos Hanzo. "Universal decoding of quantum stabilizer codes via classical guesswork". IEEE Access 11, 19059–19072 (2023).

[38] M. Zwerger, H. J. Briegel, and W. Dür. "Robustness of hashing protocols for entanglement purification". Physical Review A 90, 012314 (2014).

[39] M. Zwerger, H. J. Briegel, and W. Dür. "Measurement-based quantum communication". Applied Physics B 122, 50 (2016).

[40] Robert Raussendorf. "Measurement-based quantum computation with cluster states". International Journal of Quantum Information 07, 1053–1203 (2009).

[41] Robert Raussendorf and Hans J. Briegel. "A

one-way quantum computer". Physical Review Letters **86**, 5188–5191 (2001).

[42] Ken R. Duffy, Jiange Li, and Muriel Médard. "Capacity-Achieving Guessing Random Additive Noise Decoding". IEEE Transactions on Information Theory **65**, 4023–4040 (2019).

[43] Ioannis Chatzigeorgiou and Francisco A Monteiro. "Symbol-level GRAND for high-order modulation over block fading channels". IEEE Communications Letters **27**, 447–451 (2023).

[44] Hans Aschauer. "Quantum communication in noisy environments". PhD thesis. Ludwig-Maximilians-Universität München. (2005).

[45] Ryutaroh Matsumoto. "Conversion of a general quantum stabilizer code to an entanglement distillation protocol". Journal of Physics A: Mathematical and General **36**, 8113–8127 (2003).

[46] Reinhard F. Werner. "Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model". Physical Review A **40**, 4277–4281 (1989).

[47] W. Dür, M. Hein, J. I. Cirac, and H.-J. Briegel. "Standard forms of noisy quantum operations via depolarization". Physical Review A **72**, 052326 (2005).

[48] Robert Raussendorf and Hans Briegel. "Computational model underlying the one-way quantum computer" (2002). arxiv:quant-ph/0108067.

[49] Michael A. Nielsen and Christopher M. Dawson. "Fault-tolerant quantum computation with cluster states". Physical Review A **71**, 042323 (2005).

[50] Christopher M. Dawson, Henry L. Haselgrove, and Michael A. Nielsen. "Noise Thresholds for Optical Quantum Computers". Physical Review Letters **96**, 020501 (2006).

[51] Benjamin J. Brown and Sam Roberts. "Universal fault-tolerant measurement-based quantum computation". Physical Review Research **2**, 033305 (2020).

[52] Mercedes Gimeno-Segovia, Terry Rudolph, and Sophia E. Economou. "Deterministic generation of large-scale entangled photonic cluster state from interacting solid state emitters". Physical Review Letters **123**, 070501 (2019).

[53] W. Dür, H. Aschauer, and H.-J. Briegel. "Multiparticle Entanglement Purification for Graph States". Physical Review Letters **91**, 107903 (2003).

[54] Daniel Gottesman. "The Heisenberg representation of quantum computers" (1998). arxiv:quant-ph/9807006.

[55] Scott Aaronson and Daniel Gottesman. "Improved simulation of stabilizer circuits". Physical Review A **70**, 052328 (2004).

[56] Alexandru Paler, Simon Devitt, Kae Nemoto, and Ilia Polian. "Software-based Pauli tracking in fault-tolerant quantum circuits". In 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE). Pages 1–4. (2014).

[57] Artur Ekert and Chiara Macchiavello. "Quantum error correction for communication". Physical Review Letters **77**, 2585–2588 (1996).

[58] David P. DiVincenzo, Peter W. Shor, and John A. Smolin. "Quantum-channel capacity of very noisy channels". Physical Review A **57**, 830–839 (1998).

[59] A.S. Holevo. "The capacity of the quantum channel with general signal states". IEEE Transactions on Information Theory **44**, 269–273 (1998).

[60] C. King. "The capacity of the quantum depolarizing channel". IEEE Transactions on Information Theory **49**, 221–229 (2003).

[61] Daniel Gottesman. "Stabilizer codes and quantum error correction". PhD thesis. California Institute of Technology. (1997).

[62] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür. "Long-range big quantum-data transmission". Physical Review Letters **120**, 030503 (2018).

[63] M. Zwerger, W. Dür, and H. J. Briegel. "Measurement-based quantum repeaters". Physical Review A **85**, 062326 (2012).

[64] M. Zwerger, H. J. Briegel, and W. Dür. "Universal and optimal error thresholds for measurement-based entanglement purification". Physical Review Letters **110**, 260503 (2013).

[65] Pei-Shun Yan, Lan Zhou, Wei Zhong, and Yu-Bo Sheng. "Feasible measurement-based entanglement purification in linear optics". Optics Express **29**, 9363 (2021).

[66] Pei-Shun Yan, Lan Zhou, Wei Zhong, and

Yu-Bo Sheng. "Measurement-based entanglement purification for entangled coherent states". Frontiers of Physics **17**, 21501 (2021).

[67] M. Hein, J. Eisert, and H. J. Briegel. "Multiparty entanglement in graph states". Physical Review A **69**, 062311 (2004).

[68] J. Wallnöfer and W. Dür. "Measurement-based quantum communication with resource states generated by entanglement purification". Physical Review A **95**, 012303 (2017).

[69] Diogo Cruz, Francisco A. Monteiro, André Roque, and Bruno C. Coutinho. "Fault-tolerant noise guessing decoding of quantum random codes" (2024). arXiv:2407.01658.

[70] Narayanan Rengaswamy, Ankur Raina, Nithin Raveendran, and Bane Vasić. "Distilling GHZ states using stabilizer codes" (2022). arxiv:2109.06248.

[71] Chiara Macchiavello. "On the analytical convergence of the QPA procedure". Physics Letters A **246**, 385–388 (1998).

[72] Keisuke Fujii and Katsuji Yamamoto. "Entanglement purification with double selection". Physical Review A **80**, 042308 (2009).

[73] Naomi H. Nickerson, Ying Li, and Simon C. Benjamin. "Topological quantum computing with a very noisy network and local error rates approaching one percent". Nature Communications **4**, 1756 (2013).

## A  Probability of error as a lower bound of the fidelity

We consider the probability of error $p_e$ to be the ratio between the number of successful uses of that protocol and the total number of uses. This can be interpreted as if any uncorrected error pattern maps the initial state to an orthogonal state, that is, $\mathcal{F}(|\psi\rangle, E|\psi\rangle) = 0$, for any uncorrected error $E$. If $\mathcal{E}$ is a set of $N$ possible error patterns, and $\mathcal{C} \subseteq \mathcal{E}$ is the subset of correctable errors, then the average achieved fidelity $\langle F_a \rangle$ of the state ob-

tained at the end of the protocol verifies:

$$\langle F_a \rangle = \frac{1}{N} \sum_{E_i \in \mathcal{E}} \mathcal{F}(|\psi\rangle, E_i|\psi\rangle) = \qquad (23)$$

$$\frac{1}{N} [ \sum_{E_i \in \mathcal{C}} \mathcal{F}(|\psi\rangle, E_i|\psi\rangle) + \sum_{E_i \in \mathcal{E} \setminus \mathcal{C}} \mathcal{F}(|\psi\rangle, E_i|\psi\rangle))] \qquad (24)$$

$$\geq \frac{1}{N} \sum_{E_i \in \mathcal{C}} \mathcal{F}(|\psi\rangle, E_i|\psi\rangle) = 1 - p_e \qquad (25)$$

since it is considered that we are able to correct perfectly every error in $\mathcal{C}$, that is, $\forall_{E_i \in \mathcal{C}} \quad \mathcal{F}(|\psi\rangle, E_i|\psi\rangle) = 1$. This is equivalent to model the output states of the protocol as Werner states with fidelity $\langle F_a \rangle$.

## B  Suboptimality of the hashing protocol

Consider the typical set as defined in Equation (17). Assuming that $W$ corresponds to the density matrix of a Werner state with parameter $F$, the typical set encompasses all error patterns for which their probabilities satisfy

$$2^{-n(S(F)+\delta)} \leq P(E_i) \leq 2^{-n(S(F)-\delta)}. \qquad (26)$$

This set contains at most $2^{n(S(W)+\delta)}$ error patterns whose weight is closer to $n(1 - F)$. As defined, the hashing protocol treats all errors within this set as equally important, implying that any error pattern in this set has the same probability of being corrected. However, this correction procedure is suboptimal, regardless of the choice of $\delta$.

On one hand, a high value for $\delta$ will inherently limit the protocol's performance, since even if it manages to correct all errors within the typical set, the total probability of error is upper-bounded by the sum of probabilities of errors that are not contained within the set. On the other hand, choosing a small value for $\delta$ implies the inclusion of many errors with relatively high weight. As the number of error patterns exponentially increases with their weight, it becomes more likely (for a fixed number of syndromes) that the corrected errors will be the ones with greater weight. However, each of these errors contributes only a small amount to the overall error probability of the protocol. In Figure 14, a practical scenario illustrates how the choice of $\delta$ interferes with the hashing protocol's performance.

Accepted in ⟨ ⟩uantum 2024-09-04, click title to verify. Published under CC-BY 4.0.
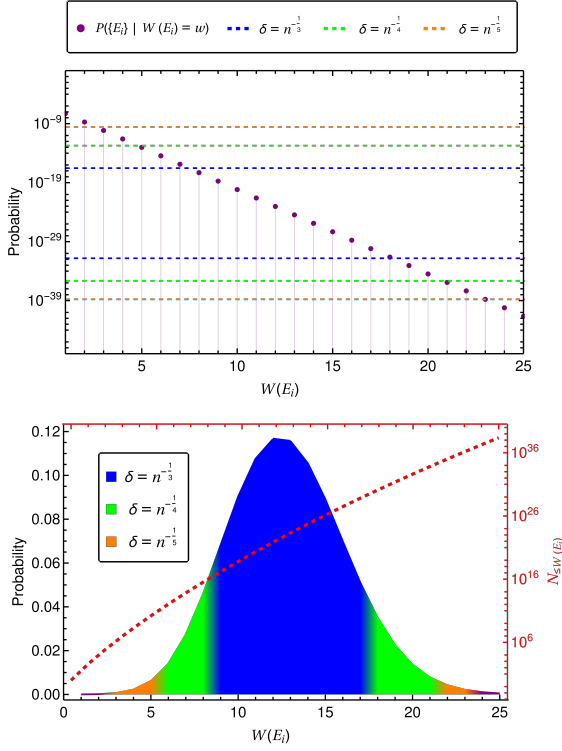
21

Figure 14: This figure illustrates how different choices of the $\delta$ parameter affect the correction capability of the hashing protocol. In plot a), each dot represents the individual probability of an error pattern based on its weight. Each pair of dashed lines of the same color represents the bounds imposed by the choice of $\delta$ (as defined in Equation (26)). In plot b), we observe the sum of the individual probabilities of error patterns with the same weight. The colored area represents the total probabilities of all errors included in the typical set, depending on the value of $\delta$. The red line indicates the number of error patterns at each weight. From this plot, it becomes evident that the correction procedure of the hashing protocol is never optimal, regardless of the choice of $\delta$. In both plots, we consider a scenario with an initial ensemble of 128 pairs subject to 10% LDN.

For illustration purposes, we have selected an ensemble containing 128 qubits with 10% LDN, but the same holds true for other choices. Even with an optimal choice of $\delta$ and a sufficiently large $n$, the correction procedure is never optimal. If we consider the computational cost of mapping each syndrome to an error pattern, it becomes evident how the hashing protocol will often fail to achieve purification for most practical cases.

## C  Review of Recurrence Protocols

Bipartite recurrence protocols are characterized by their operation within each purification step, which entails processing a fixed number $n$ of copies of a mixed state. After local manipulation, one of these copies is preserved while the remaining $n-1$ undergo measurement. Depending on the measurements outcomes, the remaining copy is either retained or discarded. If the purification step is successful, one obtains a Bell pair with increased fidelity. This iterative procedure continues, using states resulting from successful purification rounds as input for subsequent iterations. Generally, these protocols converge to a maximally entangled state [33].

Within this class of protocols, one of the simplest (yet efficient) protocols is the Oxford protocol [29], a recurrence protocol that is conceptually similar the IBM protocol [27, 28]. Consider that two noisy Bell pairs are shared between Alice and Bob. They start by applying the following unitary operations to both of their qubits

$$|0\rangle \xrightarrow{U_A} \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle), \quad |1\rangle \xrightarrow{U_A} \frac{1}{\sqrt{2}}(|1\rangle - i|0\rangle),$$
(27)

$$|0\rangle \xrightarrow{U_B} \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \quad |1\rangle \xrightarrow{U_B} \frac{1}{\sqrt{2}}(|1\rangle + i|0\rangle).$$
(28)

after which they both apply a CNOT gate on their qubits. Each measures the target qubit of the CNOT gate, and the measurement results are shared. If the measurement results agree, the unmeasured pair is kept, otherwise it is discarded. The circuit required by this protocol is depicted in Figure 15 a).

This procedure can be repeatedly applied to the purified pairs. However, at the beginning of each round, the pairs are not required to be Werner states. Instead, one considers states of the general form

$$\rho = A|\phi^+\rangle\langle\phi^+| + B|\psi^-\rangle\langle\psi^-| + C|\psi^+\rangle\langle\psi^+| + D|\phi^-\rangle\langle\phi^-| + \text{off-diagonal terms}.$$
(29)

After $r+1$ successful rounds of purification, the following state is obtained

$$A_{r+1} = \frac{A_r^2 + B_r^2}{N_r}, \quad B_{r+1} = \frac{2C_r D_r}{N_r},$$
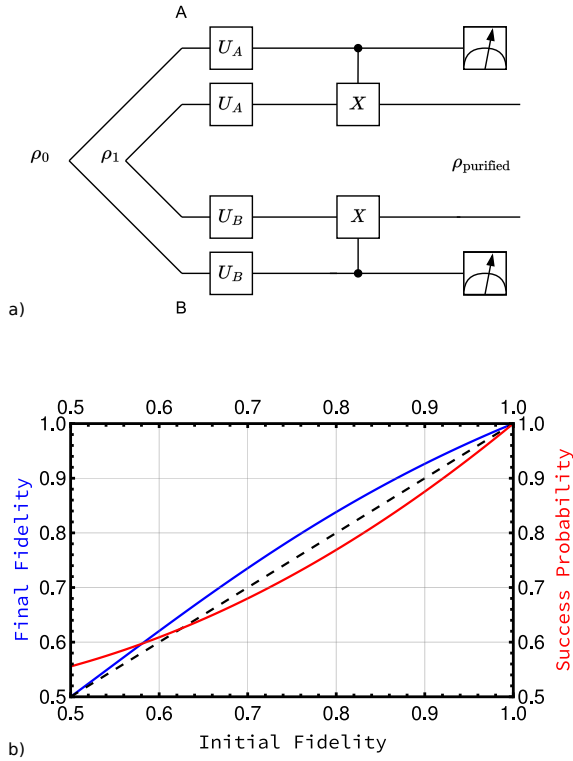$$C_{r+1} = \frac{C_r^2 + D_r^2}{N_r}, \quad D_{r+1} = \frac{2A_r B_r}{N_r}.$$
(30)

Figure 15: The Oxford Protocol. On a), the circuit required for the Oxford protocol. As long as the measurement results agree, a purified Bell pair is obtained. On b), the plot of the fidelity obtained and success probability of the Oxford protocol when applied to two Werner states in relation to its initial fidelity.

where $N_r = (A_r + B_r)^2 + (C_r + D_r)^2$ is equal to the probability of a successful purification round (i.e, the probability that Alice and Bob measurements agree). As opposed to the IBM protocol, this protocol has the advantage of not requiring a depolarization procedure between subsequent rounds of purification, leading to higher efficiencies [29, 44]. Furthermore, it has been shown that this procedure converges to the fixpoint defined by $(A_\infty = 1, B_\infty = C_\infty = D_\infty = 0)$ if and only if the initial fidelity (for Werner states, this corresponds to the parameter $A$) is greater than $\frac{1}{2}$ [71].

This protocol has been generalized by [72] to be applied to $n \geq 2$ Bell pairs and obtain a purified one. The Double Selection and Triple Selection protocols are simply the instances with $n = 3$ and $n = 4$. By increasing the number of auxiliary pairs, the amount of errors that go undetected by the protocols is reduced, resulting in
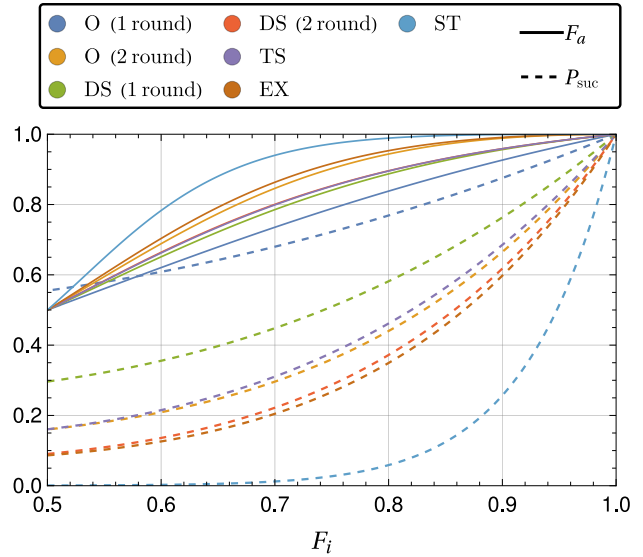


Figure 16: Probability of success $P_{\text{suc}}$ and fidelity achieved $F_a$ for the considered recurrence protocols (Oxford (O), Double Selection (DS), Triple Selection (TS), EXPEDIENT (EX) and STRINGENT (ST)) when applied to Werner states with an initial fidelity $F_i$. A tradeoff can be seen between these two quantities. For a recursive application of a given protocol, increasing the number of purification rounds increases the achieved fidelity at the cost of reducing the probability of success.

higher fidelities of the resulting state. However, this naturally comes with the downfall of reducing the probability of success of each purification round.

The other two protocols present in this paper, EXPEDIENT and STRINGENT, are 3-to-1 protocols that were developed within the context of topological quantum computing [73]. The circuit required to implement STRINGENT can be obtained from EXPEDIENT by adding some gates and single-qubit measurements. While STRINGENT is characterized for achieving high fidelities at the cost of low success probabilities, as it can be seen in Figure 16, both are some of the best performing purification protocols [31]. All of these protocols can be applied recursively, but increasing the number of purification rounds does not necessarily increases the overall protocol performance, since their success probability decreases exponentially with the number of rounds.

## D   Additional numerical results

In this section, we present complementary numerical results. In Figure 17 is possible to see different results regarding the probability of error of

---

| $F_{\min}$ | | | | | | |
|---|---|---|---|---|---|---|
| routine | 1% | 2% | 3% | 4% | 5% | 6% |
| 16-to-1 | .9238 | n/a | n/a | n/a | n/a | n/a |
| 32-to-1 | .8818 | .8996 | .9236 | n/a | n/a | n/a |
| 64-to-1 | .8608 | .8749 | .8890 | .9072 | n/a | n/a |
| 128-to-1 | .8479 | .8549 | .8711 | .8845 | .9002 | n/a |
| 256-to-1 | .8394 | .8494 | .8601 | .8713 | .8838 | .8984 |

Table 4: Minimum fidelity required to achieve purification varies according to different degrees of error in the resource states and routines. Routines that use more pairs would in principle imply utilizing resource states with a higher degree of error. However, it is possible to observe that using more pairs can lead to higher purification thresholds.

| $F_{\max}$ | | | | | | |
|---|---|---|---|---|---|---|
| routine | 1% | 2% | 3% | 4% | 5% | 6% |
| 16-to-1 | .9878 | n/a | n/a | n/a | n/a | n/a |
| 32-to-1 | .9899 | .9795 | .9650 | n/a | n/a | n/a |
| 64-to-1 | .9899 | .9799 | .9699 | .9587 | n/a | n/a |
| 128-to-1 | .9899 | .9799 | .9699 | .9599 | .9496 | n/a |
| 256-to-1 | .9899 | .9799 | .9699 | .9599 | .9599 | .9398 |

Table 5: Maximum achievable fidelity, according to different degrees of error of the resources states and sizes of the initial assemble. The achieved fidelity is primarily limited by the error of the resources states.

the protocol, for different levels of noise, ensemble sizes and computational constraints. These values were obtained solely using the theoretical expressions Equation (14) and Equation (15).

In Table 4 and Table 5 is possible to see the minimum fidelity required for purification, and the maximum achievable fidelity, respectively, for different degrees of error in the resource states and the sizes of the initial assemblies for the measurement-based version of the protocol.
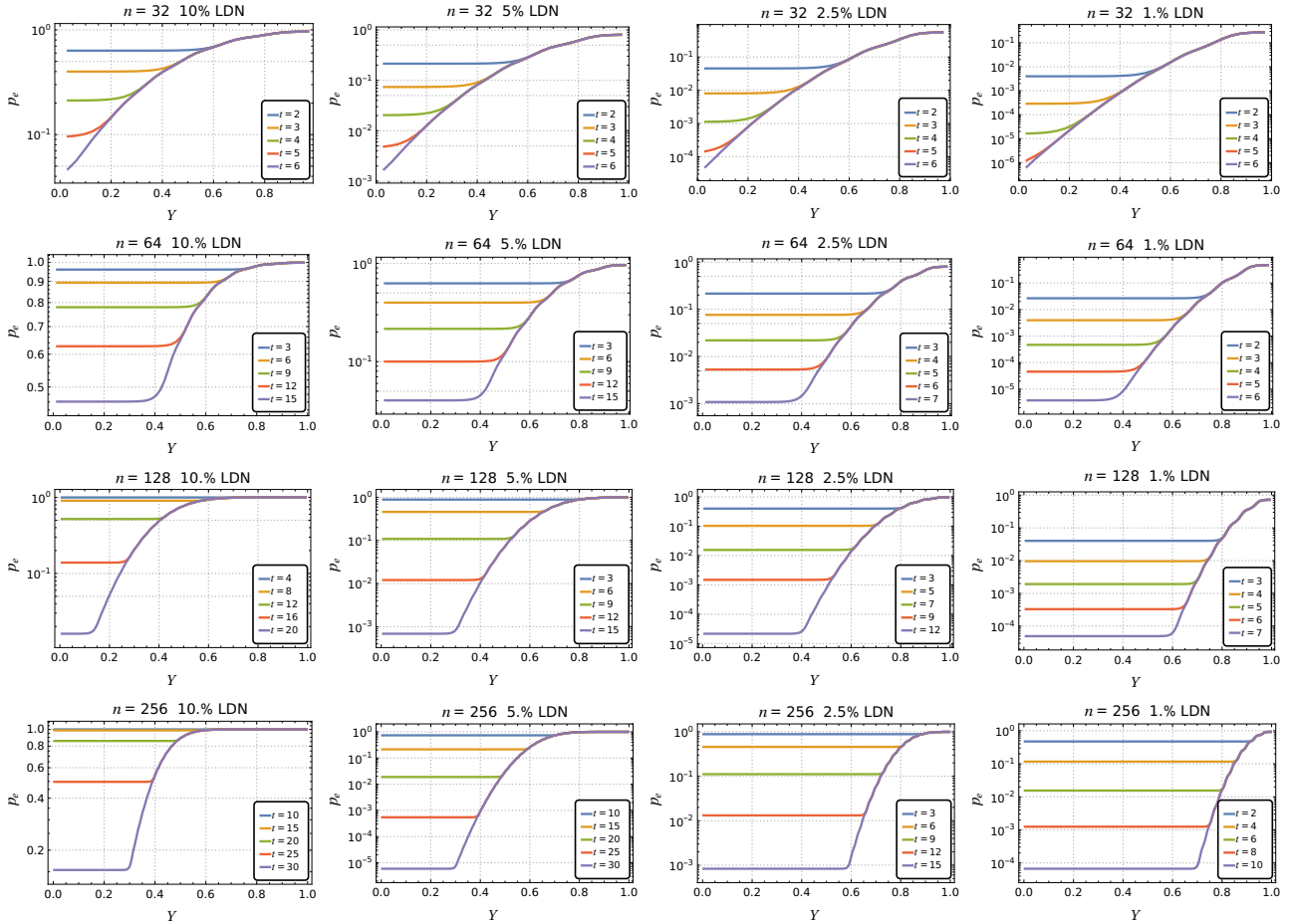
Figure 17: Plot of the error probability $p_e$ as a function of the yield for a number $n$ of pairs, where $n = 32$ (first line), $n = 64$ (second line), $n = 128$ (third line), and $n = 256$ (fourth line). Local depolarizing noise was assumed to be 10% (first column), 5% (second column), 2.5% (third column), and 1% (fourth column). In these plots, it is possible to see how the computational cost, expressed by the parameter $t$, limits the protocol's purification capabilities. The horizontal line on each curve indicates the existence of a saturation point, where most of the considered error patterns were assigned to a syndrome, and no advantage is obtained by sacrificing more pairs (i.e., using lower yields). The computational cost becomes a limiting factor when aiming for purification in scenarios with high amount of noise and/or a high number of pairs. However, for low-entropy regimes ($\leq 2.5\%$ LDN), this cost is still bearable even when considering an ensemble with 256 pairs. From these plots, it is also clear the increase in the protocol's efficiency, expressed by the yield, with the size of the ensemble.